



Европейская экономическая комиссия

Комитет по внутреннему транспорту

Рабочая группа по автомобильному транспорту

**Группа экспертов по Европейскому соглашению,
касающемуся работы экипажей транспортных средств,
производящих международные автомобильные
перевозки (ЕСТР)**

Двадцать шестая сессия

Женева, 14 июня 2021 года

Пункт 2 b) предварительной повестки дня

Программа работы: Добавление 1С

Добавление 1С

Представлено правительством Португалии*

В приложении к настоящему документу, представленному Португалией (исполняющей функции Председателя в Совете Европейского союза), содержатся предложения по внесению поправок в приложение 1С в целях приведения спецификаций Европейского союза по смарт-тахографу в соответствие с правовой базой ЕСТР.

* Изменения к настоящему документу выделены жирным шрифтом в случае новых положений и зачеркиванием в случае исключенных элементов.



Приложение

Содержание

	<i>Стр.</i>
Введение	19
1. Определения	21
2. Общие характеристики и функции контрольного устройства	29
2.1 Общие характеристики	29
2.2 Функции	30
2.3 Режимы работы	31
2.4 Безопасность	32
3. Требования к конструкции и функциям контрольного устройства	33
3.1 Контроль за карточками и их извлечением	33
3.2 Измерение скорости, местоположения и пробега	34
3.3 Измерение времени	35
3.4 Контроль за работой водителя	36
3.5 Контроль за статусом управления	36
3.6 Записи водителей	37
3.7 Управление системой блокировки, установленной предприятием	40
3.8 Мониторинг работы системы контроля	41
3.9 Выявление соответствующих событий и/или неисправностей	41
3.10 «Встроенные системы проверки и самопроверки»	44
3.11 Считывание данных из блока памяти	45
3.12 Регистрация и хранение данных в блоке памяти	45
3.13 Считывание данных с карточек тахографов	58
3.14 Регистрация и хранение данных на карточках тахографов	59
3.15 Вывод на дисплей	61
3.16 Вывод на печать	63
3.17 Сигналы предупреждения	64
3.18 Загрузка данных на внешние носители	65
3.19 Удаленная связь для целевых проверок на дорогах	66
3.20 Обмен данными с дополнительными внешними устройствами	66
3.21 Калибровка	68
3.22 Проверка калибровки на дорогах	69
3.23 Корректировка времени	70
3.24 Функциональные характеристики	70
3.25 Материалы	71
3.26 Маркировка	71
3.27 Мониторинг пересечения границ	72
3.28 Обновление программного обеспечения	72

4.	Требования к конструкции и функциям карточек тахографов	73
4.1	Видимые данные	73
4.2	Защита	75
4.3	Стандарты	76
4.4	Спецификации на воздействие окружающих условий и электромагнитную совместимость	76
4.5	Хранение данных	76
5.	Установка контрольного устройства	99
5.1	Установка	99
5.2	Установочная табличка	101
5.3	Наложение пломб	102
6.	Проверки, инспекции и ремонтные работы	103
6.1	Утверждение техников, мастерских и изготовителей транспортных средств	103
6.2	Проверка новых или отремонтированных компонентов	103
6.3	Инспекция установки	103
6.4	Периодические инспекции	103
6.5	Измерение погрешностей	105
6.6	Ремонтные работы	105
7.	Выдача карточек	105
8.	Утверждение типа контрольного устройства и карточек тахографов	106
8.1	Общие вопросы	106
8.2	Сертификат защиты	107
8.3	Сертификат функциональности	107
8.4	Сертификат эксплуатационной совместимости	108
8.5	Сертификат официального утверждения типа	109
ДОБАВЛЕНИЕ: ЗНАК ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ И СЕРТИФИКАТ		111
I.	ЗНАК ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ	111
II.	СЕРТИФИКАТ ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ АНАЛОГОВЫХ ТАХОГРАФОВ	113
III.	СЕРТИФИКАТ ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ ЦИФРОВЫХ ТАХОГРАФОВ	114
IV.	СЕРТИФИКАТ ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ СМАРТ-ТАХОГРАФОВ	115
Подраздел 1	Словарь данных	116
1.	Введение	125
1.1	Метод определения типов данных	125
1.2	Справочные материалы	125
2.	Определения типов данных	126
2.1	ActivityChangeInfo (данные об изменении вида деятельности)	126
2.2	Address (адрес)	128
2.3	AESKey (ключ AES)	128
2.4	AES128Key (ключ AES128)	128

2.5	AES192Key (ключ AES192)	129
2.6	AES256Key (ключ AES256)	129
2.7	BCDString (строка BCD)	129
2.8	CalibrationPurpose (цель калибровки)	129
2.9	CardActivityDailyRecord (запись вида деятельности на карточке)	130
2.10	CardActivityLengthRange (длина записи о деятельности на карточке)	131
2.11	CardApprovalNumber (номер официального утверждения карточки)	131
2.11a	CardBorderCrossings (данные на карточке о пересечении границы)	131
2.11b	CardBorderCrossingRecord (запись на карточке о пересечении границы)	131
2.12	CardCertificate (сертификат карточки)	132
2.13	CardChipIdentification (идентификация микросхемы карточки)	132
2.14	CardConsecutiveIndex (порядковый индекс карточки)	132
2.15	CardControlActivityDataRecord (запись данных на карточке о деятельности по контролю)	133
2.16	CardCurrentUse (текущее использование карточки)	133
2.17	CardDriverActivity (запись на карточке о деятельности водителя)	133
2.18	CardDrivingLicenceInformation (информация о водительском удостоверении на карточке)	134
2.19	CardEventData (данные о событиях на карточке)	135
2.20	CardEventRecord (запись о событиях на карточке)	135
2.21	CardFaultData (данные о сбоях в работе карточки)	136
2.22	CardFaultRecord (запись о сбоях в работе карточки)	136
2.23	CardIccIdentification (идентификация карточки ИС)	136
2.24	CardIdentification (идентификация карточки)	137
2.24a	CardLoadTypeEntries (данные о типе груза на карточке)	137
2.24b	CardLoadTypeEntryRecord (записи данных о типе груза на карточке)	138
2.24c	CardLoadUnloadOperations (операции по загрузке/разгрузке на карточке)	138
2.24d	CardLoadUnloadRecord (запись об операциях загрузки/разгрузки на карточке)	139
2.25	CardMACertificate (сертификат карточки МА)	139
2.26	CardNumber (номер карточки)	139
2.26a	CardPlaceAuthDailyWorkPeriod (разрешенный ежедневный период работы и место, указанные на карточке)	140
2.27	CardPlaceDailyWorkPeriod (ежедневный период работы и место, указанные на карточке)	140
2.28	CardPrivateKey (закрытый ключ карточки)	141
2.29	CardPublicKey (открытый ключ карточки)	141
2.30	CardRenewalIndex (индекс возобновления карточки)	141
2.31	CardReplacementIndex (индекс замены карточки)	141
2.32	CardSignCertificate (сертификат подписи карточки)	141
2.33	CardSlotNumber (номер считывающего устройства карточки)	141
2.34	CardSlotsStatus (статус считывающих устройств карточки)	142

2.35	CardSlotsStatusRecordArray (статус считывающих устройств карточки и метаданные)	142
2.36	CardStructureVersion (версия структуры карточки)	142
2.37	CardVehicleRecord (запись использования транспортного средства на карточке) ...	143
2.38	CardVehiclesUsed (использованное транспортное средство)	144
2.39	CardVehicleUnitRecord (запись использованных единиц транспортных средств)	144
2.40	CardVehicleUnitsUsed (использованные единицы транспортных средств)	145
2.41	Certificate (сертификат)	145
2.42	CertificateContent (содержание сертификата)	145
2.43	CertificateHolderAuthorisation (идентификатор прав держателя сертификата)	146
2.44	CertificateRequestID (идентификатор запроса на сертификат)	146
2.45	CertificationAuthorityKID (сертификационный орган KID)	147
2.46	CompanyActivityData (данные об операциях с карточкой предприятия)	147
2.47	CompanyActivityType (тип операции, произведенной предприятием)	148
2.48	CompanyCardApplicationIdentification (идентификация приложения карточки предприятия)	149
2.48a	CompanyCardApplicationIdentificationV2 (идентификация приложения карточки предприятияV2)	149
2.49	CompanyCardHolderIdentification (идентификация держателя карточки предприятия)	149
2.50	ControlCardApplicationIdentification (идентификация приложения карточки контролера)	150
2.50a	ControlCardApplicationIdentificationV2 (идентификация приложения карточки контролераV2)	150
2.51	ControlCardControlActivityData (данные о проверочных операциях на карточке контролера)	150
2.52	ControlCardHolderIdentification (идентификация держателя карточки контролера)	151
2.53	ControlType (тип контроля)	151
2.54	CurrentDateTime (текущая дата/время)	153
2.55	CurrentDateTimeRecordArray (данные о текущей дате/времени и метаданные)	153
2.56	DailyPresenceCounter (счетчик ежедневного присутствия)	153
2.57	Datef (формат даты)	154
2.58	DateOfDayDownloaded (дата и время загрузки)	154
2.59	DateOfDayDownloadedRecordArray (данные о дне и времени загрузки и метаданные)	154
2.60	Distance (расстояние)	155
2.60a	DownloadInterfaceVersion (версия загрузочного интерфейса)	155
2.61	DriverCardApplicationIdentification (идентификация приложения карточки водителя)	155
2.61a	DriverCardApplicationIdentificationV2 (идентификация приложения карточки водителяV2)	156
2.62	DriverCardHolderIdentification (идентификация держателя карточки водителя)	157

2.63	DSRCSecurityData (система защиты данных DSRCs)	157
2.64	EGFCertificate (сертификат EGF)	158
2.65	EmbedderIdAssemblerId (идентификатор монтажного/сборочного предприятия)	158
2.66	EntryTypeDailyWorkPeriod (ввод данных о периоде и типе ежедневной работы)	158
2.67	EquipmentType (тип оборудования)	159
2.68	EuropeanPublicKey (европейский открытый ключ)	160
2.69	EventFaultRecordPurpose (цель регистрации события или неисправности)	160
2.70	EventFaultType (событие: тип неисправности)	161
2.71	ExtendedSealIdentifier (расширенный идентификатор пломбы)	166
2.72	ExtendedSerialNumber (расширенный серийный номер)	166
2.73	FullCardNumber (полный номер карточки)	167
2.74	FullCardNumberAndGeneration (полный номер и поколение карточки)	167
2.75	Generation (поколение)	168
2.76	GeoCoordinates (геокоординаты)	168
2.77	GNSSAccuracy (точность ГНСС)	168
2.78	GNSSAccumulatedDriving (накопленное время управления по ГНСС)	168
2.79	GNSSAccumulatedDrivingRecord (запись накопленного времени управления по ГНСС)	169
2.79a	GNSSAuthAccumulatedDriving (разрешенное накопленное время управления по ГНСС)	169
2.79b	GNSSAuthStatusADRecord (запись данных в БУ о НакБУ по ГНСС)	170
2.79c	GNSSPlaceAuthRecord (запись аутентифицированного места по ГНСС)	170
2.80	GNSSPlaceRecord (запись названия места по ГНСС)	171
2.81	HighResOdometer (счетчик пробега с высоким разрешением)	171
2.82	HighResTripDistance (расстояние, пройденное за рейс, с высоким разрешением) ...	171
2.83	HolderName (фамилия и имя (имена) держателя)	171
2.84	Зарезервировано для будущего использования	172
2.85	K-ConstantOfRecordingEquipment (постоянная К записывающего оборудования)	172
2.86	KeyIdentifier (идентификатор ключа)	172
2.87	KMWCKey (ключ KMWC)	172
2.88	Language (язык)	173
2.89	LastCardDownload (последняя дата загрузки с карточки)	173
2.89a	LengthOfFollowingData (длина следующих данных)	173
2.90	LinkCertificate (связывающий сертификат)	173
2.90a	LoadType (тип груза)	173
2.91	L-TyreCircumference (окружность шины L)	173
2.92	MAC (MAC)	174
2.93	ManualInputFlag (метка ручного ввода)	174

2.94	ManufacturerCode (код изготовителя)	174
2.95	ManufacturerSpecificEventFaultData (данные о неисправности, связанной с конкретным изготовителем)	174
2.96	MemberStateCertificate (сертификат государства-члена)	175
2.97	MemberStateCertificateRecordArray (записи о сертификате государства-члена и метаданные)	175
2.98	MemberStatePublicKey (открытый ключ государства-члена)	175
2.99	Name (название)	175
2.100	NationAlpha (буквенный код страны)	176
2.101	NationNumeric (цифровой код страны)	176
2.101a	NoOfBorderCrossingRecords (число записей о пересечении границы)	176
2.102	NoOfCalibrationRecords (число записей о калибровках)	176
2.103	NoOfCalibrationsSinceDownload (число калибровок после загрузки данных)	176
2.104	NoOfCardPlaceRecords (число записей на карточке, касающихся мест)	177
2.105	NoOfCardVehicleRecords (число записей на карточке, касающихся транспортных средств)	177
2.106	NoOfCardVehicleUnitRecords (число записей на карточке, касающихся единиц транспортных средств)	177
2.107	NoOfCompanyActivityRecords (число записей, касающихся операций предприятия)	177
2.108	NoOfControlActivityRecords (число записей, касающихся операций по контролю)	177
2.109	NoOfEventsPerType (число событий по типу)	178
2.110	NoOfFaultsPerType (число неисправностей по типу)	178
2.111	NoOfGNSSADRecords (число записей ГНСС, касающихся НакВУ)	178
2.111a	NoOfLoadUnloadRecords (число записей, касающихся загрузки/разгрузки)	178
2.112	NoOfSpecificConditionRecords (число записей, касающихся особых условий)	178
2.112a	NoOfLoadTypeEntryRecords (число записей о типе поступившего груза)	178
2.113	OdometerShort (показания счетчика пробега)	179
2.114	OdometerValueMidnight (показания счетчика пробега в полночь)	179
2.114a	OperationType (тип операции)	179
2.115	OdometerValueMidnightRecordArray (показания счетчика пробега в полночь и метаданные)	179
2.116	OverspeedNumber (число превышений скорости)	180
2.116a	PlaceAuthRecord (запись аутентификации места)	180
2.116b	PlaceAuthStatusRecord (запись статуса аутентификации места)	180
2.117	PlaceRecord (место, в котором начинается или заканчивается ежедневный период работы)	181
2.117a	PositionAuthenticationStatus (статус аутентификации местоположения)	182
2.118	PreviousVehicleInfo (информация о предыдущем транспортном средстве)	182
2.119	PublicKey (открытый ключ)	182
2.120	RecordType (тип записи)	183

2.121 RegionAlpha (буквенный код региона)	184
2.122 RegionNumeric (цифровой код региона)	184
2.123 RemoteCommunicationModuleSerialNumber (серийный номер модуля удаленной связи)	185
2.124 RSAKeyModulus (модуль ключей RSA)	185
2.125 RSAKeyPrivateExponent (закрытая экспонента ключа RSA)	186
2.126 RSAKeyPublicExponent (открытая экспонента ключа RSA)	186
2.127 RtmData (данные удаленного мониторинга тахографа)	186
2.128 SealDataCard (данные, касающиеся пломб, указанных на карточке)	186
2.129 SealDataVu (данные, касающиеся пломб, в БУ)	186
2.130 SealRecord (запись, касающаяся пломб)	187
2.131 SensorApprovalNumber (номер официального утверждения датчика)	187
2.132 SensorExternalGNSSApprovalNumber (номер официального утверждения внешнего датчика ГНСС)	187
2.133 SensorExternalGNSSCoupledRecord (запись о соединении внешнего датчика ГНСС)	188
2.134 SensorExternalGNSSIdentification (идентификационные данные внешнего датчика ГНСС)	188
2.135 SensorExternalGNSSInstallation (данные, касающиеся установки внешнего датчика ГНСС)	188
2.136 SensorExternalGNSSOSIdentifier (идентификатор внешнего датчика ОС ГНСС)	189
2.137 SensorExternalGNSSK3Identifier (идентификатор внешнего датчика КЗ ГНСС)	189
2.138 SensorGNSSCouplingDate (дата соединения датчика ГНСС с БУ)	189
2.139 SensorGNSSSerialNumber (серийный номер датчика ГНСС)	190
2.140 SensorIdentification (идентификация датчика)	190
2.141 SensorInstallation (установка датчика)	190
2.142 SensorInstallationSecData (данные, касающиеся защиты при установке датчика)	191
2.143 SensorOSIdentifier (идентификатор ОС датчика)	191
2.144 SensorPaired (подсоединенный датчик)	191
2.145 SensorPairedRecord (запись данных о подсоединении датчика)	192
2.146 SensorPairingDate (дата подсоединения датчика)	192
2.147 SensorSCIdentifier (идентификатор КЗ датчика)	192
2.148 SensorSerialNumber (серийный номер датчика)	192
2.149 Signature (подпись)	192
2.150 SignatureRecordArray (набор подписей и метаданные)	193
2.151 SimilarEventsNumber (число похожих событий)	193
2.152 SpecificConditionRecord (запись особых условий)	193
2.153 SpecificConditions (особые условия)	194
2.154 SpecificConditionType (тип особых условий)	194
2.155 Speed (скорость)	194
2.156 SpeedAuthorised (разрешенная скорость)	195

2.157	SpeedAverage (средняя скорость)	195
2.158	SpeedMax (максимальная скорость)	195
2.158a	TachographCardsGen1Suppression (отмена карточек тахографа первого поколения)	195
2.159	TachographPayload (пакет данных тахографа)	195
2.160	Reserved for future use (зарезервировано для использования в будущем)	195
2.161	TDesSessionKey (тройной ключ сеанса в системе TDes)	196
2.162	TimeReal (реальное время)	196
2.163	TyreSize (размер шин)	196
2.164	VehicleIdentificationNumber (идентификационный номер транспортного средства)	196
2.165	VehicleIdentificationNumberRecordArray (идентификационный номер транспортного средства и метаданные)	197
2.166	VehicleRegistrationIdentification (идентификация регистрации транспортного средства)	197
2.166a	VehicleRegistrationIdentificationRecordArray (идентификация регистрации транспортного средства и метаданные)	197
2.167	VehicleRegistrationNumber (регистрационный номер транспортного средства)	198
2.168	VehicleRegistrationNumberRecordArray (регистрационный номер транспортного средства и метаданные)	198
2.169	VuAbility (характеристики БУ)	198
2.170	VuActivityDailyData (данные в БУ о деятельности за данный день)	199
2.171	VuActivityDailyRecordArray (записи в БУ о деятельности или статусе и метаданные)	199
2.172	VuApprovalNumber (номер официального утверждения БУ)	200
2.173	VuCalibrationData (данные в БУ о калибровке)	200
2.174	VuCalibrationRecord (запись в БУ о калибровке)	200
2.175	VuCalibrationRecordArray (данные в БУ о калибровке и метаданные)	203
2.176	VuCardIWData (данные в БУ о циклах ввода и извлечения карточек)	204
2.177	VuCardIWRecord (запись данных в БУ о циклах ввода и извлечения карточек)	204
2.178	VuCardIWRecordArray (данные о циклах ввода и извлечения карточек и метаданные)	205
2.179	VuCardRecord (запись данных в БУ об используемой карточке)	206
2.180	VuCardRecordArray (данные об используемых карточках и метаданные)	206
2.181	VuCertificate (сертификат БУ)	207
2.182	VuCertificateRecordArray (сертификат БУ и метаданные)	207
2.183	VuCompanyLocksData (данные в БУ о блокировке предприятием)	207
2.184	VuCompanyLocksRecord (запись данных в БУ о блокировке предприятием)	208
2.185	VuCompanyLocksRecordArray (запись данных в БУ о блокировке предприятием и метаданные)	208
2.185a	VuConfigurationLengthRange (длина данных о конфигурации БУ)	209
2.186	VuControlActivityData (данные в БУ о контроле за деятельностью)	209
2.187	VuControlActivityRecord (запись данных в БУ о контроле за деятельностью)	209

2.188 VuControlActivityRecordArray (запись данных в БУ о контроле за деятельностью и метаданные)	210
2.189 VuDataBlockCounter (счетчик нумерации циклов ввода и извлечения карточек в БУ)	210
2.190 VuDetailedSpeedBlock (данные в БУ о скорости транспортного средства)	211
2.191 VuDetailedSpeedBlockRecordArray (данные в БУ о скорости транспортного средства и метаданные)	211
2.192 VuDetailedSpeedData (детальные данные в БУ о скорости транспортного средства)	211
2.192a VuDigitalMapVersion (версия цифровой карты в БУ)	212
2.193 VuDownloadablePeriod (сроки хранения данных в БУ)	212
2.194 VuDownloadablePeriodRecordArray (сроки хранения записей данных в БУ и метаданные)	212
2.195 VuDownloadActivityData (данные в БУ о загрузке)	213
2.196 VuDownloadActivityDataRecordArray (данные в БУ о загрузке и метаданные)	213
2.197 VuEventData (данные в БУ о событиях)	214
2.198 VuEventRecord (запись данных в БУ о событиях)	214
2.199 VuEventRecordArray (запись данных в БУ о событиях и метаданные)	216
2.200 VuFaultData (данные в БУ о неисправностях)	216
2.201 VuFaultRecord (запись данных в БУ о неисправностях)	216
2.202 VuFaultRecordArray (запись данных в БУ о неисправностях и метаданные)	218
2.203 VuGNSSADRecord (запись данных в БУ о НакВУ по ГНСС)	218
2.203a VuBorderCrossingRecord (запись данных в БУ о пересечении границы)	219
2.203b VuBorderCrossingRecordArray (запись данных в БУ о пересечении границы и метаданные)	220
2.204 VuGNSSADRecordArray (запись данных в БУ о НакВУ по ГНСС и метаданные)	220
2.204a VuGnssMaximalTimeDifference (данные в БУ о максимальной разнице во времени по ГНСС)	221
2.205 VuIdentification (идентификация бортового устройства)	221
2.206 VuIdentificationRecordArray (идентификация БУ и метаданные)	222
2.207 VuITSConsentRecord (запись в БУ о согласии водителя использовать ИТС)	222
2.208 VuITSConsentRecordArray (запись в БУ о согласии водителя использовать ИТС и метаданные)	223
2.208a VuLoadUnloadRecord (запись данных в БУ о загрузке/разгрузке)	223
2.208b VuLoadUnloadRecordArray (запись данных в БУ о загрузке/разгрузке и метаданные)	224
2.209 VuManufacturerAddress (адрес изготовителя БУ)	224
2.210 VuManufacturerName (наименование изготовителя БУ)	224
2.211 VuManufacturingDate (дата изготовления БУ)	225
2.212 VuOverSpeedingControlData (данные в БУ о превышении скорости)	225
2.213 VuOverSpeedingControlDataRecordArray (данные в БУ о превышении скорости и метаданные)	225

2.214 VuOverSpeedingEventData (данные в БУ о событиях превышения скорости)	226
2.215 VuOverSpeedingEventRecord (запись данных в БУ о событиях превышения скорости)	226
2.216 VuOverSpeedingEventRecordArray (запись данных в БУ о событиях превышения скорости и метаданные)	227
2.217 VuPartNumber (номер детали БУ)	227
2.218 VuPlaceDailyWorkPeriodData (данные в БУ о месте, где начинается и заканчивается ежедневный период работы)	228
2.219 VuPlaceDailyWorkPeriodRecord (запись данных в БУ о месте, где начинается и заканчивается ежедневный период работы)	228
2.220 VuPlaceDailyWorkPeriodRecordArray (запись данных в БУ о месте, где начинается и заканчивается ежедневный период работы, и метаданные)	229
2.221 VuPrivateKey (закрытый ключ БУ)	229
2.222 VuPublicKey (открытый ключ БУ)	230
2.222a VuRtcTime (время в БУ по часам реального времени)	230
2.223 VuSerialNumber (серийный номер БУ)	230
2.224 VuSoftInstallationDate (дата установки программного обеспечения БУ)	230
2.225 VuSoftwareIdentification (идентификация программного обеспечения БУ)	230
2.226 VuSoftwareVersion (версия программного обеспечения БУ)	230
2.227 VuSpecificConditionData (данные об особых условиях в БУ)	231
2.228 VuSpecificConditionRecordArray (данные об особых условиях в БУ и метаданные)	231
2.229 VuTimeAdjustmentData (данные в БУ о корректировке времени)	231
2.230 Reserved for future use (зарезервирован для использования в будущем)	232
2.231 Reserved for future use (зарезервирован для использования в будущем)	232
2.232 VuTimeAdjustmentRecord (запись данных в БУ о корректировке времени)	232
2.233 VuTimeAdjustmentRecordArray (запись данных в БУ о корректировке времени и метаданные)	233
2.234 WorkshopCardApplicationIdentification (идентификация приложения карточки мастерской)	234
2.234a WorkshopCardApplicationIdentificationV2 (идентификация приложения карточки мастерской V2)	235
2.234b WorkshopCardCalibrationAddData (запись дополнительных данных калибровки карточки мастерской)	235
2.234c WorkshopCardCalibrationAddDataRecord (запись дополнительных данных калибровки карточки мастерской)	236
2.235 WorkshopCardCalibrationData (данные калибровки карточки мастерской)	236
2.236 WorkshopCardCalibrationRecord (запись данных калибровки карточки мастерской)	237
2.237 WorkshopCardHolderIdentification (идентификация держателя карточки мастерской)	239
2.238 WorkshopCardPIN (ПИН-код карточки мастерской)	239
2.239 W-VehicleCharacteristicConstant (характеристическая постоянная W транспортного средства)	239

2.240	VuPowerSupplyInterruptionRecord (запись данных в БУ о прекращении электропитания)	239
2.241	VuPowerSupplyInterruptionRecordArray (запись данных в БУ о прекращении электропитания и метаданные)	240
2.242	VuSensorExternalGNSSCoupledRecordArray (запись данных в БУ о соединении с внешним датчиком ГНСС и метаданные)	241
2.243	VuSensorPairedRecordArray (запись данных о спаренном датчике БУ и метаданные)	241
3.	Определения диапазонов значений и размеров	241
4.	Наборы символов	242
5.	Кодирование	242
6.	Идентификаторы объектов и идентификаторы приложений	243
6.1	Идентификаторы объектов	243
6.2	Идентификаторы приложения	244
Подраздел 2	Спецификация на карточки тахографов	245
1.	Введение	247
1.1	Сокращения	247
1.2	Справочные материалы	248
2.	Электрические и физические характеристики	248
2.1	Напряжение питания и потребление тока	249
2.2	Напряжение программирования V_{pp}	249
2.3	Формирование и частота тактовых сигналов	249
2.4	Контакт «вход/выход»	249
2.5	Состояние карточки	249
3.	Аппаратное обеспечение и передача данных	250
3.1	Введение	250
3.2	Протокол передачи данных	250
3.3	Правила доступа	252
3.4	Обзор команд и кодов ошибок	255
3.5	Описания команд	257
4.	Структура карточек тахографов	292
4.1	Главный файл MF	292
4.2	Приложения карточки водителя	294
4.3	Приложения карточки мастерской	302
4.4	Приложения контрольной карточки	315
4.5	Приложения карточки предприятия	319
Подраздел 3	Пиктограммы	324

Подраздел 4	Распечатки	328
1.	Общие положения	329
2.	Спецификации блоков данных	329
3.	Спецификации распечатки данных	338
3.1	Распечатка сохраненных на карточке данных о деятельности водителя за сутки	339
3.2	Распечатка сохраненных в БУ данных о деятельности водителя за сутки	340
3.3	События и неисправности из распечатки данных карточки	341
3.4	События и неисправности из распечатки БУ	341
3.5	Распечатка технических данных	342
3.6	Распечатка данных о превышении скорости	342
3.7	Архив вставленных карточек	343
Подраздел 5	Дисплей	344
Подраздел 6	Передний соединитель для калибровки и загрузки	345
1.	Аппаратное обеспечение	346
1.1	Соединитель	346
1.2	Расположение контактов	348
1.3	Блок-схема	348
2.	Интерфейс загрузки данных	348
3.	Интерфейс калибровки	349
Подраздел 7	Протоколы загрузки данных	351
1.	Введение	353
1.1	Сфера применения	353
1.2	Сокращения и обозначения	353
2.	Загрузка данных с БУ	354
2.1	Процедура загрузки	354
2.2	Протокол загрузки данных	354
2.3	Сохранение файлов на ВН	376
3.	Протокол загрузки данных с карточек тахографа	376
3.1	Сфера применения	376
3.2	Определения	376
3.3	Загрузка с карточки	376
3.4	Формат хранения данных	380
4.	Загрузка данных с карточки тахографа с помощью бортового устройства	381
Подраздел 8	Протокол калибровки	382
1.	Введение	384
2.	Термины, определения и справочные материалы	387
3.	Обзор функций	387
3.1	Поддерживаемые функции	387
3.2	Коды ответов	388

4.	Функции обмена данными	388
4.1	Функция StartCommunication	389
4.2	Функция StopCommunication	391
4.3	Функция TesterPresent	392
5.	Функции управления	393
5.1	Функция StartDiagnosticSession	394
5.2	Функция SecurityAccess	396
6.	Функции передачи данных	399
6.1	Функция ReadDataByIdentifier	400
6.2	Функция WriteDataByIdentifier	402
7.	Настройка проверочных импульсов — контрольный функциональный блок регулировки входного/выходного сигнала	404
7.1	Функция InputOutputControlByIdentifier	404
8.	Функция RoutineControl (корректировка времени)	407
8.1	Описание сообщения	407
8.2	Формат сообщений	407
9.	Форматы записей данных	410
9.1	Диапазоны передаваемых параметров	410
9.2	Форматы dataRecords	411
Подраздел 9	Официальное утверждение типа	415
1.	Введение	416
1.1	Официальное утверждение типа	416
1.2	Справочные материалы	417
2.	Рабочие испытания бортового устройства	418
3.	Рабочие испытания датчика движения	422
4.	Функциональные испытания карточек тахографа	425
5.	Испытания внешнего устройства ГНСС	433
6.	Испытания внешнего устройства удаленной связи	436
7.	Функциональные испытания бумаги	437
8.	Испытания на эксплуатационную совместимость	439
9.	Тесты OSNMA	440
9.1	Введение	440
9.2	Применимые условия	440
9.3	Определения и сокращения	440
9.4	Оборудование для генерации сигналов ГНСС	441
9.5	Условия испытаний	441
9.6	Спецификация тестов	442

Подраздел 10	Требования в области безопасности	445
Подраздел 11	Общие механизмы безопасности	446
	Преамбула	449
ЧАСТЬ А	СИСТЕМА ТАХОГРАФОВ ПЕРВОГО ПОКОЛЕНИЯ	449
1.	Введение	449
1.1	Справочные материалы	449
1.2	Условные обозначения и сокращение терминов	450
2.	Криптографические системы и алгоритмы	451
2.1	Криптографические системы	451
2.2	Криптографические алгоритмы	452
3.	Ключи и сертификаты	452
3.1	Генерация и рассылка ключей	452
3.2	Ключи	454
3.3	Сертификаты	455
4.	Механизм взаимной аутентификации	458
5.	Механизмы обеспечения конфиденциальности, целостности и аутентификации данных в процессе их передачи между БУ и карточками	461
5.1	Защищенный обмен сообщениями	461
5.2	Обработка ошибок при криптозащищенном обмене сообщениями	462
5.3	Алгоритм расчета криптографических контрольных сумм	463
5.4	Алгоритм расчета криптограмм для защиты конфиденциальности Dos	463
6.	Механизмы цифровой подписи при загрузке данных	464
6.1	Генерация подписей	464
6.2	Проверка подписей	464
ЧАСТЬ В	СИСТЕМА ТАХОГРАФОВ ВТОРОГО ПОКОЛЕНИЯ	466
7.	Введение	466
7.1	Справочные материалы	466
7.2	Условные обозначения и сокращения	467
7.3	Определения	468
8.	Криптографические системы и алгоритмы	468
8.1	Криптографические системы	468
8.2	Криптографические алгоритмы	469
9.	Ключи и сертификаты	471
9.1	Асимметричные пары ключей и сертификаты открытых ключей	471
9.2	Симметричные ключи	479
9.3	Сертификаты	487
10.	Взаимная аутентификация и безопасный обмен сообщениями с карточкой БУ	490
10.1	Общие положения	490
10.2	Взаимная проверка последовательности сертификата	491
10.3	Аутентификация БУ	496

10.4	Аутентификация микросхемы и согласование сеансовых ключей	498
10.5	Защищенный обмен сообщениями	500
11.	Соединение, взаимная аутентификация и защищенный обмен сообщениями между БУ и внешним устройством ГНСС	505
11.1	Общие положения	505
11.2	Соединение БУ и внешнего устройства ГНСС	505
11.3	Взаимная проверка последовательности сертификатов	506
11.4	Аутентификация БУ, аутентификация микросхемы и согласование сеансовых ключей	508
11.5	Защищенный обмен сообщениями	508
12.	Соединение и связь между БУ и датчиком движения	509
12.1	Общие положения	509
12.2	Соединение БУ и датчика движения с использованием различных поколений ключей	509
12.3	Соединение и связь между БУ и датчиком движения с использованием AES	510
12.4	Соединение БУ и датчика движения с использованием различных поколений оборудования	512
13.	Защита удаленной связи по DSRC	512
13.1	Общие положения	512
13.2	Шифрование данных тахографа и генерирование MAC	513
13.3	Проверка и расшифровка данных тахографа	514
14.	Подписание загружаемых данных и проверка подписей	515
14.1	Общие положения	515
14.2	Генерация подписей	515
14.3	Проверка подписей	516
Подраздел 12	Определение местоположения при помощи глобальной навигационной спутниковой системы (ГНСС)	519
1.	Введение	520
1.1	Сфера охвата	520
1.2	Сокращения и обозначения	521
2.	Основные характеристики приемника ГНСС	521
3.	Сообщения, выдаваемые приемником ГНСС	523
4.	Бортовое устройство с внешним устройством ГНСС	526
4.1	Конфигурация	526
4.2	Связь между внешним устройством ГНСС и бортовым устройством	527
4.3	Соединение, взаимная аутентификация и согласование сеансовых ключей между внешним устройством ГНСС и бортовым устройством.....	533
4.4	Обработка ошибок	533
5.	Бортовое устройство без внешнего устройства ГНСС	534
5.1	Конфигурация	534
5.2	Передача информации от приемника ГНСС в БУ	534
5.3	Передача информации из БУ в приемник ГНСС	535
5.4	Обработка ошибок	535

6.	Обработка и регистрация данных о местоположении с помощью БУ	535
7.	Нестыковка во времени ГНСС	537
8.	Противоречивые данные о движении транспортного средства	537
Подраздел 13	Интерфейс ИТС	540
1.	Введение	541
1.1	Сфера охвата	541
1.2	Акронимы и определения	541
2.	Стандарты, на которые сделаны ссылки	541
3.	Принципы работы интерфейса ИТС	542
3.1	Технология связи	542
3.2	Доступные функции	542
3.3	Доступ через интерфейс ИТС	543
3.4	Доступные данные и необходимость согласия водителя	545
4.	Перечень данных, доступных через интерфейс ИТС, и классификация личных/ неличных данных	545
Подраздел 14	Функция удаленной связи	581
1.	Введение	583
2.	Область применения	584
3.	Акронимы, определения и обозначения	585
4.	Эксплуатационные сценарии	587
4.1	Обзор	587
4.2	Безопасность/целостность	590
5.	Конструктивные характеристики и протоколы системы удаленной связи	591
5.1	Конструктивные характеристики	591
5.2	Рабочий процесс.....	594
5.3	Параметры физического интерфейса DSRC удаленной связи	596
5.4	Требования, предусмотренные протоколом DSRC к RTM	601
5.5	Зарезервировано для использования в будущем	627
5.6	Передача данных между DSRC_VU и БУ	627
5.7	Обработка ошибок	629
6.	Испытания при вводе в эксплуатацию и периодических проверках функции удаленной связи	631
6.1	Общие положения	631
6.2	ЕСНО	631
6.3	Испытания на подтверждение защищенности содержания данных	632
Подраздел 15	Переход на новые версии: управление системой параллельного использования оборудования разных поколений	640
1.	Определения	641
2.	Общие положения	641
2.1	Обзор проблемы перехода	641
2.2	Эксплуатационная совместимость между БУ и карточками	641

2.3	Эксплуатационная совместимость между БУ и датчиком движения	642
2.4	Эксплуатационная совместимость между бортовыми устройствами, карточками тахографа и оборудованием для загрузки данных	642
2.5	Эксплуатационная совместимость между БУ и калибровочным оборудованием	643
3.	Основные этапы в течение периода до даты ввода в эксплуатацию	644
4.	Нормативные положения на период после даты ввода в эксплуатацию	644
Подраздел 16	Адаптер для транспортных средств категорий M1 и N1	645
1.	Сокращения и справочные документы	646
1.1	Сокращения	646
1.2	Справочные стандарты	646
2.	Общие характеристики и функции адаптера	646
2.1	Общее описание адаптера	646
2.2	Функции	646
2.3	Безопасность	646
3.	Требования к контрольному устройству в случае установки адаптера	647
4.	Требования к конструкции и функциям адаптера	647
4.1	Обеспечение сопряжения и адаптация входящих импульсов скорости	647
4.2	Индукцирование поступающих импульсов на встроенный датчик движения	648
4.3	Встроенный датчик движения	648
4.4	Требования безопасности	648
4.5	Эксплуатационные характеристики	648
4.6	Материалы	649
4.7	Маркировка	649
5.	Требования к контрольному устройству в случае установки адаптера	649
5.1	Установка	649
5.2	Наложение пломб	650
6.	Проверка, инспекция и ремонт	650
6.1	Периодические инспекции	650
7.	Требования к контрольному устройству в случае использования адаптера	650
7.1	Общие положения	650
7.2	Сертификат функциональности	651

Введение

Система цифровых тахографов первого поколения уже внедрена с 1 мая 2006 года на территории Договаривающихся сторон. Она может использоваться до окончания срока их службы для внутренних перевозок. В области международных перевозок в течение 15 лет с момента вступления в силу настоящих правил Комиссии все транспортные средства должны быть оборудованы соответствующим требованиям, предъявляемым к «умным» тахографом, как предусмотрено в настоящих Правилах.

Система тахографов первого поколения соответствует добавлению 1В к настоящему Соглашению, а система тахографов второго поколения, известная также под названием «система смарт-тахографов», соответствует настоящему подразделу указанного добавления. В этом приложении добавлению содержатся требования к записывающему оборудованию контрольному устройству и карточкам тахографов второго поколения.

Начиная с даты ввода в эксплуатацию версии 2 записывающего оборудования контрольных устройств второго поколения она устанавливается на транспортных средствах, эксплуатируемых в соответствии с настоящим Соглашением регистрируемых впервые, и предусматривает выдачу карточек выдается карточки версии 2 тахографов второго поколения. В целях содействия беспрепятственному вводу в эксплуатацию системы тахографов второго поколения:

- карточки версии 2 тахографов второго поколения выполняются таким образом, чтобы их можно было также использовать в версии 1 бортовых устройств первого и второго поколений,
- замена действующих карточек тахографов первого поколения и версии 1 второго поколения на дату ввода в действие новой системы не требуется.

Это позволит водителям сохранить только одну карточку водителя и пользоваться ею в обеих системах.

Однако записывающее оборудование контрольное устройство второго поколения калибруется только с карточками мастерской второго поколения.

В настоящем приложении добавлении изложены все требования, связанные с эксплуатационной совместимостью систем тахографов первого и второго поколений.

Добавление Подраздел 15 содержит дополнительные детальные данные относительно того, каким образом должно обеспечиваться параллельное использование этих двух поколений систем, включая различные версии второго поколения.

Список приложений подразделов

Подраздел 1:	СЛОВАРЬ ДАННЫХ
Подраздел 2:	СПЕЦИФИКАЦИЯ НА КАРТОЧКИ ТАХОГРАФОВ
Подраздел 3:	ПИКТОГРАММЫ
Подраздел 4:	РАСПЕЧАТКИ
Подраздел 5:	ДИСПЛЕЙ
Подраздел 6:	ПЕРЕДНИЙ СОЕДИНИТЕЛЬ ДЛЯ КАЛИБРОВКИ И ЗАГРУЗКИ
Подраздел 7:	ПРОТОКОЛЫ ЗАГРУЗКИ ДАННЫХ
Подраздел 8:	ПРОТОКОЛ КАЛИБРОВКИ
Подраздел 9:	ОФИЦИАЛЬНОЕ УТВЕРЖДЕНИЕ ТИПА И МИНИМАЛЬНЫЙ ПЕРЕЧЕНЬ ТРЕБУЕМЫХ ИСПЫТАНИЙ
Подраздел 10:	ТРЕБОВАНИЯ В ОБЛАСТИ БЕЗОПАСНОСТИ
Подраздел 11:	ОБЩИЕ МЕХАНИЗМЫ ЗАЩИТЫ

- Подраздел 12: ОПРЕДЕЛЕНИЕ МЕСТОПОЛОЖЕНИЯ ПРИ ПОМОЩИ ГЛОБАЛЬНОЙ НАВИГАЦИОННОЙ СПУТНИКОВОЙ СИСТЕМЫ (ГНСС)
- Подраздел 13: ИНТЕРФЕЙС ИТС
- Подраздел 14: ФУНКЦИЯ УДАЛЕННОЙ СВЯЗИ
- Подраздел 15: ПЕРЕХОД НА НОВЫЕ ВЕРСИИ: УПРАВЛЕНИЕ СИСТЕМОЙ ПАРАЛЛЕЛЬНОГО ИСПОЛЬЗОВАНИЯ ОБОРУДОВАНИЯ РАЗНЫХ ПОКОЛЕНИЙ
- Подраздел 16: АДАПТЕР ДЛЯ ТРАНСПОРТНЫХ СРЕДСТВ КАТЕГОРИЙ M1 И N1

1. Определения

В данном ~~приложении~~ **добавлении**:

a) «активация» означает:

этап, в ходе которого тахограф полностью вводится в эксплуатацию и выполняет все функции, включая функции безопасности, с помощью карточки мастерской;

b) «аутентификация» означает:

функция, предназначенная для установления и удостоверения идентичности заявленного субъекта;

c) «аутентичность» означает:

признак, указывающий на то, что информация поступает от субъекта, идентичность которого можно проверить;

d) «встроенная система проверки (ВСП)» означает:

проверки по требованию, осуществляемые оператором или внешним устройством;

e) «календарный день» означает:

сутки с 00:00 часов до 24:00 часов. Все календарные дни определяются по системе всемирного координированного времени (UTC);

f) калибровка смарт-тахографа означает:

обновление или подтверждение параметров транспортного средства, которые должны храниться в блоке памяти. Параметры транспортного средства включают идентификационные данные транспортного средства (VIN, VRN и ~~государство-член Договаривающаяся сторона~~ регистрации) и характеристики транспортного средства (w, k, l, размер шин, параметры регулировки устройства ограничения скорости (в случае применимости), текущее время UTC, текущие показания счетчика пробега, **тип груза по умолчанию**); в процессе калибровки ~~записывающего оборудования контрольного устройства~~ в память данных должны также загружаться данные о типах и идентификаторах всех наложенных пломб, имеющих отношение к официальному утверждению типа;

любое обновление или подтверждение времени UTC считается уточнением времени, а не калибровкой, при условии что это не противоречит требованию 409;

калибровка ~~записывающего оборудования контрольного устройства~~ предполагает необходимость использования карточки мастерской;

g) «номер карточки» означает:

номер в виде 16 буквенно-цифровых знаков, который однозначно идентифицирует карточку тахографа в ~~соответствующем государстве-члене соответствующей Договаривающейся стороне~~. Номер карточки включает соответствующую **идентификацию, которая состоит из идентификации водителя или идентификации владельца карточки вместе с** соответствующим порядковым индексом карточки (~~если применимо~~), индексом замены карточки и индексом возобновления карточки;

таким образом, карточка однозначно идентифицируется с помощью кода ~~выданного ее государством-членом~~ **выдавшей ее Договаривающейся стороны** и номера карточки;

h) «порядковый индекс карточки» означает:

14-й буквенно-цифровой знак номера карточки, который позволяет дифференцировать различные карточки, выданные соответствующему предприятию, мастерской или контролирующему органу, которые имеют право на получение

нескольких карточек тахографа. Данное предприятие, мастерская или контролирующий орган однозначно идентифицируются с помощью первых 13 знаков номера карточки;

i) «индекс возобновления карточки» означает:

16-й буквенно-цифровой знак номера карточки, который увеличивается при каждом обновлении карточки тахографа, **соответствующей данной идентификации, т. е. идентификации водителя или идентификации владельца вместе с порядковым индексом;**

j) «индекс замены карточки» означает:

15-й буквенно-цифровой знак номера карточки, который увеличивается при каждой замене карточки тахографа, **соответствующей данной идентификации, т. е. идентификации водителя или идентификации владельца вместе с порядковым индексом;**

к) «характеристический коэффициент транспортного средства» означает:

числовая характеристика, придающая соответствующее значение выходному сигналу, подаваемому компонентом транспортного средства, связывающим его с ~~записывающим оборудованием~~ **контрольным устройством** (ведущий вал коробки передач или ведущая ось) после пробега транспортным средством расстояния 1 км в стандартных условиях испытания в соответствии с требованием 414. Характеристический коэффициент выражается в импульсах на километр ($w = \dots$ имп./км);

l) «карточка предприятия» означает:

карточка тахографа, выданная органами ~~государства-члена Договаривающейся стороны~~ транспортному предприятию, эксплуатирующему транспортные средства, оснащенные соответствующим тахографом, в которой указано транспортное предприятие и которая позволяет отображать, загружать и печатать хранимые в тахографе данные, заблокированные данным транспортным предприятием;

m) «постоянная величина ~~записывающего оборудования~~ **контрольного устройства**» означает:

числовая характеристика, придающая соответствующее значение входному сигналу, который необходим для просмотра и регистрации расстояния пробега в 1 км; эта постоянная выражается в импульсах на километр ($k = \dots$ имп/км);

n) «непрерывное время управления» рассчитывается ~~записывающим оборудованием~~ **контрольным устройством** следующим образом¹:

непрерывное время управления рассчитывают как текущее накопленное время управления конкретного водителя с момента окончания последнего периода его «ДОСТУПНОСТИ» или «ПЕРЕРЫВА/ОТДЫХА» или периода «НЕИЗВЕСТНО»² продолжительностью 45 минут или более (в соответствии с ~~Регламентом (ЕС) № 561/2006~~ **настоящим Соглашением** этот период можно делить на части). Результаты соответствующих расчетов производят при необходимости с учетом данных о последних видах занятости, хранящихся на карточке водителя. Если водитель не

¹ Этот способ расчета непрерывной продолжительности времени управления и совокупной продолжительности времени перерывов используется ~~записывающим оборудованием~~ **контрольным устройством** для расчета времени подачи предупредительного сигнала, указывающего на непрерывное время управления. Он не предопределяет правовое толкование этих периодов времени. Альтернативный способ расчета продолжительности управления и совокупной продолжительности времени перерывов может использоваться для замены этих определений, если они утратили актуальность в силу обновления других соответствующих законодательных актов.

² Периоды UNKNOWN соответствуют периодам, в течение которых карточка водителя не была введена в ~~записывающее оборудование~~ **контрольное устройство** и в случае которых никакие данные о занятости водителя не были введены вручную.

вставил карточку, расчет производится на основе данных, записанных в блоке памяти и относящихся к периоду, в течение которого карточка вставлена не была, и к соответствующему считывающему устройству;

о) «карточка контролера» означает:

карточка тахографа, выданная органами ~~государства-члена Договаривающейся стороны~~ национальному компетентному контролирующему органу, который назначает соответствующий контрольный орган и при необходимости сотрудника, ответственного за проведение контроля, и предоставляет доступ к данным, хранящимся в блоке памяти или на карточках водителя, а также при необходимости на карточках мастерских для их считывания, распечатки и/или загрузки;

он также обеспечивает доступ к функции проверки калибровки на дорогах и к данным устройства, считывающего показания средства удаленной связи раннего обнаружения;

р) «накопленная продолжительность перерывов» рассчитывается ~~занимающим оборудованием~~ **контрольным устройством следующим образом**¹:

накопленная продолжительность перерывов в процессе управления рассчитывается как текущее суммарное время ДОСТУПНОСТИ или ПЕРЕРЫВА/ОТДЫХА или периода НЕИЗВЕСТНО² продолжительностью 15 минут или более конкретного водителя с момента завершения последнего периода его ДОСТУПНОСТИ, ПЕРЕРЫВА/ОТДЫХА или периода НЕИЗВЕСТНО² продолжительностью 45 минут или более (в соответствии с ~~Регламентом (ЕК) № 561/2006~~ **настоящим Соглашением** этот период можно делить на части);

результаты соответствующих расчетов производят при необходимости с учетом данных о последних видах занятости, хранящихся на карточке водителя. Неизвестные периоды отрицательной продолжительности (момент начала одного неизвестного периода перекрывает момент завершения другого неизвестного периода), что обусловлено накладками по времени в данных между двумя различными видами ~~занимающего оборудования~~ **контрольных устройств**, в расчет не принимаются;

если водитель не вставил карточку, расчет производится на основе данных, записанных в блоке памяти и относящихся к периоду, в течение которого карточка вставлена не была, и к соответствующему считывающему устройству;

q) «блок памяти» означает:

электронное устройство хранения данных, встроенное в ~~занимающее оборудование~~ **контрольное устройство**;

r) «цифровая подпись» означает:

данные, прилагаемые к массиву данных, или соответствующее криптографическое преобразование этого массива, которые позволяют субъекту, получившему доступ к этому массиву данных, подтвердить его аутентичность и целостность;

s) «загрузка» означает:

копирование вместе с цифровой подписью части или всего массива файлов данных, хранящихся в блоке памяти бортового устройства или в памяти карточки тахографа, при условии, что этот процесс не приводит к изменению или удалению каких бы то ни было хранящихся данных;

изготовители бортовых устройств, оснащенных смарт-тахографами, и изготовители оборудования для загрузки файлов данных предпринимают все разумные меры с целью обеспечить такое положение, при котором загрузка таких данных осуществлялась бы транспортными предприятиями или водителями с минимальной задержкой;

для установления соответствия ~~Регламенту (ЕС) № 561/2006~~ **настоящему Соглашению** загрузка подробного файла с данными скорости может не

потребоваться, однако она может понадобиться для других целей, например для расследования дорожно-транспортных происшествий;

t) «карточка водителя» означает:

карточка тахографа, выданная органами государства-члена Договаривающейся стороны конкретному водителю, с помощью которой устанавливается личность водителя и которая позволяет хранить данные о его деятельности;

u) «эффективная окружность колес» означает:

среднее значение расстояний, пройденных каждым из колес, приводящих в движение транспортное средство (ведущими колесами) за один полный оборот. Эти расстояния измеряются в стандартных условиях испытания в соответствии с требованием 414 и выражаются в виде « $l = \dots$ мм». Изготовители транспортных средств могут использовать вместо фактического измерения этого расстояния теоретический метод расчета, который учитывает распределение веса на оси транспортного средства в снаряженном состоянии без груза³, а именно с охлаждающей жидкостью, смазочными материалами, топливом, инструментами, запасным колесом и водителем. Методы такого теоретического расчета подлежат утверждению компетентным органом государства-члена Договаривающейся стороны и могут применяться только до активации тахографа;

v) «событие» означает:

сбой в работе, обнаруженный смарт-тахографом, который может быть обусловлен попыткой подлога;

w) «внешнее устройство» ГНСС означает:

устройство, состоящее из приемника ГНСС, когда бортовое устройство не является единым блоком, и других компонентов, необходимых для защиты передачи данных о местоположении в остальные элементы бортового устройства;

x) «неисправность» означает:

сбой в работе, обнаруженный смарт-тахографом, который может быть вызван отказом или неисправностью оборудования;

y) приемник ГНСС означает:

электронное устройство, принимающее сигналы одной или нескольких глобальных навигационных спутниковых систем (ГНСС) и производящее их цифровую обработку с целью предоставить информацию о местоположении, скорости и времени.

z) «установка» означает:

монтаж тахографа на транспортном средстве;

aa) «эксплуатационная совместимость» означает:

способность систем и основных деловых процессов обмениваться данными и делиться информацией;

bb) «интерфейс» означает:

средство, обеспечивающее возможность связи и взаимодействия между системами;

³ Регламент (ЕС) № 1230/2012 о массах и габаритах определенных категорий моторных транспортных средств и прицепов, вносящий поправки в Директиву 2007/46/ЕС, с последними поправками.

cc) «местоположение» означает:

географические координаты транспортного средства в конкретный момент времени;

dd) «датчик движения» означает:

компонент тахографа, подающий сигнал, который отображает скорость транспортного средства и/или пройденное расстояние;

ee) «недействительная карточка» означает:

карточка, которая оказалась неисправной или которую не удалось идентифицировать, или срок действия которой еще не наступил, или срок действия которой уже истек;

карточка, которая также считается недействительной бортовым устройством транспортного средства:

– **если в бортовое устройство уже вставлена карточка, выданная той же Договаривающейся стороной, с той же идентификацией, т. е. идентификацией водителя или идентификацией держателя, вместе с порядковым индексом и более высоким индексом возобновления, или**

– **если в бортовое устройство уже вставлена карточка, выданная той же Договаривающейся стороной, с той же идентификацией, т. е. идентификацией водителя или идентификацией держателя, вместе с порядковым индексом и индексом возобновления, но с более высоким индексом замены;**

ff) «открытый стандарт» означает:

стандарт, указанный в соответствующем документе по спецификации стандартов, находящемся в свободном доступе или доступном за символическую плату, который можно копировать, распространять или использовать бесплатно или за символическую плату.

gg) «неприменимо» означает:

случай, когда использование ~~записывающего~~ **оборудования контрольного устройства** в соответствии с положениями ~~Регламента (ЕС) № 561/2006~~ **настоящего Соглашения** не требуется.

hh) «превышение скорости» означает:

превышение допустимой скорости транспортного средства, определяемое как любой отрезок времени продолжительностью более 60 секунд, в течение которого измеренная скорость транспортного средства превышает предел, установленный для устройства ограничения скорости в соответствии с ~~Директивой Совета 92/6/ЕЭС от 10 февраля 1992 г. об установке и эксплуатации устройств ограничения скорости для определенных категорий моторных транспортных средств в Сообществе⁴, с последними поправками; Правилами № 89 ЕЭК ООН;~~

ii) «периодическая проверка» означает:

ряд действий, производимых с целью убедиться в надлежащей работе тахографа, соответствии его регулировки параметрам транспортного средства и отсутствии средств манипулирования, пристроенных к тахографу;

jj) «принтер» означает:

компонент ~~записывающего~~ **оборудования контрольного устройства**, который позволяет распечатывать хранящиеся данные;

kk) «удаленная связь раннего обнаружения» означает:

связь между средством удаленной связи раннего обнаружения и считывающим устройством удаленной связи раннего обнаружения во время целевых проверок на

⁴ OJ No. L057, 02/03/1992, p 0027-0028.

дорогах в порядке удаленного обнаружения возможного манипулирования или неправомерного использования ~~записывающего~~ ~~оборудования~~ **контрольного устройства**;

ll) «**средство удаленной связи**», «**модуль удаленной связи**» или «**средство удаленного раннего обнаружения**» означает:

оборудование бортового устройства транспортного средства, используемое для проведения целевых проверок на дорогах;

mm) «**считывающее устройство удаленной связи раннего обнаружения**» означает:

система, используемая сотрудниками контроля для целевых проверок на дорогах.

nn) «**возобновление карточки**» означает:

выдача новой карточки тахографа в том случае, когда срок действия используемой карточки подходит к концу или когда она начинает работать со сбоями и возвращается выдавшему ее органу. ~~Возобновление всегда однозначно указывает на то, что две действительные карточки одновременно использоваться не могут;~~

oo) «ремонт» означает:

любой ремонт датчика движения или бортового устройства транспортного средства или кабеля, который предполагает необходимость его отсоединения от источника питания или от любого другого компонента тахографа, или вскрытие датчика движения или бортового устройства;

pp) «замена карточки» означает:

выдача **новой** карточки тахографа в порядке замены существующей карточки, которая, на основании полученного заявления, была утрачена, похищена или дала сбой в работе и не была возвращена выдавшему ее органу. ~~Возобновление всегда однозначно указывает на то, что две действительные карточки одновременно использоваться не могут;~~

qq) «сертификация безопасности» означает:

процедура, осуществляемая органом сертификации по общим критериям в порядке удостоверения того, что ~~записывающее~~ ~~оборудование~~ **контрольное устройство** (или компонент) или карточка тахографа, в отношении которых проводится расследование, отвечает требованиям безопасности, установленным в соответствующих схемах защиты;

rr) «самопроверка» означает:

проверки, осуществляемые на цикличной основе и в автоматическом режиме ~~записывающим оборудованием~~ **контрольным устройством** на предмет обнаружения неисправностей;

ss) «замер времени» означает:

постоянная цифровая регистрация значений универсального скоординированного времени и даты (UTC);

tt) «корректировка времени» означает:

~~автоматическая~~ корректировка текущего времени; **эта корректировка может быть автоматической через регулярные интервалы времени с использованием данных о времени, выдаваемых приемником GNSS в качестве е-максимальным допуском в одну минуту, исходных значений, или регулировкой, выполняемой выполняться в режиме калибровки;**

iii) «размер шин» означает:

указание размеров шин (внешних ведущих колес) в соответствии с ~~Директивой 92/23/ЕЭС от 31 марта 1992 года⁵, с последними поправками;~~ **Правилами ЕЭК ООН № 54;**

iv) «идентификация транспортного средства» означает:

номера, идентифицирующие транспортное средство: номер регистрации транспортного средства (VRN) с указанием ~~государства-члена~~ **Договаривающейся стороны** регистрации и опознавательный номер транспортного средства (VIN);

v) в целях расчетов в ~~записывающем оборудовании~~ **контрольном устройстве** — «неделя» означает:

период с 00:00 часов UTC в понедельник до 24:00 часов UTC в воскресенье;

vi) «карточка мастерской» означает:

карточка тахографа, выданная органами ~~государства-члена~~ **Договаривающейся стороны** назначенным сотрудникам изготовителя тахографов, специалисту по монтажу, изготовителю транспортных средств или мастерской, утвержденных ~~данним государством-членом~~ **данной Договаривающейся стороной**, по которой устанавливается личность держателя карточки и которая позволяет проводить испытания, калибровку и активацию тахографов и/или извлекать из них данные;

vii) «адаптер» означает:

устройство, передающее сигнал, постоянно отображающий скорость транспортного средства и/или пройденное расстояние, кроме сигнала, используемого для обнаружения независимого движения, и которое:

- устанавливается и используется только на транспортных средствах типа M1 и N1 (как они определены в ~~приложении II к Директиве Совета 2007/46/ЕС, с последними поправками~~), введенных в эксплуатацию ~~с 1 мая 2006 года~~ **Сводной резолюции о конструкции транспортных средств (CP.3), Пересмотр 6, ECE/TRANS/WP.29/78/Rev.6 от 11 июля 2017 года**);
- устанавливается там, где механически невозможно установить никакой другой датчик движения, который в остальном соответствует положениям настоящего ~~дополнения~~ **дополнения** и его **подразделов 1–15**;
- устанавливается между бортовым устройством и встроенными датчиками или альтернативными интерфейсами, в которых генерируются импульсы скорости/расстояния;
- если смотреть со стороны бортового устройства, то адаптер ведет себя таким же образом, как если бы к бортовому устройству был подключен датчик движения в соответствии с положениями настоящего ~~дополнения~~ **дополнения** и его **подразделов 1–16**;
- использование такого адаптера в описанных выше транспортных средствах дает возможность устанавливать и правильно эксплуатировать бортовое устройство в соответствии со всеми требованиями настоящего ~~дополнения~~ **дополнения**; в таких транспортных средствах в состав смарт-тахографа входят кабели, адаптер и бортовое устройство;

⁵ OJ No L 129, 14/05/1992, p. 0095.

zz) «целостность данных» означает:

точность и последовательность хранящихся данных, что выражается в отсутствии любых изменений данных между двумя обновлениями записи;

целостность предполагает, что данные являются точной копией первоначальной версии, т. е. что в процессе записи и считывания на карточке тахографа или в специальном оборудовании или во время передачи по любым каналам связи данные не нарушаются;

~~aaa) — конфиденциальность данных:~~

~~общие — технические — меры — обеспечения — соответствующего — применения принципов, изложенных в Директиве 95/46/ЕС от 24 октября 1995 г. о защите лиц при обработке личных данных и о свободном движении таких данных, а также данных, указанных в Директиве 2002/58/ЕС Европейского парламента и Совета от 12 июля 2002 г. об обработке личных данных и защите конфиденциальности в секторе электронных коммуникаций;~~

aaa) зарезервирован

bbb) «система смарт-тахографа» означает:

~~записывающее устройство~~ **контрольное устройство**, карточки тахографа и набор всех прямо или косвенно взаимодействующих устройств в процессе их конструирования, установки, эксплуатации, тестирования и контроля, таких как карточки, считывающее устройство удаленной связи и любое другое оборудование для загрузки и анализа данных, калибровки, генерирования, контроля или включения соответствующих элементов безопасности и т. д.;

«Смарт-тахографы» являются контрольными устройствами, соответствующими добавлению 1С к настоящему Соглашению

ccc) «дата ввода в эксплуатацию» означает:

~~еее) — 36 месяцев с момента вступления в силу подробных положений, указанных в статье 11 Регламента (ЕС) № 165/2014.~~

это дата, после которой транспортные средства, зарегистрированные впервые, **должны быть оснащены тахографом в соответствии с настоящим Соглашением;**

~~снабжаются тахографом, соединенным с сервисом установления местоположения на основе спутниковой навигационной системы;~~

~~могут передавать данные для целевых проверок на дорогах компетентным контролирующим органам во время движения транспортного средства;~~

~~и могут быть оснащены стандартными интерфейсами, позволяющими использовать данные, записанные или произведенные тахографами, в оперативном режиме на внешних устройствах;~~

ddd) «схема защиты» означает:

документ, используемый в рамках процедуры сертификации в соответствии с общими критериями и представляющий собой спецификацию требований в области обеспечения информационной безопасности, независимой от реализации на практике;

eee) «точность ГНСС» означает:

в контексте регистрации местоположения по Глобальной навигационной спутниковой системе (ГНСС) с помощью тахографов это означает показатель снижения точности при определении положения в горизонтальной плоскости (HDOP), рассчитываемый в качестве минимума значений HDOP, собранных из имеющихся ГНСС;

fff) «накопленное время управления» означает:

значение, представляющее собой общее накопленное количество минут управления конкретным транспортным средством;

значение накопленного времени управления представляет собой результат подсчета всех минут в режиме свободного хода, учитываемых функцией мониторинга контрольного устройства в качестве УПРАВЛЕНИЯ, и используется только для инициирования регистрации положения транспортного средства каждый раз, когда достигается значение, кратное трем часам накопленного времени управления. Накопление начинается в момент активации устройства управления. На него не влияют никакие другие условия, например выход за пределы условия «неприменимо» или переезд на пароме/поезде. Отображение, распечатка или загрузка данных о накопленном времени управления не предусмотрены;

ggg) «масса порожнего транспортного средства в снаряженном состоянии» означает:

a) в случае автомобиля:

масса транспортного средства с топливным(и) баком(ами), заполненным(и) не менее чем на 90 % его (их) емкости, включая массу водителя, топлива и жидкостей, оснащенного стандартным оборудованием в соответствии с техническими условиями изготовителя, и в тех случаях, когда они установлены, массу кузова, кабины, сцепного устройства и запасного(ых) колеса (колес), а также инструментов;

b) в случае прицепа:

масса транспортного средства, включая топливо и жидкости, оснащенного стандартным оборудованием в соответствии с техническими условиями изготовителя, и в тех случаях, когда они установлены, масса кузова, дополнительной сцепки (сцепных устройств), запасного колеса (колес) и инструментов;

hhh) «идентификационный номер транспортного средства» означает:

фиксированная комбинация знаков, присваиваемая изготовителем каждому транспортному средству, которая состоит из двух частей: первая, состоящая не более чем из шести знаков (букв или цифр), идентифицирующих общие характеристики транспортного средства, в частности тип и модель; вторая, состоящая из восьми знаков, первые четыре из которых могут быть буквами или цифрами, а остальные четыре только цифрами, обеспечивающими, в сочетании с первой частью, четкую идентификацию конкретного транспортного средства.

2. Общие характеристики и функции записывающего оборудования контрольного устройства

2.1 Общие характеристики

Цель ~~записывающего—оборудования~~ **контрольного устройства** состоит в регистрации, хранении, отображении, распечатке и отображении данных о занятости водителя.

Любое транспортное средство, оснащенное ~~записывающим—оборудованием~~ **контрольным устройством**, удовлетворяющим положениям настоящего ~~приложения~~ **добавления**, должно быть оборудовано спидометром и счетчиком пробега. Эти функции могут быть встроены в ~~записывающее—оборудование~~ **контрольное устройство**.

- 1) ~~Записывающее—оборудование~~ **Контрольное устройство** включает в себя электропроводку, датчик движения и бортовое устройство транспортного средства.
- 2) Интерфейс между датчиками движения и бортовыми устройствами должен соответствовать требованиям, указанным в ~~приложении~~ **подразделе 11**.

- 3) Бортовое устройство подсоединяется к глобальной навигационной спутниковой системе (или системам), как указано в ~~приложении~~ **подразделе 12**.
- 4) Бортовое устройство поддерживает связь со считывающими устройствами удаленной связи раннего обнаружения, как указано в ~~приложении~~ **подразделе 14**.
- 5) Бортовое устройство ~~может включать~~ **включает** в себя интерфейс ИТС, как указано в ~~приложении~~ **подразделе 13**. ~~Записывающее оборудование~~ **Контрольное устройство** может быть подключено к другим устройствам через дополнительные интерфейсы и/или ~~факультативный~~ интерфейс ИТС.
- 6) Любое включение или подсоединение к ~~записывающему оборудованию~~ **контрольному устройству** любой функции, устройства или устройств, сертифицированных или иных, не должно оказывать воздействия или создавать помехи, которые могут нарушить надлежащую и безопасную работу ~~записывающего оборудования~~ **контрольного устройства** и привести к нарушению положений настоящего ~~Регламента~~ **Соглашения**. Пользователи ~~записывающего оборудования~~ **контрольного устройства** вводят свои идентификационные данные в устройство с помощью карточек тахографа.
- 7) ~~Записывающее оборудование~~ **Контрольное устройство** дает право селективного доступа к данным и функциям в зависимости от вида и/или идентификационных данных пользователя. ~~Записывающее оборудование~~ **Контрольное устройство** регистрирует и хранит данные в блоке памяти, в устройстве удаленной связи и на карточках тахографа.

~~Это делается в соответствии с Директивой 95/46/ЕС от 24 октября 1995 года защите лиц при обработке личных данных и о свободном движении таких данных⁶; Директивой 2002/58/ЕС от 12 июля 2002 г. об обработке личных данных и защите конфиденциальности в секторе электронных коммуникаций⁷ и статьей 7 Регламента (ЕС) № 165/2014.~~

2.2 Функции

- 8) ~~Записывающее оборудование~~ **Контрольное устройство** выполняет следующие функции:
- контроль за вводом и извлечением карточек;
 - замеры скорости, расстояния и местоположения;
 - замер времени;
 - контроль за работой водителя;
 - контроль за статусом управления;
 - ручной ввод данных водителем:
 - ввод данных о местах, в которых начинаются и/или заканчиваются ежедневные периоды работы;
 - ручной ввод данных о занятости водителя и **согласии водителя на использование интерфейса ИТС**;
 - ввод данных об особых условиях;
 - **ввод операций по загрузке или разгрузке**;
 - управление системой блокировки, установленной предприятием;
 - мониторинг работы системы контроля;
 - выявление соответствующих событий и/или неисправностей;

⁶ OJ № L 281, 23/11/1995, с.31.

⁷ OJ № L 201, 31/07/2002, p.37.

- встроенные системы проверки и самопроверки;
- считывание данных из блока памяти;
- регистрация и хранение данных в блоке памяти;
- считывание данных с карточек тахографа;
- регистрация и хранение данных на карточках тахографа;
- вывод на дисплей;
- вывод на печать;
- предупреждение;
- загрузка данных на внешние носители;
- удаленная связь для целевых проверок на дорогах;
- вывод данных на дополнительные устройства;
- калибровка;
- проверки калибровки на дорогах;
- корректировка времени;
- **мониторинг пересечения границ;**
- **обновление программного обеспечения.**

2.3 Режимы работы

9) ~~Записывающее оборудование~~ **Контрольное устройство** работает в четырех режимах:

- рабочий режим;
- режим контроля;
- режим калибровки;
- режим предприятия.

10) ~~Записывающее оборудование~~ **Контрольное устройство** переходит в следующий режим работы в зависимости от действующих карточек тахографа, вставленных в разъем ввода карточек в блок интерфейса. Для определения режима работы поколение карточки тахографа значения не имеет, при условии, что введенная карточка действительна. Карточка мастерской первого поколения при вводе в бортовое устройство второго поколения считается недействительной во всех случаях.

Режим работы		Считывающее устройство водителя				
		Карточка не вставлена	Карточка водителя	Карточка контролера	Карточка мастерской	Карточка предприятия
Считывающее устройство второго водителя	Карточка не вставлена	Действует	Действует	Контроль	Калибровка	Предприятие
	Карточка водителя	Действует	Действует	Контроль	Калибровка	Предприятие
	Карточка контролера	Контроль	Контроль	Контроль(*)	Действует	Действует
	Карточка мастерской	Калибровка	Калибровка	Действует	Калибровка(*)	Действует
	Карточка предприятия	Предприятие	Предприятие	Действует	Действует	Предприятие(*)

(*) В этих случаях ~~записывающее оборудование~~ **контрольное устройство** использует только карточку тахографа, введенную в считывающее устройство водителя.

11) ~~Занимающееся оборудование~~ **Контрольное устройство** игнорирует вставленные недействительные карточки, за исключением случаев вывода на дисплей, вывода на печать или загрузки данных, хранящихся на карточке с истекшим сроком действия, которые должны быть возможны.

12) Все функции, перечисленные в пункте θ 2.2, работают в любом режиме за исключением следующих случаев:

- функция калибровки доступна только в режиме калибровки;
- функция проверки калибровки на дорогах доступна только в режиме контроля;
- функция реагирования на блокировку, установленную предприятием, доступна только в режиме предприятия;
- функция мониторинга контроля доступна только в режиме контроля;
- функция загрузки данных в рабочем режиме недоступна за исключением случая;
 - предусмотренного требованием 193;
 - ~~и за исключением~~ загрузки данных с карточки водителя, когда в считывающем устройстве БУ карточки другого типа нет.

13) ~~Занимающееся оборудование~~ **Контрольное устройство** может выводить любые данные на дисплей, принтер или внешние интерфейсы, за исключением следующих случаев:

- в рабочем режиме любые личные данные (фамилия и имя (имена), не соответствующие данным на вставленной карточке тахографа, меняются на пробелы, а любой номер карточки, не соответствующий данным на вставленной карточке тахографа, меняются на пробелы частично (в этом случае на пробелы меняется каждый нечетный знак слева направо);
- в режиме предприятия данные, касающиеся водителя (требования 102, 105 ~~и~~ 108, **133а и 133е**), могут быть извлечены только за периоды, когда блокировка отсутствует или блокировка не доверена другому предприятию (что идентифицируется по первым 13 цифрам номера карточки предприятия);
- когда в ~~занимающееся оборудование~~ **контрольное устройство** карточка не вставлена, данные, касающиеся водителя, могут извлекаться только за текущий и восемь предыдущих календарных дней;
- личные данные, **зарегистрированные и сгенерированные либо тахографом, либо карточками тахографа, бортовым устройством** выводятся через интерфейс ИТС бортового устройства только после проверки согласия водителя, к которому относятся эти данные;
- срок службы бортовых устройств в нормальных условиях эксплуатации оставляет 15 лет с **фактической** даты ~~выдачи~~, указанной в сертификате на бортовое устройство, но в целом бортовые устройства можно использовать еще 3 месяца, но только для загрузки данных.

2.4 Безопасность

Система безопасности имеет целью предохранить блок памяти от несанкционированного доступа к зарегистрированным данным и их манипуляции и регистрировать любые случаи таких попыток, сохранить целостность и аутентичность данных, передаваемых между датчиком движения и бортовым устройством, сохранить целостность и аутентичность данных, передаваемых между ~~занимающим оборудованием~~ **контрольным устройством** и карточками тахографа, сохранить

целостность и аутентичность данных, передаваемых между ~~записывающим оборудованием~~ **контрольным устройством** и внешним устройством ГНСС, **в случае его наличия**, сохранить конфиденциальность, целостность и аутентичность данных, передаваемых через систему удаленной связи раннего обнаружения в целях контроля и проверки целостности и аутентичности загружаемых данных.

14) В целях обеспечения безопасности системы следующие компоненты должны соответствовать требованиям безопасности, указанным в схемах защиты, предусмотренных ~~ее~~ ~~согласно приложению~~ в **подразделе 10**:

- бортовое устройство;
- карточка тахографа;
- датчик движения;
- внешнее устройство ГНСС (данная схема необходима и применима только в случае внешнего варианта **устройства ГНСС**).

3. Требования к конструкции и функциям ~~записывающего~~ **оборудования контрольного устройства**

3.1 Контроль за карточками ~~вводом~~ и их извлечением ~~карточек~~

15) ~~Записывающее оборудование~~ **Контрольное устройство** отслеживает работу интерфейса для считывания карточек в целях регистрации фактов ввода и извлечения карточки.

16) При вводе карточки (**или удаленной аутентификации карточки**) ~~записывающее оборудование~~ **контрольное устройство** устанавливает, является ли вставленная карточка действительной карточкой тахографа **в соответствии с определением (ее) в разделе 1**, и в таком случае идентифицирует тип и поколение этой карточки.

~~Если карточка с таким же номером карточки и более высоким индексом возобновления уже была введена в записывающее оборудование, карточка признается недействительной. Если карточка с таким же номером карточки и более высоким индексом замены уже была введена в записывающее оборудование контрольное устройство, карточка признается недействительной.~~

Для проверки того, вводилась ли уже эта карточка ранее, контрольное устройство использует данные этой карточки тахографа, хранящиеся в его блоке памяти данных, как указано в требовании 133.

17) Карточки тахографов первого поколения признаются ~~записывающим оборудованием~~ **контрольным устройством** недействительными, после того как мастерская закрывает возможность использования карточек тахографа первого поколения в соответствии с ~~приложением~~ **подразделом 15** (требование **MIG003 MIG_003**).

18) Карточки мастерской первого поколения, введенные в ~~записывающее оборудование~~ **контрольное устройство** второго поколения, признаются недействительными.

19) ~~Записывающее оборудование~~ **Контрольное устройство** должно быть сконструировано таким образом, чтобы карточки тахографов, после того как они были надлежащим образом вставлены в интерфейс для считывания карточек, блокировались в нем в правильном положении.

20) **Извлечение** ~~выведение~~ карточки тахографа должно быть возможным только в случае остановки транспортного средства и после регистрации соответствующих данных в память карточки. **Извлечение** ~~выведение~~ карточки производится посредством преднамеренного действия пользователя.

3.2 Измерение скорости, местоположения и пробега

- 21) Датчик движения (возможно, встроенный в адаптер) является основным источником измерения скорости и пробега.
- 22) Данная функция обеспечивает постоянное измерение пройденного расстояния и показания счетчика пробега, соответствующие полному расстоянию, пройденному транспортным средством, с использованием системы импульсов, генерируемых датчиком движения.
- 23) Данная функция производит постоянное измерение и указывает значение скорости транспортного средства при помощи системы импульсов, генерируемых датчиком движения.
- 24) Функция измерения скорости также выдает информацию о том, движется ли транспортное средство или оно остановлено. Транспортное средство считается движущимся в том случае, если эта функция обнаруживает сигнал на уровне 1 имп./с в течение как минимум 5 секунд, передаваемый датчиком движения; в противном случае транспортное средство считается остановленным.
- 25) Устройства, показывающие скорость (спидометр) и общее пройденное расстояние (счетчик пробега), установленные на любом транспортном средстве, оснащенном ~~записывающим~~ **оборудованием контрольным устройством**, соответствующим положениям настоящего ~~регламента~~ **Соглашения**, должны удовлетворять требованиям, касающимся максимальных допусков, указанных в настоящем ~~дополнении~~ **добавлении** (см. 3.2.1 и 3.2.2).
- 26) В целях выявления манипуляций с данными о движении информация из датчика движения проверяется по информации о движении транспортного средства, поступающей из приемника ГНСС, и ~~(необязательно)~~ по другим источникам, не зависящим от датчика движения. **По меньшей мере еще один независимый источник снятия показаний движения транспортного средства должен быть встроен в БУ, что исключает необходимость внешнего интерфейса.**
- 27) Эта функция позволяет определять местоположение транспортного средства, что дает возможность автоматически регистрировать:
- местоположения, в которых водитель и/или второй водитель начинает свой дневной рабочий период;
 - местоположения, в которых ~~непрерывное~~ **накопленное** время управления достигает значения, кратного трем часам;
 - **местоположения, в которых транспортное средство пересекло границу страны;**
 - **местоположения, в которых выполнялись операции по загрузке или разгрузке;**
 - местоположения, в которых водитель и/или второй водитель завершает свой дневной рабочий период.

3.2.1 Измерение пройденного расстояния

- 28) Пройденное расстояние может измеряться таким образом:
- чтобы оно включало суммарное движение как вперед, так и назад; или
 - чтобы оно включало только движение вперед.
- 29) Диапазон измерения расстояния ~~записывающего оборудования~~ **контрольным устройством** должен составлять от 0 до 9 999 999,9 км.
- 30) Расстояние измеряется с соблюдением следующих допусков (расстояния не менее 1000 м):
- ± 1 % до установки;

- ± 2 % при установке и периодических инспекциях;
- ± 4 % в процессе эксплуатации.

Эти допуски не должны использоваться для преднамеренного изменения измеренного расстояния.

31) Расстояние измеряется с точностью до не менее 0,1 км.

3.2.2 Измерение скорости

32) Диапазон измерения скорости ~~записывающим оборудованием~~ **контрольным устройством** должен составлять от 0 до 220 км/ч.

33) В целях обеспечения максимального допуска на показываемую скорость на уровне ± 6 км/ч в процессе эксплуатации и с учетом:

- допуска ± 2 км/ч на разброс входных данных (разброс, обусловленный шинами, ...),
- допуска ± 1 км/ч на измерения, производимые во время установки или периодических инспекций,

~~записывающее оборудование~~ **контрольное устройство** должно обеспечивать, в диапазоне скоростей от 20 до 180 км/ч и характеристических коэффициентов транспортного средства от ~~24000~~ до 25 000 имп./км, измерение скорости с точностью 1 км/ч (при постоянной скорости).

Примечание: Разрешающая способность системы хранения данных обуславливает дополнительный допуск на данные по скорости, регистрируемой ~~записывающим оборудованием~~ **контрольным устройством** на уровне 0,5 км/ч.

34) Скорость измеряется правильно в пределах нормальных допусков в течение 2 секунд с момента завершения фазы изменения скорости в условиях, когда показатель изменения скорости составляет не более 2 м/с².

35) Скорость должна измеряться с точностью не менее 1 км/ч.

3.2.3 Измерение местоположения

36) ~~Записывающее оборудование~~ **Контрольное устройство** замеряет абсолютное местоположение транспортного средства с помощью приемника ГНСС.

37) Абсолютное местоположение ~~указывается~~ **измеряется** с помощью географических координат широты и долготы в градусах и минутах с точностью до 1/10 минуты.

3.3 Измерение времени

38) Функция измерения времени обеспечивает постоянное измерение и цифровое отображение даты и времени UTC.

39) Дата и время UTC используются для датирования данных в ~~записывающем оборудовании~~ **контрольном устройстве** (записи, обмен данными) и всех распечаток, указанных в **подразделе 4 «Распечатки»**.

40) Для визуализации местного времени предусматривается возможность изменения разницы в выводимом на дисплей времени через получасовые интервалы. Никакие другие изменения в сторону уменьшения или увеличения, кратные получасовым интервалам, не допускаются;

41) Смещение времени не должно превышать ~~± 21~~ **секунда** в сутки **или менее** в температурных условиях, предусмотренных ~~для официального утверждения типа,~~ **в соответствии с требованием 213**, при отсутствии любых корректировок времени.

41а) Точность времени в случае корректировки времени мастерскими в соответствии с требованием 212 составляет 3 секунды или менее.

41b) Бортовое устройство управляет счетчиком смещения, который рассчитывает максимальное смещение времени с момента последней корректировки времени в соответствии с пунктом 3.23. Максимальное смещение времени определяется изготовителем транспортного средства и не должно превышать 1 секунду в день, как указано в требовании 41.

41c) Показания счетчика смещения сбрасываются на 1 секунду после каждой корректировки времени записывающего оборудования в соответствии с пунктом 3.23. Эта процедура включает в себя:

- автоматическую корректировку времени;
- корректировку времени, выполняемую в режиме калибровки.

42) Время измеряется с точностью 1 секунда или менее.

43) Измерение времени не должно нарушаться в результате прекращения электропитания от внешнего источника в течение менее 12 месяцев в условиях, предусмотренных в случае официального утверждения типа.

3.4 Контроль за работой водителя

44) Данная функция обеспечивает постоянный и отдельный контроль за деятельностью одного водителя и одного второго водителя.

45) Деятельность водителя отображается как УПРАВЛЕНИЕ, РАБОТА, ГОТОВНОСТЬ или ПЕРЕРЫВ/ОТДЫХ.

46) Водитель и/или второй водитель могут вручную выбрать функцию РАБОТА, ГОТОВНОСТЬ или ПЕРЕРЫВ/ОТДЫХ.

47) Если транспортное средство движется, то в случае водителя автоматически выбирается функция УПРАВЛЕНИЕ, а в случае второго водителя автоматически выбирается функция ГОТОВНОСТЬ.

48) Если транспортное средство останавливается, то в случае водителя автоматически выбирается функция РАБОТА.

49) Считается, что первое изменение вида деятельности в течение 120 секунд после автоматического переключения на функцию ПЕРЕРЫВ/ОТДЫХ или ГОТОВНОСТЬ в связи с остановкой транспортного средства производится в момент его остановки (что может предполагать отмену перехода на функцию РАБОТА).

50) Данная функция обеспечивает передачу данных об изменении вида деятельности в записывающее устройство с интервалом в одну минуту.

51) Если применительно к календарной минуте функция УПРАВЛЕНИЕ регистрируется непосредственно до этой минуты и сразу же после нее, то вся эта минута зачитывается как УПРАВЛЕНИЕ.

52) Если календарная минута не зачитывается в соответствии с требованием 051 в качестве УПРАВЛЕНИЯ, то вся эта минута зачитывается в качестве того же вида деятельности, что и деятельность, которая осуществлялась непрерывно дольше всего в течение этой минуты (или самая последняя в случае нескольких видов деятельности одинаковой продолжительности).

53) Данная функция также обеспечивает постоянный контроль за непрерывным временем управления и совокупным временем перерывов в работе водителя.

3.5 Контроль за статусом управления

54) Данная функция обеспечивает постоянный автоматический контроль за статусом управления.

55) Если в устройство вставляются две действительные карточки водителя, то регистрируется статус управления ЭКИПАЖ, а во всех других случаях регистрируется статус управления ОДИН.

3.6 Записи водителей

3.6.1 Ввод данных о местах, в которых начинаются и/или заканчиваются дневные периоды работы

56) Данная функция позволяет ввести названия мест, в которых, по данным водителя и/или второго водителя, начинаются и/или заканчиваются дневные периоды работы.

57) Места определяются как страна и в некоторых случаях дополнительно как регион, что вводится или подтверждается вручную.

58) **При извлечении В момент изъятия карточки водителя (или мастерской) записывающее оборудование контрольное устройство отображает местоположение транспортного средства в данный момент времени на основе информации ГНСС и сохраненной цифровой карты в соответствии с пунктом 3.12.19 и предлагает держателю карточки подтвердить или скорректировать название данного места вручную, предлагая водителю (второму водителю) доехать до «места, где заканчивается ежедневный рабочий период».**

59) **Место, указанное в соответствии с требованием 58, считается местом, в котором закончен данный дневной период работы. Оно заносится в соответствующую карточку водителя (или мастерской) как временная запись, и по этой причине может быть удалена и затем перезаписана. После этого водитель должен указать текущее место транспортного средства, которое считается временной записью.**

В следующих условиях временная запись, сделанная при последнем извлечении карточки, подтверждается (т. е. больше не перезаписывается):

- ввод места, где начинается текущий ежедневный рабочий период во время ручного ввода в соответствии с требованием (61);
- следующая запись места, в котором начинается текущий ежедневный рабочий период, если держатель карточки не внес никакого другого места, в котором начинается или заканчивается рабочий период, в процессе ручного ввода данных в соответствии с требованием (61).

В следующих условиях временная запись, сделанная при последнем извлечении карточки, перезаписывается и подтверждается внесенное новое значение:

- следующая запись места, в котором заканчивается текущий ежедневный рабочий период, если держатель карточки не внес никакого места, в котором начинается или заканчивается рабочий период, в процессе ручного ввода данных в соответствии с требованием (61).

60) Места, в которых начинаются и/или заканчиваются ежедневные периоды работы, можно вводить при помощи команд в меню. Если в течение одной календарной минуты производится ввод более чем одной такой записи, то сохраняется только последняя запись места начала и последняя запись места окончания.

Записывающее оборудование отображает текущее местоположение транспортного средства на основе информации ГНСС и сохраненной цифровой карты в соответствии с пунктом 3.12.19 и предлагает водителю подтвердить или скорректировать это место вручную.

3.6.2 Ручной ввод данных о действиях водителя и согласии водителя на использование интерфейса ИТС

61) ~~Записывающее~~—оборудование **Контрольное устройство** позволяет вручную вводить записи о деятельности только при введении карточки водителя (или мастерской) и только тогда. Ручной ввод данных о деятельности осуществляется с указанием значений местного времени и даты в часовом поясе (с учетом разницы с UTC), указанном в данный момент в бортовом устройстве.

В момент ввода карточки водителя или мастерской держателю карточки выдается информация:

- о дате и времени последнего извлечения им карточки;
- (необязательно) о разнице с местным временем, установленном в данный момент в бортовом устройстве.

При первом вводе соответствующей карточки водителя или мастерской, на данный момент неизвестной для бортового устройства, держателю карточки предлагается дать согласие на вывод личных данных, связанных с тахографом, через ~~факультативный~~ интерфейс ИТС. **Для проверки того, вводилась ли уже эта карточка ранее, регистрирующее оборудование использует данные этой карточки тахографа, хранящиеся в его блоке памяти данных, как указано в требовании 133.**

В любой момент согласие водителя (соответственно мастерской) можно активировать или отменить при помощи соответствующих команд в меню, при условии, что введена карточка водителя (соответственно мастерской).

Данные о деятельности можно вводить со следующими ограничениями:

- деятельность водителя отображается как РАБОТА, ГОТОВНОСТЬ или ПЕРЕРЫВ/ОТДЫХ;
- время начала и завершения каждого вида деятельности находится только в пределах периода между последним извлечением и текущим вводом карточки;
- дублирование видов деятельности во времени не допускается.

При необходимости записи можно вводить вручную при первом вводе ранее неиспользовавшейся карточки водителя (или мастерской).

Процедура ручного ввода видов деятельности включает в себя столько последовательных шагов, сколько необходимо для указания вида, времени начала и времени завершения каждого вида деятельности. В случае любого отрезка времени между последним извлечением карточки и ее вводом в данный момент держатель карточки может не указывать никакого вида деятельности.

При ручном вводе записей, связанных с вводом карточки, и в случае применимости, держатель карточки может указать:

- место, в котором завершился предыдущий ежедневный период работы, связанный с определенным временем (и таким образом **и подтвердить запись**, сделанную при последнем извлечении карточки);
- место, в котором начинается текущий ежедневный период работы, связанный с определенным временем (**и таким образом подтвердить временную запись, сделанную при последнем извлечении карточки**).

В случае места, в котором начинается текущий ежедневный период работы и которое было внесено при вводе карточки в данный момент времени, регистрирующее оборудование отображает местоположение транспортного средства в данный момент на основе информации ГНСС и сохраненной(ых) цифровой(ых) карты (карт) в соответствии с пунктом 3.12.19 и предлагает водителю подтвердить или скорректировать это место вручную.

Если держатель карточки не вводит никакого места, в котором начинается или завершается данный период работы, то при ручном вводе записей, связанных с

введением карточки, такие действия считаются подтверждением того, что его период работы после извлечения карточки в последний раз не изменился. Следующая запись места, в котором завершается предыдущий ежедневный период работы, записывается поверх временной записи, сделанной при последнем извлечении карточки.

Если какое-либо место введено, то оно регистрируется на соответствующей карточке тахографа.

Ручные записи прерываются, если:

- карточка извлекается; или
- если транспортное средство движется, а карточка находится в считывающем устройстве водителя.

При этом допускаются дополнительные перерывы, например перерыв после определенного периода бездействия пользователя. Если ручной ввод записи прерывается, то ~~записывающее оборудование~~ **контрольное устройство** подтверждает все завершенные записи места и вида деятельности (если указано конкретное место и время или вид деятельности, время начала и время завершения).

Если во время ручного ввода записей о деятельности на уже введенной карточке вводится карточка второго водителя или мастерской, то ручной ввод записи на первой карточке можно завершить, прежде чем начинать ручной ввод на вторую карточку.

Держатель карточки может вводить записи вручную в соответствии со следующей минимальной процедурой:

- ввести вручную в хронологическом порядке виды деятельности за последний период между последним извлечением карточки и ее вводом в данный момент;
- время начала первого вида деятельности совпадает со временем извлечения карточки. Для каждой последующей записи время начала устанавливается заранее сразу же после времени завершения предыдущей записи. Вид деятельности и время окончания выбираются для каждого вида деятельности.

Эта процедура завершается в тот момент, когда время завершения деятельности, введенной вручную, соответствует времени ввода карточки.

Записывающее оборудование позволяет водителям и мастерским попеременно загружать ручные записи, которые необходимо ввести во время этой процедуры, через интерфейс ИТС, указанный в подразделе 13, и, по желанию, через другие интерфейсы.

~~После этого записывающее оборудование~~ **Контрольное устройство** дает владельцу карточки возможность изменять, ~~по желанию,~~ любые данные о деятельности, введенные вручную, до их подтверждения с помощью выбранной конкретной команды. После этого никакие другие изменения невозможны.

3.6.3 Ввод данных об особых условиях

62) ~~Записывающее оборудование~~ **контрольное устройство** дает водителю возможность в режиме реального времени вводить следующие два конкретных условия:

- «НЕПРИМЕНИМО» (начало, конец)
- ПЕРЕЕЗД НА ПАРОМЕ/ПОЕЗДЕ (начало, конец)

Условие «ПЕРЕЕЗД НА ПАРОМЕ/ПОЕЗДЕ» ~~может не открыться~~ не откроется, если открыто условие «НЕПРИМЕНИМО». Если функция «НЕПРИМЕНИМО» открыта, то ~~записывающее оборудование~~ не должно позволять пользователям вводить метку начала условия «ПЕРЕЕЗД НА ПАРОМЕ/ПОЕЗДЕ».

В случае ввода или извлечения карточки водителя открытое условие «НЕПРИМЕНИМО» должно автоматически закрыться ~~записывающим оборудованием~~ **контрольным устройством.**

Открытое условие «НЕПРИМЕНИМО» блокирует следующие события и предупреждения:

- управление без соответствующей карточки;
- предупреждения, связанные с непрерывным временем вождения.

Водитель вводит метку, указывающую на начало ПЕРЕЕЗДА НА ПАРОМЕ/ПОЕЗДЕ, **сразу же после выбора варианта ПЕРЕРЫВ/ОТДЫХ** ~~перед тем, как заглушить двигатель~~ на пароме/поезде.

Открытое условие ПЕРЕЕЗД НА ПАРОМЕ/ПОЕЗДЕ должно быть завершено **контрольным устройством в тот момент**, когда происходит любой из следующих случаев:

- водитель вручную закрывает позицию ПЕРЕЕЗД НА ПАРОМЕ/ПОЕЗДЕ, **которая начинается по прибытии парома/поезда, перед съездом с парома/поезда;**
- **открывается позиция «НЕПРИМЕНИМО»;**
- водитель извлекает свою карточку;
- **деятельность водителя учитывается как ДВИЖЕНИЕ в течение одной календарной минуты в соответствии с пунктом 3.4.**

Если в течение одной календарной минуты выполняется более одной записи конкретных условий одного и того же типа, то регистрируется только последнее условие.

~~Открытое условие ПЕРЕЕЗД НА ПАРОМЕ/ПОЕЗДЕ заканчивается, если оно более недействительно в соответствии с правилами, изложенными в Регламенте (ЕС) № 561/2006, **настоящем Соглашении.**~~

3.6.4 Ввод операций по загрузке или разгрузке

62a) **Записывающее оборудование** позволяет водителю вводить и подтверждать в режиме реального времени информацию, *указывающую на то, что транспортное средство загружается/разгружается или что выполняется одновременная операция загрузки/разгрузки.*

Если в течение одной календарной минуты выполняется более одной записи конкретных условий одного и того же типа, то регистрируется только последнее условие.

62b) Загрузка, разгрузка или одновременные операции по загрузке/разгрузке регистрируются как отдельные события.

62c) Информация о загрузке/разгрузке вводится до того, как транспортное средство покинет место, где выполняется операция по загрузке/разгрузке.

3.7 Управление системой блокировки, установленной предприятием

63) Данная функция позволяет управлять установленной предприятием системой блокировки в целях ограничения доступа к данным в режиме работы предприятия только для самого предприятия.

64) Функция блокировки предприятием заключается в указании даты/времени начала (блокировки) и даты/времени завершения (разблокировки) в увязке с идентификацией предприятия с помощью номера карточки предприятия (в момент блокировки).

65) Блокировку можно поставить в положение «включено» или «выключено» только в режиме реального времени.

66) Разблокировку может произвести только предприятие, которое произвело блокировку (идентифицируемое с помощью первых 13 цифр номера карточки предприятия), или

67) Разблокировка производится автоматически, если блокировку производит другое предприятие.

68) В том случае, если какое-либо предприятие производит блокировку и если предыдущая блокировка была произведена этим же предприятием, предполагается, что предыдущая блокировка не была снята и все еще находится в положении «включено».

3.8 Мониторинг работы системы контроля

69) Данная функция предусмотрена для осуществления контроля за операциями ВЫВОД НА ДИСПЛЕЙ, ВЫВОД НА ПРИНТЕР, БОРТОВОЕ УСТРОЙСТВО и ЗАГРУЗКА карточки и КАЛИБРОВКА НА ДОРОГАХ, осуществляемыми в режиме контроля.

70) Данная функция также отслеживает работу системы КОНТРОЛЬ ЗА ПРЕВЫШЕНИЕМ СКОРОСТИ в режиме контроля. Считается, что контроль за превышением скорости производится в том случае, если в режиме контроля на принтер или дисплей выводится сообщение «превышение скорости» или если из блока памяти данных бортового устройства загружаются данные «события и неисправности».

3.9 Выявление соответствующих событий и/или неисправностей

71) Данная функция позволяет обнаруживать следующие события и/или неисправности:

3.9.1 Событие «Ввод недействительной карточки»

72) Данное событие отображается в том случае, если введена любая недействительная карточка, если введена карточка водителя, которая уже была заменена, и/или если срок действия введенной карточки истекает.

3.9.2 Событие «несовместимость карточек»

73) Данное событие отображается в том случае, когда возникает комбинация из любых действительных карточек, отмеченных в следующей таблице знаком X:

Несовместимость карточек		Считывающее устройство водителя				
		Карточка не вставлена	Карточка водителя	Карточка контролера	Карточка мастерской	Карточка предприятия
Считывающее устройство второго водителя	Карточка не вставлена					
	Карточка водителя				X	
	Карточка контролера			X	X	X
	Карточка мастерской		X	X	X	X
	Карточка предприятия			X	X	X

3.9.3 Событие «Нестыковка во времени»

74) Данное событие отображается в том случае, когда текущая дата/время ввода карточки в ~~записывающем оборудовании~~ **контрольном устройстве** предшествует дате/времени последнего извлечения карточки водителя, считываемым с карточки.

3.9.4 Событие «Вождение без соответствующей карточки»

75) Данное событие отображается в случае любой комбинации действительных карточек тахографа, отмеченных знаком X в следующей таблице, когда вид деятельности водителя изменяется на УПРАВЛЕНИЕ или когда изменяется режим работы в то время, когда деятельность водителя соответствует функции УПРАВЛЕНИЕ:

Управление без соответствующей карточки		Считывающее устройство водителя				
		Карточка не вставлена	Карточка водителя	Карточка контролера	Карточка мастерской	Карточка предприятия
Считывающее устройство второго водителя	Карточка не вставлена	X		X		X
	Карточка водителя	X		X	X	X
	Карточка контролера	X	X	X	X	X
	Карточка мастерской	X	X	X		X
	Карточка предприятия	X	X	X	X	X

3.9.5 Событие «Ввод карточки во время управления»

76) Данное событие отображается в том случае, когда карточка тахографа вводится в любое считывающее устройство в то время, когда вид деятельности водителя соответствует функции УПРАВЛЕНИЕ.

3.9.6 Событие «Неправильное завершение последнего сеанса использования карточки»

77) Данное событие отображается в том случае, когда в момент ввода карточки ~~записывающее оборудование~~ **контрольное устройство** обнаруживает, что несмотря на положения пункта 3.1 предыдущий сеанс использования карточки был завершён неправильно (карточка была извлечена прежде, чем на ней были сохранены соответствующие данные). Данное событие отображается только в случае карточек водителя и мастерской.

3.9.7 Событие «Превышение скорости»

78) Данное событие отображается в каждом случае превышения скорости.

3.9.8 Событие «Прекращение электропитания»

79) Данное событие отображается, за исключением режима калибровки или контроля, в случае прекращения питания датчика движения и/или бортового устройства в течение более 200 миллисекунд. Пороговую величину прекращения устанавливает изготовитель. В случае падения напряжения в результате запуска двигателя транспортного средства данное событие не отображается.

3.9.9 Событие «Ошибка связи со средством удаленной связи»

80) Данное событие отображается, за исключением режима калибровки, в том случае, когда средство удаленной связи не подтверждает факт успешного получения данных удаленной связи, отправленных из бортового устройства, более чем с трех попыток.

3.9.10 Событие «Отсутствие информации о местоположении от приемника ГНСС»

81) Это событие отображается, за исключением режима калибровки, в случае отсутствия информации о местоположении, выдаваемой приемником ГНСС (внутренним или внешним) по прошествии более трех часов накопленного времени движения.

3.9.11 Событие «Ошибка связи с внешним устройством ГНСС»

82) Данное событие отображается, за исключением режима калибровки, в случае прерывания связи между внешним устройством ГНСС и бортовым устройством более чем на 20 минут подряд во время движения транспортного средства.

3.9.12 Событие «Ошибочные данные о движении»

83) Данное событие отображается, за исключением режима калибровки, в случае нарушения нормального потока данных между датчиком движения и бортовым устройством и/или в случае ошибки, указывающей на нарушение целостности или аутентичности данных в процессе передачи данных между датчиком движения и бортовым устройством. **Это событие также отображается, за исключением режима калибровки, в том случае, если скорость, рассчитанная по импульсам датчика движения, увеличивается с 0 до более чем 40 км/ч в течение 1 секунды, а затем остается выше 40 км/ч в течение не менее 3 секунд.**

3.9.13 Событие «Противоречивая информация о движении транспортного средства»

84) Данное событие отображается, **как указано в подразделе 12 добавления**, за исключением режима калибровки, в том случае, если информация о движении, выдаваемая датчиком движения, противоречит информации, выдаваемой внутренним приемником ГНСС или внешним устройством ГНСС **или и, возможно, другим(и) независимым(и) источником(ами) в соответствии с требованием 26, как указано в приложении 12.** Данное событие не отображается во время переезда на пароме/поезде, при активной функции НЕПРИМЕНИМО или если нет информации о местоположении из приемника ГНСС.

3.9.14 Событие «Попытка нарушения системы защиты»

85) Данное событие отображается в случае любого другого факта нарушения защиты датчика движения и/или бортового устройства и/или внешнего устройства ГНСС, как указано в ~~приложении~~ **подразделе 10**, за исключением режима калибровки.

3.9.15 Событие «Нестыковка по времени»

86) Данное событие отображается, за исключением режима калибровки, если бортовое устройство обнаруживает несоответствие ~~продолжительностью более 4 минуты~~ между временем срабатывания функции замера времени бортового устройства и временем, выданным ~~из аутентифицированных точек, переданных приемником ГНСС или внешним устройством ГНСС.~~ **«Нестыковка по времени» обнаруживается, если разница во времени превышает ± 3 секунды, что соответствует точности времени, установленной в требовании 41а, с учетом того, что она увеличивается на установленную величину максимального смещения времени в сутки.** Это событие регистрируется вместе с показаниями внутренних часов ~~контрольного устройства транспортного средства и передается вместе с автоматической регулировкой времени.~~ **После возникновения события, связанного с противоречивой информацией о времени, бортовое устройство не будет генерировать другие события такого же характера в течение следующих 12 часов.** Данное событие

~~не отображается в тех случаях, когда приемник ГНСС не обнаруживает действительного сигнала ГНСС в течение последних 30 дней. БУ должно выполнять проверку на отображение события «нестыковка по времени» непосредственно перед тем, как БУ автоматически еще раз скорректирует внутренние часы БУ в соответствии с требованием 211. Однако если информация о местоположении, выданная приемником ГНСС, появляется снова, производится автоматическая корректировка времени.~~

3.9.16 Неисправность «Карточка»

87) Эта неисправность отображается в случае сбоя в работе карточки тахографа, возникшего в процессе работы.

3.9.17 Неисправность «Записывающее оборудование Контрольное устройство»

88) Эта неисправность отображается в случае возникновения любых из перечисленных ниже сбоев, за исключением режима калибровки:

- внутренние неполадки в БУ;
- неисправность принтера;
- неисправность дисплея;
- ошибка при загрузке;
- неисправность датчика;
- неисправность приемника ГНСС или внешнего устройства ГНСС;
- неисправность средства удаленной связи;
- **неисправность интерфейса ИТС (если применимо).**

3.9.18 Событие «Аномалия ГНСС»

88a) Это событие отображается, за исключением режима калибровки, в том случае, если приемник ГНСС выявляет попытку взлома или когда аутентификация навигационных сообщений не подтвердилась, как указано в подразделе 12. После отображения события, связанного с аномалией ГНСС, БУ прекращает выдавать другие события, связанные с аномалией, в течение следующих 10 минут.

3.10 «Встроенные системы проверки и самопроверки»

89) ~~Записывающее оборудование~~ **Контрольное устройство** самостоятельно обнаруживает неисправности посредством проведения самопроверки и с помощью встроенной системы проверки в соответствии со следующей таблицей:

<i>Компонент, подлежащий проверке</i>	<i>Система самопроверки</i>	<i>Встроенная система проверки</i>
Программное обеспечение		Целостность
Блок памяти	Доступ	Доступ, целостность данных
Интерфейсы для считки карточек	Доступ	Доступ
Клавиатура		Ручная проверка
Принтер	(по усмотрению изготовителя)	Распечатка
Дисплей		Визуальная проверка

<i>Компонент, подлежащий проверке</i>	<i>Система самопроверки</i>	<i>Встроенная система проверки</i>
Загрузка (осуществляется только в процессе загрузки)	Работает нормально	
Датчик	Работает нормально	Работает нормально
Неисправность средства удаленной связи	Работает нормально	Работает нормально
Устройство ГНСС	Работает нормально	Работает нормально
Интерфейс ИТС (факультативно)	Работает нормально	

3.11 Считывание данных из блока памяти

90) ~~Записывающее оборудование~~ **Контрольное устройство** способно считывать любые данные, содержащиеся в его блоке памяти.

3.12 Регистрация и хранение данных в блоке памяти

Для целей настоящего пункта:

- «365 дней» определяется как 365 календарных суток усредненной продолжительности деятельности водителя на транспортном средстве. Усредненная продолжительность деятельности в день на транспортном средстве определяется в расчете, как минимум, на 6 водителей или вторых водителей, 6 циклов ввода и извлечения карточек и 256 случаев изменения вида деятельности. Таким образом, термин «365 дней» включает, как минимум, 2190 водителей (вторых водителей), 2190 циклов ввода и извлечения карточек и 93 440 случаев изменения вида деятельности;
- **среднесуточное количество записей мест определяется в расчете, как минимум, на 6 записей, когда начинается ежедневный рабочий период, и 6 записей, когда заканчивается ежедневный рабочий период, вследствие чего «365 дней» включают не менее 4380 записей мест;**
- **среднесуточное количество местоположений, когда накопленное время управления достигает кратности три часа, определяется в расчете, как минимум, на 6 местоположений, вследствие чего «365» дней включают, как минимум, 2190 таких местоположений, когда начинается ежедневный рабочий период, 6 местоположений, когда непрерывное накопленное время вождения водителя достигает кратности три часа, и 6 местоположений, когда ежедневный рабочий период заканчивается, так что «365 дней» включают по меньшей мере 6570 местоположений;**
- **среднесуточное количество пересечений границы определяется в расчете, как минимум, на 20 пересечений, вследствие чего «365 дней» включают не менее 7300 пересечений границы;**
- **среднесуточное количество операций загрузки/разгрузки определяется в расчете, как минимум, на 25 операций (независимо от типа), вследствие чего «365 дней» включают не менее 9125 операций загрузки/разгрузки;**
- время регистрируется с точностью до одной минуты, если не предусмотрено иное;
- показания счетчик пробега регистрируются с точностью до одного километра;

- показания спидометра регистрируются с точностью 1 км/ч;
- местоположение (широта и долгота) регистрируется в градусах и минутах с точностью 1/10 минуты с учетом соответствующей точности ГНСС и времени получения **и с отображением метки, указывающей на аутентификацию данного местоположения.**

91) Данные, хранящиеся в блоке памяти, не должны нарушаться в результате прекращения внешнего электропитания продолжительностью не более 12 месяцев в условиях, предусмотренных официальным утверждением типа. Кроме того, данные, хранящиеся во внешнем устройстве удаленной связи, как указано в ~~приложении~~ **подразделе 14**, не должны нарушаться в результате прекращения электропитания в течение не менее 28 дней.

92) ~~Записывающее оборудование~~ **Контрольное устройство** способно самостоятельно или по команде регистрировать и хранить в своей памяти следующие данные:

3.12.1 Идентификационные данные оборудования

3.12.1.1 Идентификационные данные бортового устройства

93) ~~Записывающее оборудование~~ **Контрольное устройство** способно хранить в своей памяти следующие идентификационные данные бортового устройства:

- название изготовителя;
- адрес изготовителя;
- номер деталей;
- серийный номер;
- поколение БУ;
- возможность использовать карточки тахографов первого поколения;
- номер версии программного обеспечения;
- дата установки программного обеспечения;
- год изготовления оборудования;
- номер официального утверждения;
- **идентификатор версии цифровой карты (требование 1331).**

94) Идентификационные данные бортового устройства регистрируются и хранятся раз и навсегда изготовителем бортового устройства, за исключением ~~даты и номера официального утверждения программного обеспечения, которые могут~~, которая может быть изменена в случае перехода на обновленную версию программы, и возможности использовать карточки тахографов первого поколения.

3.12.1.2 Идентификационные данные датчика движения

95) Датчик движения способен хранить в своей памяти следующие идентификационные данные:

- название изготовителя;
- серийный номер;
- номер официального утверждения;
- идентификатор встроенного компонента защиты (например, номер встроенной интегральной микросхемы/процессора);
- идентификатор операционной системы (например, номер версии программного обеспечения).

96) Идентификационные данные датчика движения регистрируются и хранятся раз и навсегда в памяти датчика движения изготовителем.

97) Бортовое устройство способно регистрировать и хранить в своей памяти следующие данные, связанные с 20 последними **успешными** подсоединениями датчиков движения (если в течение одного календарного дня произведено несколько сопряжений, то информация сохраняется только о первом и последнем за указанный день).

По каждому такому подсоединению регистрируются следующие данные:

- идентификационные данные датчика движения:
 - серийный номер;
 - номер официального утверждения;
- данные подсоединения датчиков движения:
 - дата подсоединения.

3.12.1.3 Идентификационные данные глобальных навигационных спутниковых систем

98) Внешнее устройство ГНСС способно хранить в своей памяти следующие идентификационные данные:

- название изготовителя;
- серийный номер;
- номер официального утверждения;
- идентификатор встроенного компонента защиты (например, номер встроенной интегральной микросхемы/процессора);
- идентификатор операционной системы (например, номер версии программного обеспечения).

99) Идентификационные данные регистрируются и хранятся раз и навсегда в памяти внешнего устройства ГНСС изготовителем внешнего устройства ГНСС.

100) Бортовое устройство способно регистрировать и хранить в своей памяти следующие данные, связанные с 20 последними **успешными** подсоединениями внешних устройств ГНСС (если в течение одного календарного дня произведено несколько подсоединений, то информация сохраняется только о первом и последнем за указанный день).

По каждому такому подсоединению регистрируются следующие данные:

- идентификационные данные внешнего устройства ГНСС:
 - серийный номер;
 - номер официального утверждения;
- данные о подсоединении к внешнему устройству ГНСС:
 - дата подсоединения.

3.12.2 Ключи и сертификаты

101) ~~Записывающее оборудование~~ **Контрольное устройство** способно хранить ряд криптографических ключей и сертификатов, как указано в частях А и В, **подраздел 11**.

3.12.3 Данные о вводе и извлечении карточек водителя или мастерской

102) В случае каждого цикла ввода в устройство карточки водителя или мастерской и ее извлечения из него ~~записывающее оборудование~~ **контрольное устройство** регистрирует и хранит в своей памяти следующие данные:

- фамилия и имя (имена) держателя карточки, записанные в блоке памяти карточки;

- номер карточки, название выдавшего выдавшей ее ~~государства-члена Договаривающейся стороны~~ и дата истечения срока действия, записанные в блоке памяти карточки;
- поколение карточки;
- дата и время ввода;
- показание счетчика пробега транспортного средства в момент ввода карточки;
- считывающее устройство, в которое вводится карточка;
- дата и время извлечения;
- показание счетчика пробега транспортного средства в момент извлечения карточки;
- следующая информация о предыдущем транспортном средстве, которым пользовался водитель, записанная в блоке памяти карточки:
- VRN (регистрационный номер транспортного средства) и ~~государство-член Договаривающейся стороны~~ регистрации;
- поколение БУ (если есть);
- дата и время извлечения карточки;
- метка, указывающая на момент ввода карточки, ввел ли держатель карточки данные о своей деятельности вручную или нет.

103) Блок памяти способен хранить эти данные в течение не менее 365 дней.

104) Когда объем памяти заполнен, новые данные записываются поверху самых старых данных.

3.12.4 Данные о деятельности водителя

105) ~~Занимающее оборудование~~ **Контрольное устройство** должно регистрировать и хранить в своей памяти все факты изменения деятельности водителя и/или второго водителя и/или все случаи изменения статуса управления и/или все случаи ввода или извлечения карточки водителя или мастерской:

- статус управления (ЭКИПАЖ, ОДИН);
- считывающее устройство (ВОДИТЕЛЬ, ВТОРОЙ ВОДИТЕЛЬ);
- статус карточки в соответствующем считывающем устройстве (ВСТАВЛЕНА, НЕ ВСТАВЛЕНА);
- вид деятельности (УПРАВЛЕНИЕ, ГОТОВНОСТЬ, РАБОТА, ПЕРЕРЫВ/ОТДЫХ);
- дата и время изменения.

Статус ВСТАВЛЕНА означает, что в считывающее устройство вставлена действительная карточка водителя или мастерской. Статус НЕ ВСТАВЛЕНА означает обратное, т. е. в считывающем устройстве нет ни действительной карточки водителя, ни действительной карточки мастерской (например, вставлена карточка предприятия или никакой карточки в устройстве нет).

Данные о деятельности, которые вводятся водителем вручную, в блоке памяти не регистрируются.

106) Блок памяти способен хранить эти данные о деятельности водителя в течение не менее 365 дней.

107) Когда объем памяти заполнен, новые данные записываются поверху самых старых данных.

3.12.5 Места и местоположения, в которых начинаются и заканчиваются ежедневные периоды работы и/или достигается 3-часовое предельное значение непрерывного накопленного времени управления

108) ~~Записывающее оборудование~~ **Контрольное устройство** способно считывать любые данные, содержащиеся в его блоке памяти:

- места и местоположения, в которых водитель и/или второй водитель начинает свой дневной рабочий период;
- местоположения, в которых ~~непрерывное~~ **накопленное** время управления достигает значения, кратного трем часам;
- места и местоположения, в которых водитель и/или второй водитель начинает свой дневной рабочий период.

109) Если местоположение транспортного средства в эти моменты времени по данным приемника ГНСС неизвестно, то ~~записывающее оборудование~~ **контрольное устройство** использует данные последнего записанного местоположения и соответствующие дату и время.

110) Наряду с каждым местом и местоположением ~~записывающее оборудование~~ **контрольное устройство** способно считывать любые данные, содержащиеся в его блоке памяти:

- номер карточки водителя (второго водителя) и государство-член, выдавшее Договаривающаяся сторона, выдавшая карточку;
- поколение карточки;
- дата и время изменения;
- тип ввода (начало, окончание или 3-часовой отрезок ~~непрерывного~~ **накопленного** времени управления);
- соответствующие данные, касающиеся точности, даты и времени ГНСС, если применимо;
- показания счетчика пробега транспортного средства;
- **метка, указывающая на то, было ли аутентифицировано данное местоположение.**

110а) В случае мест, в которых начинается или заканчивается ежедневный рабочий период, введенный во время процедуры ручного ввода карточки в соответствии с требованием 61, сохраняется текущее значение счетчика пробега и местоположение транспортного средства.

111) Блок памяти способен хранить места и местоположения, в которых начинаются и заканчиваются ежедневные периоды работы и/или достигается 3-часовой период ~~непрерывного~~ **накопленного** времени управления, в течение не менее 365 дней.

112) Когда объем памяти заполнен, новые данные записываются поверху самых старых данных.

3.12.6 Данные счетчика пробега

113) ~~Записывающее оборудование~~ **Контрольное устройство** записывает в свой блок памяти данных показания счетчика пробега транспортного средства и соответствующую дату в полночь каждого календарного дня.

114) Блок памяти данных способен хранить показания счетчика пробега по состоянию на полночь в течение не менее 365 календарных дней.

115) Когда объем памяти заполнен, новые данные записываются поверху самых старых данных.

3.12.7 Детальные данные о скорости

116) ~~Записывающее оборудование~~ **Контрольное устройство** в своем блоке памяти регистрирует и хранит мгновенную скорость транспортного средства и соответствующие дату и время с интервалом в 1 секунду, как минимум, за последние 24 часа, в течение которых транспортное средство находилось в движении.

3.12.8 Данные о событиях

Для целей настоящего подпункта время регистрируется с точностью до 1 секунды.

117) ~~Записывающее оборудование~~ **Контрольное устройство** в своем блоке памяти регистрирует и хранит следующие данные по каждому обнаруженному событию в соответствии с указанными ниже правилами хранения:

<i>Событие</i>	<i>Правила хранения</i>	<i>Данные по каждому событию, подлежащие записи</i>
Ввод недействительной карточки	– 10 самых последних событий	<ul style="list-style-type: none"> – дата и время события – тип и номер карточки (карточек), государство-член, выдавшее Договаривающаяся сторона, выдавшая карточку, и поколение карточки, явившейся причиной данного события – число аналогичных событий за указанный день
Несовместимость карточки	– 10 самых последних событий	<ul style="list-style-type: none"> – дата и время начала события – дата и время окончания события – тип карточки (карточек), номер, государство-член, выдавшее Договаривающаяся сторона, выдавшая карточку, и поколение двух карточек, явившихся причиной несовместимости
Управление без соответствующей карточки	<ul style="list-style-type: none"> – самое длительное событие за каждый из 10 последних дней возникновения таких событий – 5 самых длительных событий за последние 365 дней 	<ul style="list-style-type: none"> – дата и время начала события – дата и время окончания события – тип карточки (карточек), номер, государство-член, выдавшее Договаривающаяся сторона, выдавшая любую карточку, вставленную в начале и/или в конце события и ее поколение – число аналогичных событий за указанный день
Ввод карточки во время управления	– самое длительное событие за каждый из 10 последних дней с начала возникновения таких событий	<ul style="list-style-type: none"> – дата и время события – тип карточки (карточек), номер, государство-член, выдавшее Договаривающаяся сторона, выдавшая карточки, и их поколение – число аналогичных событий за указанный день

Событие	Правила хранения	Данные по каждому событию, подлежащие записи
Неправильное завершение последнего сеанса использования карточки	– 10 самых последних событий	<ul style="list-style-type: none"> – дата и время ввода карточки – тип карточки (карточек), номер, государство-член, выдавшее Договаривающаяся сторона, выдавшая карточки, и их поколение – последняя дата сеанса использования, записанная на карточке: – дата и время ввода карточки – VRN, Договаривающаяся сторона регистрации и поколение БУ
Превышение скорости (1)	<ul style="list-style-type: none"> – наиболее серьезное событие за последние 10 дней возникновения таких событий (т. е. случай регистрации самой высокой средней скорости) – 5 самых длительных событий за последние 365 дней – первое событие, наступившее после последней калибровки 	<ul style="list-style-type: none"> – дата и время начала события – дата и время окончания события – максимальная скорость, измеренная во время события – среднеарифметическая скорость, измеренная во время события – тип карточки, номер, государство-член, выдавшее Договаривающаяся сторона, выдавшая карточку водителя (если применимо) – число аналогичных событий за указанный день
Прекращение электропитания (2)	<ul style="list-style-type: none"> – самое длительное событие за каждый из 10 последних дней возникновения таких событий – 5 самых длительных событий за последние 365 дней 	<ul style="list-style-type: none"> – дата и время начала события – дата и время окончания события – тип карточки (карточек), номер, государство-член, выдавшее Договаривающаяся сторона, выдавшая любую карточку, вставленную в начале и/или конце события, и ее поколение – число аналогичных событий за указанный день
Ошибка связи с устройством удаленной связи	<ul style="list-style-type: none"> – самое длительное событие за каждый из 10 последних дней возникновения такого события – 5 самых длительных событий за последние 365 дней 	<ul style="list-style-type: none"> – дата и время начала события – дата и время окончания события – тип карточки (карточек), номер, государство-член, выдавшее Договаривающаяся сторона, выдавшая любую карточку, вставленную в начале и/или конце события – число аналогичных событий за указанный день
Отсутствие информации о местоположении от приемника ГНСС	<ul style="list-style-type: none"> – самое длительное событие за каждый из 10 последних дней возникновения такого события – 5 самых длительных событий за последние 365 дней 	<ul style="list-style-type: none"> – дата и время начала события – дата и время окончания события – тип карточки (карточек), номер, государство-член, выдавшее Договаривающаяся сторона, выдавшая любую карточку

Событие	Правила хранения	Данные по каждому событию, подлежащие записи
Ошибка связи с внешним устройством ГНСС	<ul style="list-style-type: none"> – самое длительное событие за каждый из 10 последних дней возникновения такого события – 5 самых длительных событий за последние 365 дней 	<ul style="list-style-type: none"> – и введенную в начале и/или в конце события, и ее (их) поколение – число аналогичных событий за указанный день – дата и время начала события – дата и время окончания события – тип карточки (карточек), номер, Договаривающая сторона, выдавшая любую карточку, введенную в начале и/или конце события – число аналогичных событий за указанный день
Ошибочные данные о движении	<ul style="list-style-type: none"> – самое длительное событие за каждый из 10 последних дней возникновения такого события – 5 самых длительных событий за последние 365 дней 	<ul style="list-style-type: none"> – дата и время начала события – дата и время окончания события – тип карточки (карточек), номер, государство-член, выдавшее Договаривающая сторона, выдавшая любую карточку, вставленную в начале и/или конце события – число аналогичных событий за указанный день
Противоречивые данные о движении транспортного средства	<ul style="list-style-type: none"> – самое длительное событие за каждый из 10 последних дней возникновения такого события – 5 самых длительных событий за последние 365 дней 	<ul style="list-style-type: none"> – дата и время начала события – дата и время окончания события – тип карточки (карточек), номер, государство-член, выдавшее Договаривающая сторона, выдавшая любую карточку, введенную в начале и/или конце события – число аналогичных событий за указанный день
Попытка нарушения системы защиты	<ul style="list-style-type: none"> – 10 самых последних событий по типу события 	<ul style="list-style-type: none"> – дата и время начала события (если применимо) – дата и время окончания события – тип карточки (карточек), номер, государство-член, выдавшее Договаривающая сторона, выдавшая любую карточку, вставленную в начале и/или конце события, и ее (их) поколение – тип события
Нестыковка по времени	<ul style="list-style-type: none"> – самое продолжительное самое продолжительное серьезное событие за каждый из 10 последних дней возникновения такого события (т. е. те, в случае которых была наибольшая разница между датой и временем, отображенным контрольным устройством, 	<ul style="list-style-type: none"> – дата и время, указанные на записывающем оборудовании контрольном устройстве – дата и время по ГНСС – тип карточки (карточек), номер, государство-член, выдавшее Договаривающая сторона, выдавшая любую карточку,

<i>Событие</i>	<i>Правила хранения</i>	<i>Данные по каждому событию, подлежащие записи</i>
Аномалия ГНСС	и датой и временем, выданным ГНСС)	введенную в начале и/или конце события
	– 5 самых длительных серьезных событий за последние 365 дней	– число аналогичных событий за указанный день
	– самое длительное событие за каждый из 10 последних дней возникновения такого события	– дата и время начала события – дата и время окончания события – тип карточки (карточек), номер, Договаривающая сторона, выдавшая любую карточку, введенную в начале и/или конце события, и поколение этой карточки
	– 5 самых длительных событий за последние 365 дней	– число аналогичных событий за указанный день

1) ~~Записывающее оборудование~~ **Контрольное устройство** в своем блоке памяти также регистрирует и хранит следующие данные:

- дата и время последнего КОНТРОЛЯ ЗА ПРЕВЫШЕНИЕМ СКОРОСТИ;
- дата и время первого превышения скорости после данного КОНТРОЛЯ ЗА ПРЕВЫШЕНИЕМ СКОРОСТИ;
- число случаев превышения скорости после последнего КОНТРОЛЯ ЗА ПРЕВЫШЕНИЕМ СКОРОСТИ.

2) Эти данные могут регистрироваться только при восстановлении электропитания, при том, что время должно быть известно с точностью до минуты.

3.12.9 Данные о неисправностях

Для целей настоящего подпункта время регистрируется с точностью до 1 секунды.

118) ~~Записывающее оборудование~~ **Контрольное устройство** в своем блоке памяти регистрирует и хранит следующие данные по каждому обнаруженному событию в соответствии с указанными ниже правилами хранения:

<i>Неисправность</i>	<i>Правила хранения</i>	<i>Данные, подлежащие записи по каждой неисправности</i>
Неисправность в работе карточки	– 10 последних неисправностей в работе карточки водителя	– дата и время начала неисправности – дата и время окончания неисправности – тип карточки (карточек), номер, государство-член, выдавшее Договаривающаяся сторона, выдавшая карточку, и поколение карточки
Неисправности в работе записывающего оборудования контрольного устройства	– 10 самых последних неисправностей по каждому типу неисправности – первая неисправность после последней калибровки	– дата и время начала неисправности – дата и время окончания неисправности – тип неисправности – тип, карточки (карточек), номер и государство-член, выдавшее Договаривающаяся сторона, выдавшая карточку, и поколение любой карточки, введенной в начале и/или конце неисправности

3.12.10 Данные калибровки

119) ~~Занимающее оборудование~~ **Контрольное устройство** в своем блоке памяти также регистрирует и хранит следующие данные:

- известные параметры калибровки в момент активации;
- самая первая калибровка после активации;
- первая калибровка на данном транспортном средстве (идентифицируемом с помощью его опознавательного номера VIN);
- самые последние 20 калибровок (если несколько калибровок производятся в течение одного календарного дня, то сохраняются данные только по первой и последней калибровке в указанный день).

120) По каждой из этих калибровок регистрируются следующие данные:

- цель калибровки (активация, первая установка, установка, периодическая инспекция);
- название и адрес мастерской;
- номер карточки мастерской, ~~государство-член, —~~ **выданное Договаривающаяся сторона, выдавшая** карточку, и дата истечения срока действия карточки;
- идентификационные данные транспортного средства;
- обновленные или подтвержденные параметры: w, k, l, размер шин, регулировка устройства ограничения скорости, счетчик пробега (прежние и новые показания), дата и время (прежние и новые значения);
- типы и идентификаторы всех наложенных пломб;
- **серийные номера датчика движения, внешнего устройства ГНСС (в случае наличия) и внешнего средства удаленной связи (в случае наличия);**
- **тип груза по умолчанию, связанный с транспортным средством (либо товары, либо пассажиры);**
- **страна, в которой была выполнена калибровка, а также дата и время, когда местоположение, использованное для определения этой страны, было выдано приемником ГНСС.**

121) Кроме того, ~~занимающее оборудование~~ **контрольное устройство** регистрирует и хранит в своем блоке памяти данные о своей способности использовать карточки тахографов первого поколения (все еще действительные или уже нет).

122) Датчик движения регистрирует и хранит в своем блоке памяти следующие данные об установке:

- первое подключение к БУ (дата, время, номер официального утверждения БУ, серийный номер БУ);
- последнее подключение к БУ (дата, время, номер официального утверждения БУ, серийный номер БУ).

123) Внешнее устройство ГНСС регистрирует и хранит в своем блоке памяти следующие данные об установке:

- первое подключение к БУ (дата, время, номер официального утверждения БУ, серийный номер БУ);
- последнее подключение к БУ (дата, время, номер официального утверждения БУ, серийный номер БУ).

3.12.11 Данные корректировки времени

124) ~~Записывающее оборудование~~ **Контрольное устройство** записывает и хранит в своем блоке памяти данные, связанные с корректировкой времени, выполненной в режиме калибровки вне плана регулярной калибровки (определение в пункте f):

- последняя корректировка времени;
- 5 самых существенных корректировок времени.

125) По каждой из этих корректировок времени регистрируются следующие данные:

- дата и время, прежнее значение;
- дата и время, новое значение;
- название и адрес мастерской;
- номер карточки мастерской, ~~государство-член, —~~ **выдавшее Договаривающаяся сторона, выдавшая** карточку, поколение карточки и дата истечения срока действия карточки.

3.12.12 Данные о работе по контролю

126) ~~Записывающее оборудование~~ **Контрольное устройство** записывает и хранит в своем блоке памяти следующие данные о 20 последних операциях по контролю:

- дата и время контроля;
- номер карточки контролера, ~~государство-член, —~~ **выдавшее Договаривающаяся сторона, выдавшая** карточку, и поколение карточки;
- тип контроля (вывод на дисплей и/или на печать и/или загрузка данных с БУ и/или загрузка с карточки и/или проверка калибровки на дорогах).

127) В случае загрузки данных регистрируются также даты самого давнего и самого последнего дня загрузки.

3.12.13 Данные блокировки, установленной предприятием

128) ~~Записывающее оборудование~~ **Контрольное устройство** записывает и хранит в своем блоке памяти следующие данные о 255 последних операциях по контролю:

- дата и время блокировки;
- дата и время разблокировки;
- номер карточки предприятия, ~~государство-член, —~~ **выдавшее Договаривающаяся сторона, выдавшая** карточку, и поколение карточки;
- название и адрес предприятия.

Данные, ранее заблокированные посредством блокировки, которые удалены из памяти вследствие превышения установленного предела, считаются незаблокированными.

3.12.14 Данные о работе по загрузке

129) ~~Записывающее оборудование~~ **Контрольное устройство** регистрирует и хранит в своем блоке памяти следующие данные о последней загрузке из блока памяти на внешние носители в режиме предприятия или калибровки:

- дата и время загрузки;
- номер карточки предприятия или мастерской, ~~государство-член, —~~ **выдавшее Договаривающаяся сторона, выдавшая** карточку, и поколение карточки;
- название предприятия или мастерской.

3.12.15 Данные об особых условиях

130) ~~Записывающее оборудование~~ **Контрольное устройство** записывает и хранит в своем блоке памяти следующие данные, имеющие отношение к конкретным условиям:

- дата и время записи;
- тип особого условия.

131) Блок памяти данных способен хранить данные об особых условиях не менее 365 дней (в предположении, что в среднем ежедневно открывается и закрывается одна позиция, указывающая на особое условие). Когда объем памяти заполнен, новые данные записываются поверху самых старых данных.

3.12.16 Данные карточек тахографов

132) ~~Записывающее оборудование~~ **Контрольное устройство** способно хранить следующие данные, связанные с различными карточками тахографов, использовавшихся в БУ:

- номер и серийный номер карточки тахографа;
- изготовитель карточки тахографа;
- тип карточки тахографа;
- версия карточки тахографа.

133) ~~Записывающее оборудование~~ **Контрольное устройство** способно хранить не менее 88 таких записей.

3.12.17 Пересечение границ

133а) **Записывающее оборудование регистрирует и хранит в своем блоке памяти следующую информацию о пересечении границы:**

- страна, которую покидает транспортное средство;
- страна, в которую въезжает транспортное средство;
- местоположение, в котором транспортное средство пересекло границу.

133б) **Вместе с каждым местоположением записывающее оборудование регистрирует и хранит в своем блоке памяти следующие данные:**

- номер карточки водителя (второго водителя) и название Договаривающейся стороны, выдавшей карточку;
- поколение карточки;
- соответствующие данные о точности, дате и времени ГНСС;
- метка, указывающая на то, было ли аутентифицировано данное местоположение;
- показания счетчика пробега транспортного средства на момент обнаружения факта пересечения границы.

133с) Блок памяти способен хранить данные о пересечении границы в течение не менее 365 дней.

133д) Когда объем памяти заполнен, новые данные записываются поверху самых старых данных.

3.12.18 Операции по загрузке/разгрузке

133е) **Контрольное устройство записывает и хранит в своем блоке памяти следующую информацию об операциях по загрузке и разгрузке транспортного средства:**

- тип операции (загрузка, разгрузка или одновременная загрузка/разгрузка);
- местоположение, в котором произведена операция загрузки/разгрузки.

133f) Если местоположение транспортного средства на момент загрузки и разгрузки приемник ГНСС не выдает, то контрольное устройство использует данные последнего зарегистрированного места и соответствующую дату и время.

133g) Вместе с каждым типом операции и местоположением контрольное устройство записывает и хранит в своем блоке памяти следующие данные:

- номер карточки водителя и/или второго водителя и название Договаривающейся стороны, выдавшей карточку;
- поколение карточки;
- дата и время операции по загрузке/разгрузке;
- соответствующие данные о точности, дате и времени ГНСС, в случае применимости;
- метка, указывающая на то, было ли аутентифицировано данное местоположение;
- показания счетчика пробега транспортного средства.

133h) Блок памяти данных способен хранить данные об операциях по загрузке/разгрузке в течение не менее 365 календарных дней.

133i) Когда объем памяти заполнен, новые данные записываются поверху самых старых данных.

3.12.19 Цифровая карта

133j) Для регистрации положения транспортного средства при пересечении границы соответствующей страны записывающее устройство хранит в своей памяти данных соответствующую цифровую карту.

133k) Доступ к разрешенным цифровым картам для поддержки функции мониторинга пересечения границы записывающим устройством обеспечивается лабораторией, ответственной за проведение испытаний на эксплуатационную совместимость, для загрузки со специального защищенного веб-сайта в различных форматах.

133l) Для каждой из этих карт на веб-сайте обеспечивается доступ к соответствующему идентификатору версии и соответствующему хэш-значению.

133m) На картах отображаются следующие позиции:

- уровень разрешения, соответствующий уровню НТЕС-0, согласно Номенклатуре территориальных единиц для статистики;
- масштаб 1:1 млн.

133n) Изготовители тахографов выбирают соответствующую карту на веб-сайте и загружают ее в безопасном режиме.

133o) Изготовители тахографов используют загруженную с веб-сайта карту только после проверки ее целостности с помощью хэш-значения карты.

133p) Выбранная карта вводится в контрольное устройство его изготовителем в соответствующем формате, но семантика введенной карты остается неизменной.

133q) Изготовитель также хранит идентификатор версии карты, используемой в контрольном устройстве.

133r) Возможно обновление или замена сохраненной цифровой карты на новую, предоставляемую лабораторией, компетентной в вопросах проведения испытаний на совместимость.

133s) Обновление цифровых карт производится с помощью механизмов обновления программного обеспечения, установленных изготовителем, в соответствии с требованиями 226d и 226e, с тем чтобы контрольное устройство могло проверить аутентичность и целостность новой введенной карты, прежде чем сохранить ее и заменить предыдущую.

133t) Изготовители тахографов могут добавлять к базовой карте, упомянутой в требовании (133m), дополнительную информацию для иных целей, помимо регистрации пересечения границ, например, информацию о границах регионов Договаривающихся сторон, при условии, что семантика основной карты не изменяется.

3.13 Считывание данных с карточек тахографов

134) ~~Записывающее оборудование~~ **Контрольное устройство** в определенных условиях способно считывать с карточек тахографов первого и второго поколений необходимые данные с целью:

- установить тип карточки, держателя карточки, ранее использованное транспортное средство, дату и время последнего извлечения карточки и вид деятельности, выбранный в тот момент времени;
- проверить правильность завершения последнего сеанса использования карточки;
- рассчитать непрерывное время управления транспортным средством водителем, накопленное время перерывов и накопленное время управления за предыдущую и текущую неделю;
- вывести на печать требуемые данные, записанные на карточке водителя;
- загрузить данные с карточки водителя на внешний носитель.

Данное требование применимо только к карточкам тахографов первого поколения, если мастерская не отказалась от их использования.

135) В случае ошибки при считывании ~~записывающее оборудование~~ **контрольное устройство** производит очередную попытку (максимум три раза) выполнить ту же команду на считывание данных, после чего сообщает, если считать данные не удалось, что карточка неисправна и недействительна.

135a) Структура в приложении «TACHO_G2» зависит от версии. Карточки версии 2 содержат дополнительные элементарные файлы к карточкам версии 1, в частности:

- в карточках водителей и мастерских:
 - позиция EF Places_Authentication содержит статус аутентификации местоположений транспортных средств, хранящихся в файле EF Places. С каждым статусом аутентификации сохраняется временная метка, которая должна точно совпадать с датой и временем записи, сохраненной в соответствующей позиции в файле EF Places;
 - позиция EF GNSS_Places_Authentication содержит статус аутентификации местоположений данного транспортного средства, хранящихся в файле EF GNSS_Places. С каждым статусом аутентификации сохраняется временная метка, которая должна точно совпадать с датой и временем записи, сохраненной в соответствующей позиции в файле EF Places;

- позиции EF Border_Crossings, EF Load_Unload_Operations и EF Load_Type_Entries содержат данные, связанные с пересечением границ, операциями загрузки/разгрузки и типами грузов;
- в карточках мастерской:
 - позиция EF Calibration_Add_Data содержит дополнительные данные калибровки к тем из них, которые хранятся в файле EF Calibration. Прежнее значение даты и времени и идентификационный номер транспортного средства сохраняются с каждой дополнительной записью данных калибровки, которые должны быть точно такими же, как и прежние значения даты и времени и идентификационный номер транспортного средства, сохраненные вместе с соответствующими данными калибровки в файле EF Calibration;
- во всех карточках тахографа:
 - позиция EF VU_Configuration содержит настройки, относящиеся конкретно к тахографу держателя карточки.

Бортовое устройство игнорирует любой статус аутентификации, выявленный в позиции EF Places_Authentication или EF GNSS_Places_Authentication, если в файле EF Places или EF GNSS_Places местоположение транспортного средства с той же временной меткой не выявлено.

Бортовое устройство игнорирует файл «EF VU_Configuration» во всех карточках по той причине, что в случае использования такого элементарного файла никакие специальные правила не предусмотрены. Эти правила устанавливаются посредством внесения соответствующей поправки в добавление 1С, которая должна включать изменение или исключение данного пункта.

3.14 Регистрация и хранение данных на карточках тахографов

3.14.1 Регистрация и хранение данных на карточках тахографа первого поколения

136) При условии, что мастерская не отказалась от использования карточек тахографов первого поколения, ~~записывающее оборудование~~ **контрольное устройство** регистрирует и хранит данные так же, как и ~~записывающее оборудование~~ **контрольное устройство** первого поколения.

137) ~~Записывающее оборудование~~ **Контрольное устройство** записывает «данные о сеансе использования карточки» на карточке водителя или мастерской сразу же после ее ввода.

138) ~~Записывающее оборудование~~ **Контрольное устройство** обновляет данные, хранящиеся на действительных карточках водителя, мастерской предприятия и/или контролера, со всеми необходимыми данными, относящимися к периоду, в течение которого карточка была введена в устройство, и к держателю карточки. Данные, хранящиеся на этих карточках, указаны в главе 4.

139) ~~Записывающее оборудование~~ **Контрольное устройство** обновляет данные о деятельности водителя и местах (как указано в пунктах 4.5.3.1.9 и 4.5.3.1.11), хранящиеся на действительной карточке водителя и/или мастерской, с учетом данных о видах деятельности и местах, введенных держателем карточки вручную.

140) Все события и неисправности, не определенные для ~~записывающего оборудования~~ **контрольного устройства** первого поколения, на карточках водителя и мастерской не хранятся.

141) Порядок обновления данных на карточках тахографа должен быть таким, чтобы в случае необходимости и с учетом фактического объема памяти хранения последние данные записывались поверху самых старых данных.

142) В случае ошибки в процессе записи ~~записывающее оборудование~~ **контрольное устройство** производит очередную попытку (максимум три раза) выполнения той же команды записи данных, после чего сообщает, если записать данные не удалось, что карточка неисправна и недействительна.

143) До извлечения карточки водителя или мастерской и после сохранения на ней всех соответствующих данных ~~записывающее оборудование~~ **контрольное устройство** приводит «данные о сеансе использования карточки» в исходное состояние.

3.14.2 Регистрация и хранение данных на карточках тахографа второго поколения

144) Карточки тахографов второго поколения оснащены двумя приложениями, первое из которых точно такое же, как и приложение TACHO для карточек тахографов первого поколения, а второе — TACHO_G2, как описано в главе 4 и ~~приложении~~ **подразделе 2**.

Структура в приложении «TACHO_G» зависит от версии. Карточки версии 2 содержат элементарные файлы, дополнительные к тем, которые содержатся на карточках версии 1.

145) ~~Записывающее оборудование~~ **Контрольное устройство** записывает «данные о сеансе использования карточки» на карточке водителя или мастерской сразу же после ее ввода.

146) ~~Записывающее оборудование~~ **Контрольное устройство** обновляет данные, хранящиеся в двух приложениях действительных карточек водителя, мастерской, предприятия и/или контролера, со всеми необходимыми данными, относящимися к периоду, в течение которого карточка оставалась в устройстве, и к держателю карточки. Данные, хранящиеся на этих карточках, указаны в главе 4.

147) ~~Записывающее оборудование~~ **Контрольное устройство** обновляет данные о деятельности водителя и местах и местоположениях (как указано в пунктах 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 и 4.5.3.2.11), хранящиеся на действительной карточке водителя и/или мастерской, с учетом данных о видах деятельности и местах, введенных владельцем карточки вручную.

147а) При вводе карточки водителя или мастерской контрольное устройство сохраняет на карточке тип груза транспортного средства по умолчанию.

147б) При вводе карточки водителя или мастерской и после процедуры ручного ввода контрольное устройство проверяет последнее место начала или завершения ежедневного рабочего периода, записанного на карточке. Это место может быть временным, как указано в требовании 59. Если это место находится в иной стране, чем та, в которой в настоящее время находится транспортное средство, то контрольное устройство сохраняет на карточке запись о пересечении границы, с указанием:

- **страны, из которой выехал водитель: недоступно;**
- **страны, в которую въезжает водитель: страна, в которой находится транспортное средство в данный момент;**
- **даты и времени, когда водитель пересек границу: время ввода карточки;**
- **местоположения водителя при пересечении границы: недоступно;**
- **показания счетчика пробега транспортного средства: недоступно.**

148) Порядок обновления данных на карточках тахографа должен быть таким, чтобы в случае необходимости и с учетом фактического объема памяти хранения последние данные записывались поверху самых старых данных.

149) В случае ошибки при записи ~~записывающее оборудование~~ **контрольное устройство** производит очередную попытку (максимум три раза) выполнения той же команды записи данных, после чего сообщает, если записать данные не удалось, что карточка неисправна и недействительна.

150) До извлечения карточки водителя и после сохранения в двух ее приложениях всех соответствующих данных ~~записывающее оборудование~~ **контрольное устройство** приводит «данные о сеансе использования карточки» в исходное состояние.

150a) Бортовое устройство игнорирует элементарный файл «EF VU_Configuration» во всех карточках по той причине, что в случае использования такого элементарного файла никакие специальные правила не предусмотрены. Эти правила устанавливаются посредством внесения соответствующей поправки в добавление 1С, которая должна включать изменение или исключение данного пункта.

3.15 Вывод на дисплей

151) Вывод сообщения на дисплей включает не менее 20 знаков.

152) Минимальный размер знака — 5 мм в высоту и 3,5 мм в ширину.

153) Дисплей поддерживает знаки, указанные в ~~добавлении~~ **подразделе 1** главы 4 «Наборы символов». На дисплее могут использоваться упрощенные наборные знаки (например, ударные знаки могут отображаться без знака ударения или строчные буквы могут отображаться в виде заглавных).

154) Дисплей оснащается надлежащей неослепляющей подсветкой.

155) Индикация должна быть видимой вне контрольного устройства.

156) ~~Записывающее оборудование~~ **Контрольное устройство** способно отображать следующие данные:

- данные по умолчанию;
- данные о предупреждениях;
- данные о доступе к меню;
- другие данные, запрашиваемые пользователем.
- ~~Записывающее оборудование~~ **Контрольное устройство** может выводить на дисплей дополнительную информацию при условии, что ее можно четко отличить от информации, требуемой выше.

157) Дисплей ~~записывающего оборудования~~ **контрольного устройства** использует пиктограммы или комбинации пиктограмм, перечисленные в ~~добавлении~~ **подразделе 3**. На дисплей могут также выводиться дополнительные пиктограммы или комбинации пиктограмм при условии, что их можно четко отличить от пиктограмм или комбинаций пиктограмм, упомянутых выше.

158) Когда транспортное средство находится в процессе движения, дисплей всегда находится во включенном состоянии.

159) ~~Записывающее оборудование~~ **Контрольное устройство** может быть оснащено ручной или автоматической функцией, позволяющей отключать дисплей, когда транспортное средство остановлено.

Формат отображения данных указан в ~~добавлении~~ **подразделе 5**.

3.15.1 Индикация данных по умолчанию

160) Когда иную информацию на дисплей выводить не требуется, ~~занимающее оборудование~~ **контрольное устройство** отображает по умолчанию следующие данные:

- местное время (время UTC плюс корректировка на смещение, сделанная водителем);
- режим работы;
- текущий вид деятельности водителя и текущий вид деятельности второго водителя;
- информация, касающаяся водителя:
 - если текущим видом его деятельности является УПРАВЛЕНИЕ: текущее время непрерывного управления и текущая совокупная продолжительность перерывов,
 - если текущим видом его деятельности не является УПРАВЛЕНИЕ: продолжительность его текущей деятельности (с момента выбора этой функции) и текущая накопленная продолжительность перерывов.

161) Вывод на дисплей данных, относящихся к каждому водителю, должно быть четким, полным и однозначным. В том случае, если информацию, относящуюся к водителю и второму водителю, нельзя вывести на дисплей одновременно, ~~занимающее оборудование~~ **контрольное устройство** отображает информацию, относящуюся к водителю, и дает пользователю возможность выводить на дисплей информацию, относящуюся ко второму водителю.

162) В том случае, если ширина дисплея не позволяет по умолчанию отображать режим работы, ~~занимающее оборудование~~ **контрольное устройство** выводит на дисплей кратковременное сообщение с указанием нового режима работы в момент его изменения.

163) ~~Занимающее оборудование~~ **Контрольное устройство** выводит на дисплей кратковременное сообщение с указанием фамилии держателя карточки в момент ее ввода.

164) Когда открывается позиция «OUT OF SCOPE» (НЕПРИМЕНИМО) или «FERRY/TRAIN» (ПАРОМ/ПОЕЗД), на дисплее отображается — по умолчанию, с использованием соответствующей пиктограммы — тот факт, что эта позиция открыта (при этом допускается, что текущий вид деятельности водителя в это время может не отображаться).

3.15.2 Вывод на дисплей предупреждения

165) ~~Занимающее оборудование~~ **Контрольное устройство** выводит на дисплей предупреждающую информацию с использованием прежде всего пиктограмм, указанных в ~~добавлении~~ **подразделе 3**, дополненных, в случае необходимости, другой информацией в виде числового кода. Кроме того, может быть включено текстовое описание предупреждения на языке, выбранном водителем.

3.15.3 Доступ к меню

166) ~~Занимающее оборудование~~ **Контрольное устройство** содержит необходимые команды, подаваемые с использованием соответствующего меню.

3.15.4 Другие отображаемые данные

167) По соответствующему запросу на дисплей на выборочной основе можно выводить следующие данные:

- дата и время UTC с корректировкой на местное время;

- содержание любой из ~~шести~~ распечаток, **перечисленных в требовании 169**, в том же формате, что и сами распечатки;
- продолжительность управления и ~~ежедневное~~ **накопленное** время перерывов в работе водителя;
- продолжительность управления и ~~ежедневное~~ **накопленное** время перерывов в работе второго водителя;
- ~~ежедневное~~ **накопленное** время управления водителем за предыдущую и текущую недели;
- ~~ежедневное~~ **накопленное** время управления вторым водителем за предыдущую и текущую неделю;
- факультативно:
- продолжительность текущей деятельности второго водителя (с момента выбора этой функции);
- ~~ежедневное~~ **накопленное** время управления водителем за текущую неделю;
- ~~ежедневное~~ **накопленное** время управления вторым водителем за текущий ежедневный период работы;
- накопленное время управления водителем за текущий ежедневный период работы.

168) Вывод на дисплей содержания распечаток производится в последовательном порядке построчно. Если ширина дисплея составляет менее 24 знаков, пользователь может просматривать полную информацию в соответствующей форме (несколько строк, прокрутка, ...). **Строки распечатки, предназначенные для внесения информации вручную, на дисплей могут не выводиться.** ~~Строки распечатки, предназначенные для внесения информации вручную, на дисплей могут не выводиться.~~

3.16 Вывод на печать

169) ~~Записывающее оборудование~~ **Контрольное устройство** способно выводить на печать информацию, содержащуюся в его памяти и/или на карточках тахографа, в виде следующих шести видов распечаток:

- ежедневная распечатка данных о деятельности водителя, записанных на карточке;
- ежедневная распечатка данных о деятельности водителя, записанных в бортовом устройстве;
- распечатка данных о событиях и неисправностях, хранящихся на карточке;
- распечатка данных о событиях и неисправностях, хранящихся в бортовом устройстве;
- распечатка технических данных;
- распечатка данных о превышении скорости;
- хронологическая последовательность данных на карточке тахографа в связи с данным БУ (см. главу 3.12.16);
- детальный формат и содержание этих распечаток указываются в ~~добавлении~~ **подразделе 4**.

В конце распечаток могут содержаться дополнительные данные.

~~Записывающим оборудованием~~ **Контрольным устройством** могут также выдаваться дополнительные распечатки, если они четко отличаются от семи распечаток, упомянутых выше.

170) «Ежедневная распечатка данных о деятельности водителя, записанных на карточке» и «распечатка данных о событиях и неисправностях, записанных на карточке» выдается только в том случае, если в ~~записывающее оборудование~~ **контрольное устройство** введена карточка водителя или карточка мастерской. До выдачи распечатки ~~записывающее оборудование~~ **контрольное устройство** обновляет данные, содержащиеся в памяти соответствующей карточки.

171) Для того чтобы сделать «ежедневную распечатку данных о деятельности водителя, записанных на карточке» или «распечатку данных о событиях и неисправностях, записанных на карточке», ~~записывающее оборудование~~ **контрольное устройство**:

- автоматически выбирает карточку водителя или карточку мастерской, если в устройство вставлена только одна из этих карточек;
- или предусматривает команду, позволяющую выбрать исходную карточку или карточку, вставленную в считывающее устройство водителя, если в ~~записывающее оборудование~~ **контрольное устройство** вставлены обе эти карточки.

172) Принтер способен печатать 24 знака в строке.

173) Минимальный размер знака — 2,1 мм в высоту и 1,5 мм в ширину.

174) Принтер поддерживает знаки, указанные в главе 4 ~~добавления~~ **подраздела 1** «Наборы знаков».

175) Принтеры сконструированы таким образом, что они могут выдавать эти распечатки с такой разрешающей способностью, которая исключала бы двоякое толкование при их чтении.

176) Распечатки сохраняют свои размеры и содержащиеся в них данные в нормальных условиях влажности (10–90 %) и температуры.

177) На бумаге утвержденного типа, используемой ~~записывающим оборудованием~~, **контрольным устройством**, нанесен соответствующий знак официального утверждения типа и указание типа (типов) ~~записывающего оборудования~~ **контрольного устройства**, на котором она может использоваться.

178) Распечатки остаются легко читаемыми и распознаваемыми в обычных условиях хранения (интенсивность света, влажность и температура) в течение не менее двух лет.

179) Распечатки соответствуют, как минимум, тестовым спецификациям, указанным в ~~приложении~~ **подразделе 9**.

180) Кроме того, предусматривается возможность включения в эти документы примечаний, написанных от руки, например подписи водителя.

181) В том случае, если во время распечатки закончилась бумага, ~~записывающее оборудование~~ **контрольное устройство** возобновляет печатание после загрузки бумаги с начала распечатки или продолжает печатание с четкой ссылкой на ту часть, которая была выдана на печать ранее.

3.17 Сигналы предупреждения

182) ~~Записывающее оборудование~~ **Контрольное устройство** предупреждает водителя в случае обнаружения любого события и/или неисправности.

183) Предупреждение о прекращении электропитания может подаваться с задержкой до тех пор, пока электропитание не будет восстановлено.

184) ~~Записывающее—оборудование~~ **Контрольное устройство** предупреждает водителя за 15 минут до момента и в тот момент, когда непрерывное время управления превышает максимально допустимое значение.

185) Предупреждения должны быть визуальными. В дополнение к визуальным предупреждениям могут также предусматриваться звуковые предупреждения.

186) Визуальные предупреждения четко распознаются пользователем, располагаются в поле визуального восприятия водителя и удобочитаемы как в дневное, так и в ночное время.

187) Система визуального предупреждения может быть встроена в ~~записывающее оборудование~~ **контрольное устройство** и/или вынесена за его пределы.

188) В последнем случае на нем ставится пометка в виде буквы «Т».

189) Предупреждения подаются в течение как минимум 30 секунд, если только пользователь не нажимает на любую клавишу или несколько конкретных клавиш ~~записывающего—оборудования~~ **контрольного устройства** для подтверждения того, что он принял предупреждение к сведению. Это первое подтверждение не влечет за собой удаление выведенной на дисплей причины, указанной в следующем пункте.

190) Причина предупреждения выводится на дисплей ~~записывающего—оборудования~~ **контрольного устройства** и остается видимой до тех пор, пока пользователь не введет специальный код или команду на ~~записывающем—оборудовании~~ **контрольном устройстве**.

191) В этой связи могут предусматриваться дополнительные предупреждения, если они не вводят водителей в заблуждение по поводу предупреждений, определенных выше.

3.18 Загрузка данных на внешние носители

192) ~~Записывающее—оборудование~~ **Контрольное устройство** способно по команде загружать данные из своей памяти или с карточки водителя на внешние носители через разъем калибровки/загрузки. До начала загрузки ~~записывающее—оборудование~~ **контрольное устройство** обновляет данные, содержащиеся в памяти соответствующей карточки.

193) В дополнение и в качестве факультативной функции ~~записывающее оборудование~~ **контрольное устройство** в любом режиме работы может загружать данные в базу данных предприятия, идентифицированного по этому каналу связи, через любой другой ~~интерфейс разъем~~. В подобном случае к этой операции загрузки применяются права доступа к данным в режиме предприятия.

194) Загрузка не приводит к изменению или удалению любых сохраненных данных.

195) Электрический разъем калибровочного/загрузочного интерфейса определяется в ~~добавлении~~ **подразделе 6**.

196) Протоколы загрузки определяются в ~~добавлении~~ **подразделе 7**.

196а) Транспортное предприятие, которое эксплуатирует транспортные средства, оснащенные контрольным устройством, соответствующим настоящему добавлению, обеспечивает загрузку всех данных с бортового устройства и карточек водителя.

Максимальный период, в течение которого загружаются соответствующие данные, не должен превышать:

- **90 дней для данных, загружаемых с бортового устройства;**
- **28 дней для данных, загружаемых с карточки водителя.**

196b) Транспортные предприятия хранят данные, загруженные с бортового устройства и карточки водителя, в течение не менее двенадцати месяцев после записи.

3.19 Удаленная связь для целевых проверок на дорогах

197) При включенном зажигании бортовое устройство сохраняет в устройстве удаленной связи через каждые 60 секунд самые свежие данные для целевых проверок на дорогах. Такие данные шифруются и защищаются подписью, как описано в ~~добавлении~~ **подразделе 11 и подразделе 14.**

198) Данные, которые проверяются на удалении, передаются в считывающие устройства удаленной связи с помощью беспроводных средств, как описано в ~~добавлении~~ **подразделе 14.**

199) Данные, необходимые для целевых проверок на дорогах:

- самая последняя попытка нарушения системы защиты;
- самое продолжительное прекращение электропитания;
- неисправность датчика;
- ошибочные данные о движении;
- противоречивые данные о движении транспортного средства;
- управление без действительной карточки;
- ввод карточки во время управления;
- данные о корректировке времени;
- данные о калибровке, включая даты двух последних сохраненных записей калибровки;
- регистрационный номер транспортного средства;
- скорость, зарегистрированная тахографом;
- **местоположение транспортного средства;**
- **указание на то, может ли водитель в данный момент нарушить временной режим управления.**

3.20 ~~Вывод данных на дополнительные внешние устройства~~ Обмен данными с дополнительными внешними устройствами

200) ~~Записывающее оборудование~~ **Контрольное устройство** также оснащается стандартизированными интерфейсами(ом) ИТС в соответствии с **подразделом 13**, позволяющими использовать данные, записанные или выдаваемые тахографами или карточками тахографов, ~~в оперативном режиме на внешнем устройстве.~~

В рабочем режиме для передачи личных данных через интерфейс ИТС требуется согласие водителя. Тем не менее согласие водителя не распространяется на данные тахографа или карточки, доступ к которым осуществляется в режиме контроля, предприятия или калибровки. Права доступа к данным и соответствующим функциям в случае этих режимов указаны в требованиях 12 и 13.

К данным ИТС, доступным через этот интерфейс, применяются следующие требования:

- личные данные должны быть доступны только после получения поддающегося проверке согласия водителя, допускающего, что личные данные могут быть извлечены из бортовой сети транспортного средства.

Соответствующий набор отобранных существующих данных, которые могут быть доступны через интерфейс ИТС, и классификация данных в качестве как личных, так и неличных указаны в подразделе 13. В дополнение к набору данных, представленных в подразделе 13 добавления, могут быть также извлечены соответствующие дополнительные данные. Изготовитель БУ классифицирует эти данные как «личные» или «неличные», при том, что согласие водителя требуется применительно только к тем данным, которые классифицируются как «личные»:

- согласие водителя можно активировать или отменить в любой момент при помощи команд в меню, при условии, что карточка водителя введена;
- в любом случае наличие интерфейса ИТС не должно нарушать надлежащее функционирование и безопасность бортового устройства или воздействовать на него.

Дополнительные интерфейсы бортовых устройств могут использоваться одновременно при условии, что они полностью соответствуют требованиям подраздела 13 в части согласия водителя. Контрольное устройство должно иметь возможность передавать статус согласия водителя на другие платформы в бортовой сети транспортного средства и на внешние устройства.

В случае личных данных, введенных в бортовую сеть транспортного средства, которые в дальнейшем обрабатываются вне бортовой сети этого транспортного средства, изготовитель тахографа не несет ответственность за соответствие обработки этих неличных данных действующему в ЕС законодательству о защите данных.

Интерфейс ИТС также обеспечивает возможность ввода данных во время процедуры ручного ввода в соответствии с требованием 61 как водителем, так и вторым водителем.

Интерфейс ИТС можно также использовать для ввода в режиме реального времени дополнительной информации, такой как:

- выбор деятельности водителя в соответствии с требованием 46;
- места в соответствии с требованием 56;
- особые условия в соответствии с требованием 62;
- операции по загрузке/разгрузке в соответствии с требованием 62а.

Эта информация также может быть введена с помощью других интерфейсов.

~~В приложении подразделе 13 добавления описан стандартизированный факультативный интерфейс ИТС. Могут использоваться и другие похожие интерфейсы, если они полностью соответствуют требованиям приложения подраздела 13 добавления с точки зрения перечня минимальных данных, безопасности и согласия водителя.~~

~~Согласие водителя не распространяется на данные, передаваемые контрольным устройством в бортовую сеть. В случае, если личные данные, введенные в сеть транспортного средства, в дальнейшем обрабатываются вне сети транспортного средства, изготовитель транспортного средства несет ответственность за то, чтобы эта обработка личных данных соответствовала законодательству о защите личных данных, действующему на территории Договаривающихся сторон, и Конвенции о защите физических лиц при автоматизированной обработке личных данных. Согласие водителя также не распространяется на данные тахографа, направленные в удаленное предприятие (требование 193), поскольку этот сценарий контролируется правом доступа к карточке предприятия.~~

~~К данным ИТС, доступным через этот интерфейс, применяются следующие требования:~~

- ~~— эти данные представляют собой набор отдельных существующих данных из словаря данных тахографов (приложение **подраздел 1 добавления**);~~
- ~~— подмножество таких избранных данных помечается как «личные данные»;~~
- ~~— подмножество «личные данные» доступно только при наличии поддающегося проверке согласия водителя, подтверждающего, что его личные данные могут покинуть сеть транспортного средства;~~
- ~~— согласие водителя можно активировать или отменить в любой момент при помощи команд в меню, при условии, что карточка водителя введена;~~
- ~~— множество и подмножество данных передается через протокол беспроводной связи «Bluetooth» в радиусе кабины транспортного средства с частотой обновления 1 минута;~~
- ~~— соединение внешнего устройства с интерфейсом ИТС защищено отдельным произвольным ПИН-кодом, состоящим не меньше, чем из 4 цифр, который записан и доступен через дисплей каждого бортового устройства;~~
- ~~— в любом случае наличие интерфейса ИТС не должно нарушать надлежащее функционирование и безопасность бортового устройства или воздействовать на него.~~

~~Помимо набора избранных существующих данных, представляющих собой минимальный перечень, также могут выводиться другие данные, если они не могут рассматриваться как личные данные.~~

~~Записывающее оборудование **Контрольное устройство** уведомляет другие внешние устройства о том, что у него есть **согласие на передачу** статуса согласия водителя **другим платформам в пределах бортовой сети транспортных средств**.~~

~~Когда зажигание транспортного средства включено, эти данные должны передаваться постоянно.~~

201) Интерфейс последовательного канала, как указано в **Приложении добавления 1В к Регламенту (ЕЭС) N 3821/85** **настоящему Соглашению** с последними изменениями, может и впредь использоваться для оснащения тахографов в порядке обратной совместимости. **Последовательный канал классифицируется как часть бортовой сети транспортного средства в соответствии с требованием 200.** Однако в случае передачи личных данных все равно требуется согласие водителя.

3.21 Калибровка

202) Функция калибровки позволяет:

- автоматически подсоединять датчик движения к БУ;
- автоматически подсоединять внешнее устройство ГНСС к БУ, в случае применимости;
- приводить в цифровой форме постоянную величину **записывающего оборудования контрольного устройства (k)** в соответствии с характеристическим коэффициентом транспортного средства (w);
- корректировать текущее время в пределах срока действия введенной карточки мастерской;
- корректировать текущие показания счетчика пробега;
- обновлять идентификационные данные датчика движения, записанные в блоке памяти;

- обновлять, в случае применимости, идентификационные данные внешнего устройства ГНСС, записанные в блоке памяти;
- обновлять типы и идентификаторы всех наложенных пломб;
- обновлять или подтверждать другие параметры, заложенные в ~~записывающем~~ ~~оборудовании~~ **контрольном устройстве**: идентификационные данные транспортного средства, показатели w и l , размер шин и регулировку устройства ограничения скорости (в случае применимости) **и тип груза по умолчанию**;
- **сохранять в автоматическом режиме название страны, в которой была выполнена калибровка, и время на дату выдачи местоположения, использованного для определения данной страны, приемником ГНСС.**

203) Кроме того, функция калибровки позволяет отказаться от использования карточек тахографов первого поколения в ~~записывающем~~ ~~оборудовании~~ **контрольном устройстве**, если выполняются условия, изложенные в ~~приложении~~ **подразделе 15**.

204) Сопряжение датчика движения с БУ заключается, как минимум, в:

- обновлении данных установки датчика движения, содержащихся в памяти датчика движения (при необходимости);
- копировании из блока памяти датчика движения в блок памяти БУ необходимых идентификационных данных датчика движения.

205) Сопряжение внешнего устройства ГНСС с БУ заключается, как минимум, в:

- обновлении данных об установке внешнего устройства ГНСС, содержащихся в блоке памяти внешнего устройства ГНСС (при необходимости);
- копировании необходимых идентификационных данных внешнего устройства ГНСС, включая его серийный номер, из блока памяти внешнего устройства ГНСС в блок памяти БУ.

~~После подсоединения проводитея проверка информации ГНСС о местоположении.~~

206) Функция калибровки обеспечивает ввод необходимых данных с помощью калибровочного/загрузочного разъема в соответствии с протоколом калибровки, определенным в ~~добавлении~~ **подразделе 8**. Функция калибровки может также обеспечивать ввод необходимых данных с помощью других разъемов.

3.22 Проверка калибровки на дорогах

207) Функция проверки калибровки на дорогах позволяет считывать серийный номер датчика движения (возможно, встроенный в адаптер) и серийный номер внешнего устройства ГНСС (в случае применимости), соединенного с бортовым устройством, в момент запроса.

208) Такое считывание должно быть возможным, как минимум, с дисплея бортового устройства с помощью соответствующих команд в меню.

209) Функция проверки калибровки на дорогах также позволяет контролировать выбор режима калибровки ввода/вывода сигнальной линии калибровки ввода/вывода, как указано в ~~приложении~~ **подразделе 6**, через интерфейс К-линии. Это можно сделать с помощью функции «ECUAdjustmentSession» (сеанс корректировки ECUA), как описано в ~~приложении~~ **подразделе 8**, часть 7 «Настройка проверочных импульсов — Контрольный функциональный блок регулировки входного/выходного сигнала».

Если режим ввода/вывода сигнальной линии калибровки ввода/вывода активирован в соответствии с этим требованием, то предупреждение

«Управление без соответствующей карточки» (требование 75) бортовым устройством не активируется.

3.23 Корректировка времени

210) Функция корректировки времени позволяет автоматически корректировать текущее время. В ~~записывающем оборудовании~~ контрольном устройстве для корректировки времени используются два источника времени: 1) внутренние часы БУ и 2) приемник ГНСС.

211) Установка времени на внутренних часах БУ автоматически корректируется ~~с интервалами с разными временными интервалами не более 12 часов.~~ Следующая автоматическая повторная корректировка времени производится через 72–168 ч после предыдущей и после того, как БУ получит доступ к функции времени ГНСС с помощью действительного аутентифицированного сообщения о местоположении в соответствии с подразделом 12. Тем не менее корректировка времени ни в коем случае не должна быть больше, чем накопленное максимальное смещение времени за день, рассчитанное изготовителем БУ в соответствии с требованием 41b. Если разница между временем внутренних часов БУ и временем приемника ГНСС больше, чем накопленное максимальное смещение времени за день, то корректировка времени должна приблизить время внутренних часов БУ как можно ближе к времени приемника ГНСС. Установка времени может быть выполнена только в том случае, если время, выданное приемником ГНСС, получено с помощью аутентифицированных сообщений о местоположении в соответствии с подразделом 12. ~~Если эта задержка истекла и повторная корректировка невозможна из-за отсутствия сигнала ГНСС, то установка времени должна быть выполнена, как только БУ сможет получить доступ к действительному времени, выданному приемником ГНСС, в соответствии с условиями системы зажигания транспортного средства.~~ Исходное время для автоматической установки времени на внутренних часах БУ **представляет собой время, указанное в аутентифицированном сообщении о местоположении берется из приемника ГНСС.** Событие «противоречивая информация о времени» происходит в том случае, если текущее время отличается от времени в информации о времени, передаваемой приемником ГНСС, более чем на одну (1) минуту.

212) Функция корректировки времени также позволяет произвести синхронизированную корректировку текущего времени в режиме калибровки.

Мастерские могут корректировать время:

- либо посредством записи значения времени в БУ, используя функцию «WriteDataByIdentifier» в соответствии с частью 6.2 подраздела 8;
- либо посредством запроса на установку часов БУ по времени, выдаваемому приемником ГНСС. Это можно сделать только в том случае, если время, выдаваемое приемником ГНСС, получено с помощью аутентифицированных сообщений о местоположении. В этом последнем случае используется функция «RoutineControl» в соответствии с частью 8 подраздела 8.

3.24 Функциональные характеристики

213) Бортовое устройство полностью работоспособно в диапазоне температур от $-20\text{ }^{\circ}\text{C}$ до $70\text{ }^{\circ}\text{C}$, внешнее устройство ГНСС — в диапазоне температур от $-20\text{ }^{\circ}\text{C}$ до $70\text{ }^{\circ}\text{C}$, а датчик движения — в диапазоне температур от $-40\text{ }^{\circ}\text{C}$ до $135\text{ }^{\circ}\text{C}$. Содержимое блока памяти данных должно сохраняться при температуре до $-40\text{ }^{\circ}\text{C}$.

214) Тахограф полностью работоспособен в диапазоне влажности от 10 % до 90 %.

215) Пломбы, используемые в смарт-тахографе выдерживают такие же условия, как пломбы компонентов тахографа, на которые они наложены.

216) ~~Записывающее оборудование~~ **Контрольное устройство** должно быть защищено от перепадов напряжения, несоблюдения полярности источника питания и короткого замыкания.

217) Датчики движения:

- либо реагируют на магнитное поле, нарушающее условия регистрации движения транспортного средства. В подобных обстоятельствах бортовое устройство регистрирует и хранит данный случай как неисправность датчика (требование 88),
- либо оснащаются чувствительным элементом, защищенным от магнитных полей или не реагирующим на них.

218) ~~Записывающее оборудование~~ **Контрольное устройство** и внешнее устройство ГНСС соответствуют ~~международному регламенту~~ **международным Правилам № 10 ЕЭК ООН R10** и защищены от электростатических разрядов и переходных процессов.

3.25 Материалы

219) Все составные части ~~записывающего оборудования~~ **контрольного устройства** изготавливаются из материалов, обладающих достаточной устойчивостью и механической прочностью со стабильными электромагнитными характеристиками.

220) В обычных условиях эксплуатации все внутренние детали оборудования защищены от действия влаги и пыли.

221) Бортовое устройство и внешнее устройство ГНСС соответствуют классу защиты IP 40, а датчик движения соответствует классу защиты IP 64, согласно стандарту IEC 60529:1989, включая A1:1999 и A2:2013.

222) ~~Записывающее оборудование~~ **Контрольное устройство** соответствует применимым техническим спецификациям, регламентирующим параметры эргономичности.

223) ~~Записывающее оборудование~~ **Контрольное устройство** защищается от случайного повреждения.

3.26 Маркировка

224) Если ~~записывающее оборудование~~ **контрольное устройство** выводит на дисплей показания счетчика пробега и спидометра транспортного средства, то на дисплее отображаются следующие детали:

- около цифры, показывающей расстояние, — единица измерения расстояния, обозначаемая с помощью сокращения «км»;
- около цифры, указывающей на скорость, — сокращение «км/ч».

~~Записывающее оборудование~~ **Контрольное устройство** может также переключаться в режим отображения скорости в милях в час; в этом случае единица измерения скорости указывается с помощью сокращения «mph» (миль/ч). ~~Записывающее оборудование~~ **Контрольное устройство** может также переключаться в режим отображения расстояния в милях; в этом случае единица измерения расстояния указывается с помощью сокращения «mi» (миля).

225) К каждому отдельному компоненту ~~записывающего оборудования~~ **контрольного устройства** прикреплена поясняющая табличка с указанием следующих данных:

- название и адрес изготовителя ~~оборудования~~;

- номер детали, присвоенный изготовителем, и год изготовления оборудования;
- серийный номер оборудования;
- знак официального утверждения типа оборудования.

226) Если на табличке физически не хватает места для указания вышеупомянутых данных, то на ней следует указать хотя бы название или логотип изготовителя и номер детали данного оборудования.

3.27 Мониторинг пересечения границ

226a) Эта функция определяет момент, когда транспортное средство пересекло границу той или иной страны, из какой страны оно выехало и в какую страну оно въехало.

226b) Выявление факта пересечения границы определяется на основе координат местоположения, измеренных контрольным устройством, и сохраненной цифровой карты в соответствии с пунктом 3.12.19.

226c) Пересечение границы, в случае которого транспортное средство находится в данной стране в течение периода продолжительностью менее 120 секунд, не регистрируется.

3.28 Обновление программного обеспечения

226d) Бортовое устройство транспортного средства включает функцию обновления программного обеспечения во всех случаях, когда такие обновления не требуют наличия дополнительных аппаратных ресурсов, помимо тех, которые указаны в требовании 226f, и когда органы по официальному утверждению типа дают свое разрешение на обновление программного обеспечения с помощью установленного бортового устройства транспортного средства официально утвержденного типа в соответствии с настоящим Соглашением.

226e) Функция обновления программного обеспечения разработана в целях поддержки следующих функциональных особенностей во всех случаях, предусмотренных законом:

- модификация функций, упомянутых в пункте 2.2, за исключением самой функции обновления программного обеспечения;
- добавление новых функций, непосредственно связанных с обеспечением соблюдения законодательства ЕС в области автомобильного транспорта;
- изменение режимов работы, указанных в пункте 2.3;
- изменение структуры файлов, например, включение дополнительных новых данных или увеличение размера файлов;
- развертывание системы программных корректировок в порядке устранения дефектов программного обеспечения, а также дефектов в системе защиты или в порядке реагирования на сообщения о случаях злонамеренного воздействия на функции контрольного устройства.

226f) Бортовое устройство транспортного средства обеспечивает незадействованные аппаратные ресурсы на уровне не менее 35 % в части программного обеспечения и данных, необходимых для выполнения требования 226e, и незадействованные аппаратные ресурсы — на уровне не менее 65 % в части обновления цифровой карты на основе аппаратных ресурсов, необходимых для карты «NUTS 0» версии 2021 года.

4. Требования к конструкции и функциям карточек тахографов

4.1 Видимые данные

На первой странице указываются:

227) слова «Карточка водителя», или «Карточка контролера», или «Карточка мастерской» или «Карточка предприятия», напечатанные заглавными буквами на официальном языке или языках ~~государства-члена, выдавшего~~ **Договаривающейся стороны, выдавшей** карточку, в соответствии с данным типом карточки.

228) название ~~государства-члена — выдавшего~~ **Договаривающейся стороны, выдавшей** карточку (факультативно);

229) В случае **государств — членов** ЕС отличительный знак государств-членов, выдавших карточку, напечатанный в виде негатива в синем прямоугольнике в окружении 12 желтых звезд. Отличительные знаки:

B	Бельгия	LV	Латвия
BG	Болгария	L	Люксембург
CZ	Чешская Республика	LT	Литва
CY	Кипр	M	Мальта
DK	Дания	NL	Нидерланды
D	Германия	A	Австрия
EST	Эстония	PL	Польша
GR	Греция	P	Португалия
		RO	Румыния
		SK	Словакия
		SLO	Словения
E	Испания	FIN	Финляндия
F	Франция	S	Швеция
HR	Хорватия		
H	Венгрия		
IRL	Ирландия	UK	Соединенное Королевство
I	Италия		

Для Договаривающихся сторон, не входящих в ЕС, — отличительный знак Договаривающейся стороны, выдавшей карточку. Отличительными знаками Договаривающихся сторон, не входящих в Европейский союз, являются знаки, выполненные в соответствии с Венской конвенцией о дорожном движении 1968 года или с Женевской конвенцией о дорожном движении 1949 года.

230) Конкретная информация, касающаяся выданной карточки, под следующими номерами:

	<i>Карточка водителя</i>	<i>Карточка контролера</i>	<i>Карточка предприятия или мастерской</i>
1.	Фамилия водителя	Название контрольного органа	Название предприятия или мастерской
2.	Имя (имена) водителя	Фамилия контролера (если применимо)	Фамилия держателя карточки (если применимо)
3.	Дата рождения водителя	Имя (имена) контролера (если применимо)	Имя (имена) держателя карточки (если применимо)

	<i>Карточка водителя</i>	<i>Карточка контролера</i>	<i>Карточка предприятия или мастерской</i>
4.a	Начало срока действия карточки		
4.b	Истечение срока действия карточки		
4.c	Название компетентного органа, выдавшего карточку (может быть напечатано на обратной стороне)		
4.d	Номер, отличный от номера, указанного в позиции 5, для административных целей (факультативно)		
5.a	Номер водительского удостоверения (на дату выдачи карточки водителя)	–	–
5.b	Номер карточки		
6.	Фотография водителя	Фотография контролера (факультативно)	Фотография техника (факультативно)
7.	Подпись держателя (факультативно)		
8.	Обычное место жительства или почтовый адрес держателя (факультативно)	Почтовый адрес контрольного органа	Почтовый адрес предприятия или мастерской

231) даты записываются в формате «дд/мм/гггг» или «дд.мм.гггг» (день, месяц, год).

На обратной стороне указываются следующие данные:

232) разъяснение пронумерованных позиций, содержащихся на лицевой стороне карточки;

233) с письменного согласия держателя в каждом конкретном случае в карточку может включаться информация, которая не относится к работе с карточкой; такая дополнительная информация не должна никоим образом изменять метод использования этого образца в качестве карточки тахографа.

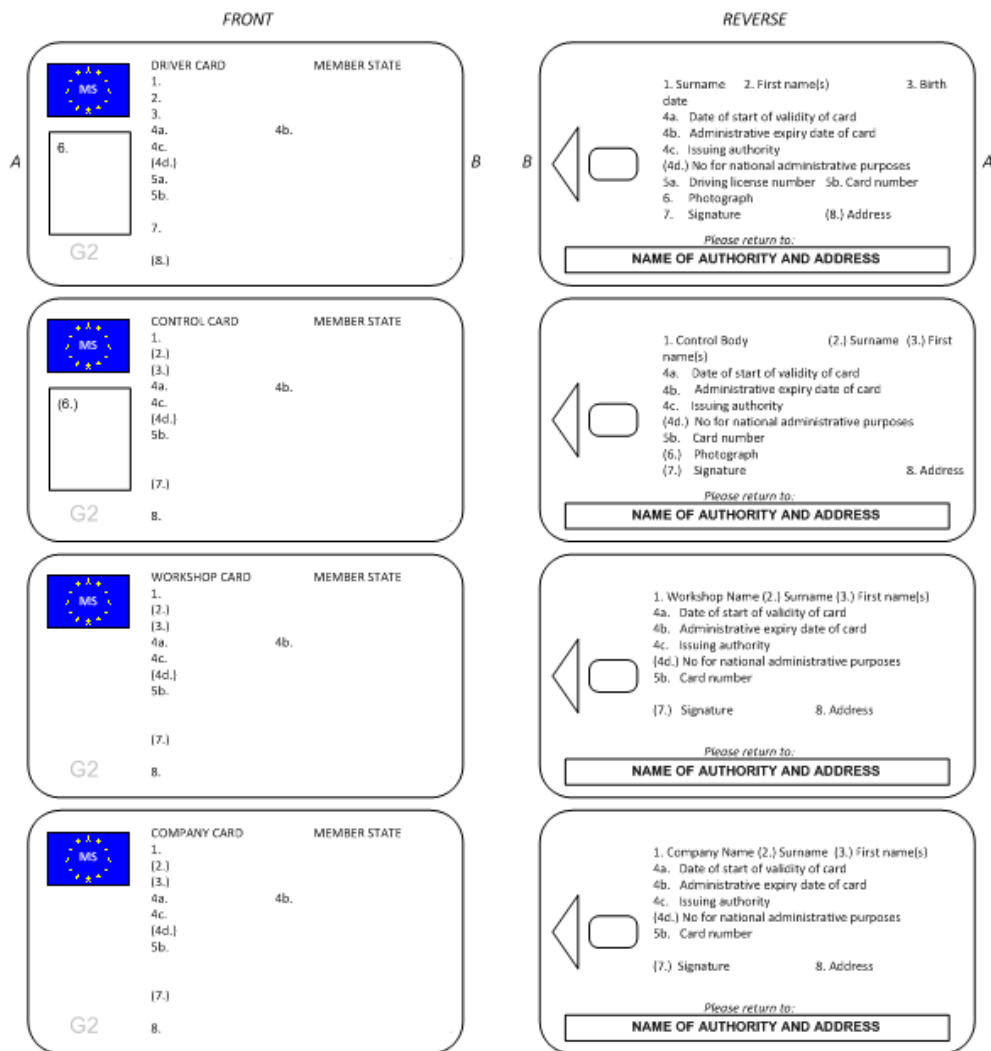
234) Текст карточек тахографа печатается на фоне следующих основных цветов:

- карточка водителя: белый;
- карточка контролера: синий;
- карточка мастерской: красный;
- карточка предприятия: желтый.

235) Карточки тахографа содержит, как минимум, следующие элементы защиты основы карточки от подделки и фальсификации:

- защитный фоновый рисунок тонкой сетки блокперфект и печатная расцветка цветами радуги;
- на месте фотографии — фоновый защитный рисунок, который перекрывается фотографией;
- по крайней мере одна двухцветная линия — микропринт.

COMMUNITY MODEL TACHOGRAPH CARDS



236) **Договаривающиеся стороны** могут добавлять цвета или маркировку, такие как национальные символы и элементы безопасности, без ущерба для других положений настоящего приложения **добавления**.

~~Временные карточки, упомянутые в статье 26.4 Регламента (ЕС) N° 165/2014 должны соответствовать положениям настоящего Приложения.~~

237) **Зарезервирован.**

4.2 Защита

Цель системы защиты — предохранить целостность и подлинность данных, передаваемых между карточками и ~~записывающим оборудованием~~ **контрольным устройством**, предохранить целостность и подлинность данных, загружаемых с карточки, предоставить возможность производить некоторые операции по записи данных на карточку только ~~записывающим оборудованием~~ **контрольным устройством**, исключить любую возможность подлога данных, хранящихся на карточках, предотвратить фальсификацию и обнаружить любые попытки такого рода.

238) В целях обеспечения защиты системы карточки тахографа должны соответствовать требованиям безопасности, изложенным в ~~приложениях~~ **подразделах 10 и 11.**

239) Карточки тахографа могут считываться другими устройствами, например, персональными компьютерами.

4.3 Стандарты

240) Карточки тахографов соответствуют следующим стандартам:

- ISO/IEC 7810 Карточки идентификационные — физические характеристики;
- ISO/IEC 7816 Карточки идентификационные — карточки на интегральных микросхемах:
 - Часть 1: Физические характеристики;
 - Часть 2: Размеры и расположение контактов (ISO/IEC 7816-2:2007);
 - Часть 3: Электрический интерфейс и протоколы передачи (ISO/IEC 7816-3:2006);
 - Часть 4: Организация, безопасность и команды обмена (ISO/IEC 7816-4:2013 + Cor 1:2014);
 - Часть 6: Межсекторные элементы данных для обмена (ISO/IEC 7816-6:2004 + Cor 1:2006);
 - Часть 8: Команды операций по обеспечению безопасности (ISO/IEC 7816-8:2004).

Карточки тахографов тестируются в соответствии с ISO/IEC 10373-3:2010 Идентификационные карточки — методы испытаний. Часть 3: Карточки на интегральных микросхемах с контактами и связанные с ними устройства интерфейса.

4.4 Спецификации на воздействие окружающих условий и электромагнитную совместимость

241) Карточки тахографа способны надлежащим образом работать в любых климатических условиях, которые обычно встречаются на территории ~~Соединенных~~ **Договаривающихся сторон**, как минимум в диапазоне температур от $-25\text{ }^{\circ}\text{C}$ до $+70\text{ }^{\circ}\text{C}$ с нерегулярными пиковыми значениями до $+85\text{ }^{\circ}\text{C}$; при этом термин «нерегулярные» означает не более 4 часов каждый раз и не более 100 раз в течение всего срока службы карточки.

242) Карточки тахографа работоспособны в диапазоне влажности от 10 % до 90 %.

243) Карточки тахографа способны надлежащим образом работать в течение пяти лет, если они используются с соблюдением указанных спецификаций на условия окружающей среды и электромагнитную совместимость.

244) В процессе работы карточки тахографа соответствуют Правилам № 10 ЕЭК, касающимся электромагнитной совместимости, и защищены от электростатических разрядов.

4.5 Хранение данных

Для целей настоящего пункта:

- время регистрируется с точностью до одной минуты, если не предусмотрено иное;
- показания счетчика пробега регистрируются с точностью до 1 км;
- показания спидометра регистрируются с точностью до 1 км/ч;

- местоположение (широта и долгота) регистрируется в градусах и минутах с точностью до 1/10 минуты.

Функции, команды и логические структуры карточек тахографа, соответствующие требованиям, предъявляемым к хранению данных, представлены в ~~приложении~~ **подразделе 2**.

Если не указано иное, хранение данных на карточках тахографов организуется таким образом, чтобы в случае нехватки предусмотренного объема памяти для определенных записей новые данные записывались поверху самых старых данных.

245) В настоящем пункте определяется минимальный объем памяти хранения различных файлов данных соответствующих приложений. Карточки тахографа способны передавать ~~записывающему оборудованию~~ **контрольному устройству** данные о фактическом объеме памяти для хранения данных этих файлов.

246) На карточках тахографов могут храниться любые дополнительные данные, **при условии что хранение таких данных соответствует действующему законодательству, регламентирующему защиту данных** ~~связанные с другими приложениями, которые могут быть записаны на карточке, хранятся в соответствии с Директивой 95/46/ЕС законодательству о защите личных данных, применимого на территории от 24 октября 1995 года о Договаривающихся сторонах и Конвенцией о защите лиц при автоматической обработке личных данных и о свободном движении таких данных⁸ и Директивой 2002/58/ЕС от 12 июля 2002 года об обработке личных данных и защите конфиденциальности⁹ в секторе электронных коммуникаций и статьей 7 Регламента (ЕС) № 165/2014.~~

247) Каждый главный файл (MF) на любой карточке тахографа включает в себя до пяти элементарных файлов (EF), предназначенных для управления карточкой, а также для приложений и идентификации микросхемы, и два специальных файла (DF):

- «DF Tachograph» с приложением, доступным для бортовых устройств первого поколения и имеющимся также на карточках тахографов первого поколения;
- «DF Tachograph_G2» с приложением, доступным только для бортовых устройств второго поколения и имеющимся только на карточках тахографов второго поколения.

Примечание: Версия 2 карточек второго поколения содержит дополнительные элементарные файлы в «DF Tachograph_G2».

Подробная информация о структуре карточек тахографов представлена в ~~приложении~~ **подразделе 2**.

4.5.1 Элементарные файлы для идентификации карточек и работы с ними

4.5.2 Идентификационные данные карточки на интегральных микросхемах

248) Карточки тахографа способны хранить следующие идентификационные данные карточки на интегральной микросхеме:

- остановка часов;
- серийный номер карточки (включая исходные заводские данные);
- номер официального утверждения типа карточки;
- идентификатор учреждения по персонализации карточки (ИД);
- ИД монтажного предприятия;
- идентификатор ИС.

⁸ OJ No L281, 23/11/1995, P 31.

⁹ OJ No L201, 31/07/2002, P 37.

4.5.2.1 Идентификационные данные карточки на интегральной микросхеме

249) Карточки тахографа способны хранить следующие идентификационные данные интегральных микросхем (ИС):

- серийный номер ИС;
- исходные заводские данные ИС.

4.5.2.2 DIR (только на карточках тахографа второго поколения)

250) Карточки тахографа способны хранить следующие объекты идентификационных данных приложений, указанные в ~~приложении~~ **подразделе 2**.

4.5.2.3 Информация ATR (в определенных условиях, только на карточках тахографа второго поколения)

251) Карточки тахографа способны хранить следующие объекты информационных данных расширенной длины:

в случае карточки тахографа, поддерживающей поля расширенной длины, — объект информационных данных расширенной длины, указанный в ~~приложении~~ **подразделе 2**.

4.5.2.4 Информация расширенной длины (в определенных условиях, только на карточках тахографа второго поколения)

252) Карточки тахографа способны хранить следующие объекты информационных данных расширенной длины:

в случае карточки тахографа, поддерживающей поля расширенной длины, — объект информационных данных расширенной длины, указанный в ~~приложении~~ **подразделе 2**.

4.5.3 Карточка водителя

4.5.3.1 Приложение тахографа (доступно для бортовых устройств первого и второго поколений)

4.5.3.1.1 Идентификационные данные приложения

253) Карточка водителя способна хранить следующие идентификационные данные приложения:

- идентификационные данные приложения тахографа;
- идентификационные данные типа карточки тахографа.

4.5.3.1.2 Ключи и сертификаты

254) Карточка водителя способна хранить ряд криптографических ключей и сертификатов, как указано в части А ~~приложения~~ **подраздела 11**.

4.5.3.1.3 Идентификационные данные карточки

255) Карточка водителя способна хранить следующие идентификационные данные карточки:

- номер карточки;
- ~~выдавшее ее государство-член~~ **выдавшая ее Договаривающаяся сторона**, название выдавшего компетентного органа, дата выдачи;
- дата начала срока действия карточки, дата истечения срока действия карточки.

4.5.3.1.4 Идентификационные данные карточки держателя

256) Карточка водителя способна хранить следующие идентификационные данные держателя карточки:

- фамилия водителя;
- имя (имена) держателя;
- дата рождения;
- предпочитаемый язык.

4.5.3.1.5 Загрузка данных с карточки

257) Карточка водителя способна хранить следующие данные, касающиеся загрузки данных карточки:

- дата и время последней загрузки данных с карточки (для иных целей, кроме контроля).

258) Карточка водителя способна хранить одну такую запись.

4.5.3.1.6 Информация о водительском удостоверении

259) Карточка водителя способна хранить следующие идентификационные данные водительского удостоверения:

- ~~выдавшее его государство~~ **выдавшая его Договаривающаяся сторона**, название выдавшего компетентного органа;
- номер водительского удостоверения (на дату выдачи карточки).

4.5.3.1.7 Данные о событиях

Для целей настоящего подпункта время регистрируется с точностью до 1 секунды.

260) Карточка водителя способна хранить данные, связанные со следующими событиями, выявленными ~~занимающим оборудованием~~ **контрольным устройством**, в момент ввода карточки:

- нестыковка во времени (в тех случаях, когда причиной этого события является данная карточка);
- ввод карточки в процессе управления (в тех случаях, когда причиной этого события является данная карточка);
- неправильное завершение последнего сеанса использования карточки (в тех случаях, когда причиной этого события является данная карточка);
- прекращение электропитания;
- ошибка данных о движении;
- попытка нарушения системы защиты.

261) Карточка водителя способна хранить следующие данные, касающиеся этих событий:

- код события;
- дата и время начала события (или ввода карточки, если в данный момент это событие продолжается);
- дата и время окончания события (или извлечения карточки, если в данный момент это событие продолжается);
- VRN и ~~государство-член~~ **Договаривающаяся сторона** регистрации транспортного средства, к которому относится это событие.

Примечание: В случае события «несстыковка во времени»:

- дата и время начала события соответствуют дате и времени извлечения карточки из предыдущего транспортного средства;
- дата и время окончания события соответствуют дате и времени ввода карточки в устройство используемого транспортного средства;
- данные о транспортном средстве соответствуют транспортному средству, которое используется в данный момент и к которому относится данное событие.

Примечание: Событие «Неправильное завершение последнего сеанса использования карточки»:

- дата и время начала события соответствуют дате и времени ввода карточки в случае неправильно заверщенного сеанса ее использования;
- дата и время окончания события соответствуют дате и времени ввода карточки в ходе данного сеанса использования, во время которого зафиксировано данное событие (текущий сеанс);
- данные о транспортном средстве соответствуют транспортному средству, на котором сеанс использования карточки был завершён неправильно.

262) Карточка водителя способна хранить данные о шести последних событиях каждого типа (т. е. 36 событий).

4.5.3.1.8 Данные о неисправностях

Для целей настоящего подпункта время регистрируется с точностью до 1 секунды.

263) Карточка водителя способна хранить данные, касающиеся следующих неисправностей, обнаруженных ~~записывающим оборудованием~~ **контрольным устройством** с введенной в него карточкой:

- неисправность карточки (в тех случаях, когда причиной ~~этого события~~ этой неисправности является сама карточка);
- неисправность ~~записывающего оборудования~~;
- **неисправность контрольного устройства.**

264) Карточка водителя способна хранить следующие данные, касающиеся этих неисправностей:

- код неисправности;
- дата и время начала неисправности (или ввода карточки, если в данный момент неисправность еще не устранена);
- дата и время окончания неисправности (или извлечения карточки, если в данный момент неисправность еще не устранена);
- VRN и ~~государство-член~~ **Договаривающаяся сторона** регистрации транспортного средства, к которому относится эта неисправность.

265) ~~Карточка водителя должна иметь возможность хранить данные о двенадцати последних неисправностях каждого типа (т. е. 24 неисправности)~~ **Карточка водителя способна хранить данные о двенадцати последних неисправностях каждого типа (т. е. 24 неисправности).**

4.5.3.1.9 Данные о деятельности водителя

266) За каждый календарный день, в течение которого используется данная карточка или в течение которого водитель вручную внес данные о своей деятельности, карточка водителя способна хранить следующие данные:

- дата;
- счетчик ежедневного присутствия (показания которого увеличиваются на одну единицу за каждый календарный день);
- общее расстояние, пройденное водителем на транспортном средстве в течение этого дня;
- статус водителя на 00:00 часов;
- все случаи, когда водитель меняет вид деятельности и/или статус управления и/или вводит или извлекает свою карточку;
- статус управления (ЭКИПАЖ, ОДИН);
- считывающее устройство (ВОДИТЕЛЬ, ВТОРОЙ ВОДИТЕЛЬ);
- статус карточки (ВСТАВЛЕНА, НЕ ВСТАВЛЕНА);
- вид деятельности (УПРАВЛЕНИЕ, ГОТОВНОСТЬ, РАБОТА, ПЕРЕРЫВ/ОТДЫХ);
- время изменения.

267) Блок памяти карточки водителя способен хранить данные о деятельности водителя как минимум 28 дней (показатель усредненной деятельности водителя определяется в качестве 93 изменений видов деятельности в день).

268) Данные, перечисленные в требованиях 261, 264 и 266, хранятся таким образом, чтобы данные о видах деятельности можно было извлечь из памяти в хронологическом порядке их ввода, даже в случае нестыковки во времени.

4.5.3.1.10 Данные об используемых транспортных средствах

269) За каждый календарный день, в течение которого используется карточка, и за каждый период использования данного транспортного средства в течение указанного дня (период использования включает все последовательные циклы ввода/извлечения данной карточки на транспортном средстве с точки зрения карточки) карточка водителя способна хранить следующие данные:

- дата и время первого использования транспортного средства (т. е. первый ввод карточки за этот период использования транспортного средства или 00:00 часов, если в этот момент данный период использования продолжается);
- показание счетчика пробега транспортного средства в это время;
- дата и время последнего использования транспортного средства (т. е. последнее извлечение карточки за этот период использования транспортного средства или 23 часа 59 минут, если в этот момент данный период использования продолжается);
- показание счетчика пробега транспортного средства в это время;
- VRN и государство-член Договаривающаяся сторона регистрации транспортного средства.

270) Карточка водителя способна хранить не менее 84 таких записей.

4.5.3.1.11 Места, в которых начинаются и/или заканчиваются дневные периоды работы

271) Карточка водителя способна хранить следующие данные, касающиеся мест, в которых начинаются и/или заканчиваются ежедневные периоды работы, введенные водителем:

- дата и время ввода (или дата/время, относящиеся к вводу этих данных, если этот ввод производится вручную);
- тип ввода (начало или конец, условие ввода);
- введенное название страны и региона;
- показания счетчика пробега транспортного средства.

272) Блок памяти карточки водителя способен хранить не менее 42 пар таких записей.

4.5.3.1.12 Данные о сеансе использования карточки

273) Карточка водителя способна хранить данные, касающиеся транспортного средства, на котором начат текущий сеанс ее использования:

- дата и время начала сеанса (т. е. ввода карточки) с точностью до одной секунды;
- VRN и ~~государство-член~~ **Договаривающаяся сторона** регистрации транспортного средства.

4.5.3.1.13 Данные о деятельности по контролю

274) Карточка водителя способна хранить следующие данные, касающиеся деятельности по контролю:

- дата и время контроля;
- номер карточки контролера и ~~государство-член~~, **выдавшее Договаривающаяся сторона, выдавшая** карточку;
- тип контроля (вывод на дисплей и/или на печать и/или загрузка данных с БУ и/или загрузка с карточки (см. примечание));
- период, за который загружаются данные, в случае загрузки;
- VRN и ~~государство-член~~ **Договаривающаяся сторона** регистрации транспортного средства, к которому относится эта деятельность по контролю.

Примечание: Загрузка данных с карточки регистрируется только в том случае, если она осуществляется через ~~записывающее оборудование~~ **контрольное устройство**.

275) Карточка водителя способна хранить одну такую запись.

4.5.3.1.14 Данные об особых условиях

276) Карточка водителя способна хранить следующие данные, касающиеся особых условий, которые были введены в то время, когда карточка была вставлена в устройство (независимо от считывающего устройства):

- дата и время ввода данных;
- тип особых условий.

277) Карточка водителя способна хранить не менее 56 таких записей.

4.5.3.2 Приложение тахографа второго поколения (недоступно для бортовых устройств первого поколения, **доступно для бортовых устройств версии 1 и версии 2 второго поколения**)

4.5.3.2.1 Идентификационные данные приложения

278) Карточка водителя способна хранить следующие идентификационные данные приложения:

- идентификационные данные приложения тахографа;
- идентификационные данные типа карточки тахографа.

4.5.3.2.1.1 Дополнительная идентификация приложения (недоступна для бортовых устройств версии 1 второго поколения)

278a) Карточка водителя способна хранить дополнительные идентификационные данные приложения, применимые только в случае версии 2.

4.5.3.2.2 Ключи и Сертификаты сертификаты

279) Карточка водителя способна хранить ряд криптографических ключей и сертификатов, как указано в части В приложения подраздела 11.

4.5.3.2.3 Идентификационные данные карточки

280) Карточка водителя способна хранить следующие идентификационные данные карточки:

- номер карточки;
- **выдавшее ее государство – член Договаривающаяся сторона, выдавшая карточку**, название выдавшего ее компетентного органа, дата выдачи;
- дата начала срока действия карточки, дата истечения срока действия карточки.

4.5.3.2.4 Идентификационные данные карточки держателя

281) Карточка водителя способна хранить следующие идентификационные данные держателя карточки:

- фамилия держателя;
- имя (имена) держателя;
- дата рождения;
- предпочитаемый язык.

4.5.3.2.5 Загрузка данных с карточки

282) Карточка водителя способна хранить следующие данные, касающиеся загрузки данных карточки:

- дата и время последней загрузки данных с карточки (для иных целей, кроме контроля).

283) Карточка водителя способна хранить одну такую запись.

4.5.3.2.6 Информация о водительском удостоверении

284) Карточка водителя способна хранить следующие идентификационные данные водительского удостоверения:

- **выдавшее ее государство – член Договаривающаяся сторона, выдавшая карточку**, название выдавшего компетентного органа, номер водительского удостоверения (на дату выдачи карточки).

4.5.3.2.7 Данные о событиях

Для целей настоящего подпункта время регистрируется с точностью до 1 секунды.

285) Карточка водителя способна хранить данные, касающиеся следующих событий, обнаруженных ~~занимающим оборудованием~~ **контрольным устройством** со вставленной в него карточкой:

- нестыковка во времени (в тех случаях, когда причиной этого события является сама карточка);
- ввод карточки в процессе управления (в тех случаях, когда причиной этого события является сама карточка);
- неправильное завершение последнего сеанса использования карточки (в тех случаях, когда причиной этого события является данная карточка);
- прекращение электропитания;
- ошибка связи со средством удаленной связи;
- отсутствие информации о местоположении, выдаваемой приемником ГНСС;
- ошибка связи с внешним устройством ГНСС;
- ошибка данных о движении;
- противоречивые данные о движении транспортного средства;
- попытка нарушения системы защиты;
- противоречивые данные о времени.

286) Карточка водителя способна хранить следующие данные, касающиеся этих событий:

- код события;
- дата и время начала события (или ввода карточки, если в данный момент это событие еще продолжается);
- дата и время окончания события (или извлечения карточки, если в данный момент это событие еще продолжается);
- VRN и ~~государство-член~~ **Договаривающаяся сторона** регистрации транспортного средства, к которому относится это событие.

Примечание: В случае события «нестыковка во времени»:

- дата и время начала события соответствуют дате и времени извлечения карточки из предыдущего транспортного средства;
- дата и время окончания события соответствуют дате и времени ввода карточки в устройство используемого транспортного средства в данный момент;
- данные о транспортном средстве соответствуют используемому в данный момент транспортному средству, к которому относится данное событие.

Примечание: Событие «Неправильное завершение последнего сеанса использования карточки»:

- дата и время начала события соответствуют дате и времени ввода карточки в случае неправильно заверщенного сеанса ее использования;
- дата и время окончания события соответствуют дате и времени ввода карточки в ходе данного сеанса использования, во время которого зафиксировано данное событие (текущий сеанс);

- данные о транспортном средстве соответствуют транспортному средству, на котором сеанс использования карточки был завершен неправильно.

287) Карточка водителя способна хранить данные о шести последних событиях каждого типа (т. е. ~~36~~ **132** событий).

4.5.3.2.8 Данные о неисправностях

Для целей настоящего подпункта время регистрируется с точностью до 1 секунды.

288) Карточка водителя способна хранить данные, касающиеся следующих неисправностей, обнаруженных ~~записывающим оборудованием~~ **контрольным устройством** со вставленной в него карточкой:

- неисправность карточки (в тех случаях, когда причиной **неисправности** ~~записывающего оборудования~~ является сама карточка);
- **неисправность контрольного устройства.**

289) Карточка водителя способна хранить следующие данные, касающиеся этих неисправностей:

- код неисправности;
- дата и время начала неисправности (или ввода карточки, если в данный момент неисправность еще не устранена);
- дата и время окончания неисправности (или извлечения карточки, если в данный момент неисправность еще не устранена);
- VRN и ~~государство-член~~ **Договаривающаяся сторона** регистрации транспортного средства, к которому относится эта неисправность.

290) Карточка водителя способна хранить данные о ~~24~~ **двенадцати** последних событиях каждого типа (т. е. ~~24~~ **48** неисправностей). ~~Карточка водителя способна хранить данные о двенадцати последних событиях каждого типа (т. е. 24 неисправности).~~

4.5.3.2.9 Данные о деятельности водителя

291) За каждый календарный день, в течение которого используется данная карточка или в течение которого водитель вручную внес данные о своей деятельности, карточка водителя способна хранить следующие данные:

- дата;
- счетчик ежедневного присутствия (показания которого увеличиваются на одну единицу за каждый календарный день);
- общее расстояние, пройденное водителем на транспортном средстве в течение этого дня;
- статус водителя на 00:00 часов;
 - во всех случаях, когда водитель меняет вид деятельности и/или статус управления и/или вводит или извлекает свою карточку;
 - статус управления (ЭКИПАЖ, ОДИН);
 - считывающее устройство (ВОДИТЕЛЬ, ВТОРОЙ ВОДИТЕЛЬ);
 - статус карточки (ВСТАВЛЕНА, НЕ ВСТАВЛЕНА);
 - вид деятельности (УПРАВЛЕНИЕ, ГОТОВНОСТЬ, РАБОТА, ПЕРЕРЫВ/ОТДЫХ);
 - время изменения.

292) Блок памяти карточки водителя способен хранить данные о деятельности водителя ~~как минимум 2856~~ **дней** (показатель усредненной деятельности водителя

определяется в случае этого требования на уровне ~~93~~ **117** изменений видов деятельности в день).

293) Данные, перечисленные в требованиях 286, 289 и 291, хранятся таким образом, чтобы данные о видах деятельности можно было извлечь из памяти в хронологическом порядке их ввода, даже в случае нестыковки во времени.

4.5.3.2.10 Данные об используемых транспортных средствах

294) За каждый календарный день, в течение которого используется карточка, и за каждый период использования данного транспортного средства в течение указанного дня (период использования включает все последовательные циклы ввода/извлечения данной карточки на транспортном средстве с точки зрения карточки) карточка водителя способна хранить следующие данные:

- дата и время первого использования транспортного средства (т. е. первый ввод карточки за этот период использования транспортного средства или 00:00 часов, если в этот момент данный период использования продолжается);
- показание счетчика пробега транспортного средства на момент первого использования;
- дата и время последнего использования транспортного средства (т. е. последнее извлечение карточки за этот период использования транспортного средства или 23 ч 59 м, если в этот момент данный период использования продолжается);
- показание счетчика пробега транспортного во время последнего использования;
- VRN и ~~государство-член Договаривающаяся сторона~~ регистрации транспортного средства;
- VIN транспортного средства.

295) Карточка водителя способна хранить, ~~как минимум,~~ **200 84** таких записей.

4.5.3.2.11 Места и местоположения, в которых начинаются и/или заканчиваются дневные периоды работы

296) Карточка водителя способна хранить следующие данные, касающиеся мест, в которых начинаются и/или заканчиваются ежедневные периоды работы, введенные водителем:

дата и время ввода (или дата/время, относящиеся к вводу этих данных, если этот ввод производится вручную),

- тип ввода (начало или конец, условие ввода);
- введенное название страны и региона;
- показания счетчика пробега транспортного средства;
- местоположение транспортного средства;
- точность ГНСС, дата и время определения местоположения.

297) Блок памяти карточки водителя способен хранить, ~~как минимум,~~ **112 84** пар таких записей.

4.5.3.2.12 Данные о сеансе использования карточки

298) Карточка водителя способна хранить данные, касающиеся транспортного средства, на котором начат текущий сеанс ее использования:

- дата и время начала сеанса (т. е. ввода карточки) с точностью до одной секунды;

- VRN и государство-член Договаривающаяся сторона регистрации.

4.5.3.2.13 Данные о деятельности по контролю

299) Карточка водителя способна хранить следующие данные, касающиеся деятельности по контролю:

- дата и время контроля;
- номер карточки контролера и Договаривающаяся сторона, выдавшая карточку;
- тип контроля (вывод на дисплей и/или на печать и/или загрузка данных с БУ и/или загрузка с карточки (см. примечание));
- период, за который загружаются данные, в случае загрузки;
- VRN и государство-член Договаривающаяся сторона регистрации транспортного средства, на котором производится этот контроль.

Примечание: Требования, касающиеся безопасности, предусматривают, что загрузка данных с карточки регистрируется только в том случае, если она осуществляется с помощью записывающего оборудования **контрольного устройства**.

300) Карточка водителя способна хранить одну такую запись.

4.5.3.2.14 Данные, касающиеся особых условий

301) Карточка водителя способна хранить следующие данные, касающиеся особых условий, которые были введены в то время, когда карточка была вставлена (независимо от считывающего устройства):

- дата и время ввода данных;
- тип особых условий.

302) Карточка водителя способна хранить, как минимум, **11256** таких записей.

4.5.3.2.15 Данные используемых бортовых устройств

303) Карточка водителя способна хранить следующие данные, связанные с различными бортовыми устройствами, в которых использовалась эта карточка:

- дата и время начала периода использования бортового устройства (т.е. первый ввод карточки в бортовое устройство в течение рассматриваемого периода);
- изготовитель бортового устройства;
- тип бортового устройства;
- номер версии программного обеспечения бортового устройства.

304) Карточка водителя способна хранить, как минимум, **200 84** таких записей.

4.5.3.2.16 Данные о местах в процессе ~~непрерывного~~ **накопленного** времени управления

305) Карточка водителя способна хранить следующие данные о местоположении транспортного средства, когда ~~непрерывное~~ **накопленное** время управления ~~водителем~~ достигает значения, кратного трем часам:

- дата и время, когда ~~непрерывное~~ **накопленное** время управления ~~держателем карточки~~ достигает значения, кратного трем часам;
- местоположение транспортного средства;
- точность по ГНСС, дата и время определения местоположения;
- **показания счетчика пробега транспортного средства.**

306) Карточка водителя способна хранить, ~~как минимум,~~ **336** таких записей ~~252~~ такие записи.

4.5.3.2.17 Статус аутентификации в случае местоположений, связанных с местами, в которых начинаются и/или заканчиваются ежедневные рабочие периоды (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

306a) Карточка водителя способна хранить дополнительные данные, касающиеся мест, в которых начинаются и/или заканчиваются ежедневные периоды работы, введенные водителем в соответствии с пунктом 4.5.3.2.11:

- дата и время записи, которые должны точно совпадать с датой и временем, сохраненными в папке «EF Places» в специальном файле «DF Tachograph_G2»;
- метка, указывающая на то, было ли это местоположение аутентифицировано.

306b) Блок памяти карточки водителя способен вместить **112** таких записей.

4.5.3.2.18 Статус аутентификации в случае местоположений, в которых накапливаются три часа управления (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

306c) Карточка водителя способна хранить дополнительные данные, связанные с местоположением транспортного средства, когда накопленное время управления достигает значения, кратного трем часам, в соответствии с пунктом 4.5.3.2.16:

- дата и время, когда накопленное время управления достигает значения, кратного трем часам, которые должны быть точно такими же, как дата и время, сохраненные в папке «EF GNSS_Places» в специальном файле «DF Tachograph_G2»;
- метка, указывающая на то, было ли это местоположение аутентифицировано.

306d) Карточка водителя способна хранить **336** таких записей.

4.5.3.2.19 Статус пересечения границы (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

306e) Карточка водителя способна хранить следующие данные, связанные с пересечением границы, либо в случае ввода карточки в соответствии с требованием 147b, либо в случае, когда карточка уже введена:

- страна, которую покидает транспортное средство;
- страна, в которую въезжает транспортное средство;
- дата и время пересечения границы транспортным средством;
- местоположение транспортного средства в момент пересечения границы;
- точность ГНСС;
- метка, указывающая на то, было ли это местоположение аутентифицировано;
- показания счетчика пробега транспортного средства.

306f) Блок памяти карточки водителя способен хранить **1120** таких записей.

4.5.3.2.20 Операции по загрузке/разгрузке (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

306g) Карточка водителя способна хранить следующие данные, связанные с операциями по загрузке/разгрузке:

- тип операции (загрузка, разгрузка или одновременная загрузка/разгрузка);
- дата и время операции по загрузке/разгрузке;
- местоположение транспортного средства;
- точность ГНСС, дата и время, когда было определено данное местоположение;
- метка, указывающая на то, было ли это местоположение аутентифицировано;
- показания счетчика пробега транспортного средства.

306h) Карточка водителя способна хранить 1624 операции по загрузке/разгрузке.

4.5.3.2.21 Записи о типе груза (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

306i) Карточка водителя способна хранить следующие данные, относящиеся к типу груза, автоматически вводимые БУ в каждом случае ввода карточки:

- введенные данные о типе груза (товары или пассажиры);
- дата и время ввода данных.

306j) Карточка водителя способна хранить 336 таких записей.

4.5.3.2.22 Конфигурации БУ (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

306k) Карточка водителя способна хранить конкретные настройки держателя карточки тахографа.

306l) Объем памяти карточки водителя для хранения конкретных настроек держателя карточки тахографа составляет 3072 байта.

4.5.4 Карточка мастерской

4.5.4.1 Приложение тахографа (доступно для бортовых устройств первого и второго поколений)

4.5.4.1.1 Идентификационные данные приложения

307) Карточка мастерской способна хранить следующие идентификационные данные приложения:

- идентификационные данные приложения тахографа;
- идентификационные данные типа карточки тахографа.

4.5.4.1.2 Ключи и сертификаты Сертификаты

308) Карточка мастерской способна хранить ряд криптографических ключей и сертификатов, как указано в части А приложения подраздела 11.

309) Карточка мастерской способна хранить персональный идентификационный номер (ПИН-код).

4.5.4.1.3 Идентификационные данные карточки

310) Карточка мастерской способна хранить следующие идентификационные данные карточки:

- номер карточки;
- ~~выдавшее~~ ~~ее~~ государство-член, **Договаривающаяся сторона, выдавшая карточку**, название выдавшего компетентного органа, дата выдачи;
- дата начала срока действия карточки, дата истечения срока действия карточки.

4.5.4.1.4 Идентификационные данные карточки держателя

311) Карточка мастерской способна хранить следующие идентификационные данные карточки:

- название мастерской;
- адрес мастерской;
- фамилия держателя;
- имя (имена) держателя;
- предпочитаемый язык.

4.5.4.1.5 Загрузка данных с карточки

312) Карточка мастерской способна хранить запись о загрузке данных карточки таким же образом, как и карточка водителя.

4.5.4.1.6 Данные о калибровке и корректировке времени

313) Карточка мастерской способна хранить запись о калибровке и/или корректировке времени, произведенной в то время, когда карточка была введена в ~~записывающее оборудование~~ **контрольное устройство**.

314) Каждая запись о калибровке способна хранить следующие данные:

- цель калибровки (активация, первая установка, установка, периодическая инспекция);
- идентификационные данные транспортного средства;
- обновление или подтверждение параметров (w, k, l, размер шин, настройки устройства ограничения скорости, счетчик пробега (новые и старые значения), дата и время (новые и старые значения));
- идентификационные данные ~~записывающего~~ ~~оборудования~~ **контрольного устройства** (номер частей БУ, серийный номер БУ, серийный номер датчика движения).

315) Карточка мастерской способна хранить, как минимум, 88 таких записей.

316) На карточке мастерской есть счетчик, указывающий число калибровок, произведенных на карточке.

317) На карточке мастерской есть счетчик, указывающий число калибровок, произведенных на карточке после последней загрузки данных с карточки.

4.5.4.1.7 Данные о событиях и неисправностях

318) Карточка мастерской способна хранить запись данных о событиях и неисправностях таким же образом, как и карточка водителя.

319) Карточка мастерской способна хранить данные о трех последних событиях каждого типа (т. е. 18 событий) и о шести последних неисправностях каждого типа (т. е. 12 неисправностей).

4.5.4.1.8 Данные о деятельности водителя

320) Карточка мастерской способна хранить данные о деятельности водителя таким же образом, как и карточка водителя.

321) Карточка мастерской способна хранить данные о деятельности водителя, как минимум, за 1 день усредненной деятельности водителя.

4.5.4.1.9 Данные об используемых транспортных средствах

322) Карточка мастерской способна хранить запись данных об используемых транспортных средствах таким же образом, как и карточка водителя.

323) Карточка мастерской способна хранить, как минимум, 4 такие записи.

4.5.4.1.10 Данные о начале и/или окончании ежедневных периодов работы

324) Карточка мастерской способна хранить запись данных об используемых транспортных средствах таким же образом, как и карточка водителя.

325) Карточка мастерской способна хранить, как минимум, 3 пары таких записей.

4.5.4.1.11 Данные о сеансе использования карточки

326) Карточка мастерской способна хранить данные о сеансе использования карточки таким же образом, как и карточка водителя.

4.5.4.1.12 Данные о деятельности по контролю

327) Карточка мастерской способна хранить данные о деятельности по контролю таким же образом, как и карточка водителя.

4.5.4.1.13 Данные, касающиеся особых условий

328) Карточка мастерской способна хранить данные, касающиеся особых условий, таким же образом, как и карточка водителя.

329) Карточка мастерской способна хранить, как минимум, 2 такие записи.

4.5.4.2 Приложение к тахографу поколения 2 (недоступно для бортовых устройств первого поколения, **доступно для бортовых устройств второго поколения версии 1 и версии 2)**

4.5.4.2.1 Идентификационные данные приложения

330) Карточка мастерской способна хранить следующие идентификационные данные приложения:

- идентификационные данные приложения тахографа;
- идентификационные данные типа карточки тахографа.

4.5.4.2.1.1 Дополнительные идентификационные данные приложения (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

330а) Карточка мастерской способна хранить дополнительные идентификационные данные приложения, применимые только для версии 2.

4.5.4.2.2 Ключи и ~~Сертификаты~~ сертификаты

331) Карточка мастерской способна хранить целый ряд криптографических ключей и сертификатов, как указано в части В приложения подраздела 11.

332) Карточка мастерской способна хранить персональный идентификационный номер (ПИН-код).

4.5.4.2.3 Идентификационные данные карточки

333) Карточка мастерской способна хранить следующие идентификационные данные карточки:

- номер карточки;
- ~~выдавшее ее государство-член,~~ **Договаривающаяся сторона, выдавшая карточку**, название выдавшего компетентного органа, дата выдачи;
- дата начала срока действия карточки, дата истечения срока действия карточки.

4.5.4.2.4 Идентификационные данные карточки держателя

334) Карточка мастерской способна хранить следующие идентификационные данные карточки держателя:

- название мастерской;
- адрес мастерской;
- фамилия держателя;
- имя (имена) держателя;
- предпочитаемый язык.

4.5.4.2.5 Загрузка данных с карточки

335) Карточка мастерской способна хранить запись о загрузке данных карточки таким же образом, как и карточка водителя.

4.5.4.2.6 Данные о калибровке и корректировке времени

336) Карточка мастерской способна хранить запись о калибровке и/или корректировке времени, произведенной в то время, когда карточка была введена в ~~записывающее оборудование~~ **контрольное устройство**.

337) Каждая запись о калибровке способна хранить следующие данные:

- цель калибровки (активация, первая установка, установка, периодическая инспекция);
- идентификационные данные транспортного средства;
- обновление или подтверждение параметров (w, k, l, размер шин, настройки устройства ограничения скорости, счетчик пробега (новые и старые значения), дата и время (новые и старые значения));
- идентификационные данные ~~записывающего оборудования~~ **контрольного устройства** (номер деталей БУ, серийный номер БУ, серийный номер датчика движения, серийный номер средства удаленной связи номер и серийный номер внешнего устройства ГНСС, в случае применимости);
- тип и идентификатор всех наложенных пломб;
- способность БУ работать с карточками тахографов первого поколения (активированных или нет).

338) Карточка мастерской способна хранить, ~~как минимум, 255 88~~ таких записей.

339) На карточке мастерской есть счетчик, указывающий на общее число калибровок, произведенных на карточке.

340) На карточке мастерской есть счетчик, указывающий на число калибровок, произведенных на карточке после последней загрузки данных с карточки.

4.5.4.2.7 Данные о событиях и неисправностях

341) Карточка мастерской способна хранить записи данных о событиях и неисправностях таким же образом, как и карточка водителя.

342) Карточка мастерской способна хранить данные о трех самых последних событиях каждого типа (т. е. 33 события) и о шести последних неисправностях каждого типа (т. е. 12 неисправностей).

4.5.4.2.8 Данные о деятельности водителя

343) Карточка мастерской способна хранить данные о деятельности водителя таким же образом, как и карточка водителя.

344) Карточка мастерской способна хранить данные о деятельности водителя, ~~как минимум, за 1 день,~~ **насчитывающий 240 изменений видов деятельности усредненной деятельности водителя.**

4.5.4.2.9 Данные об используемых транспортных средствах

345) Карточка мастерской способна хранить запись данных об используемых транспортных средствах таким же образом, как и карточка водителя.

346) Карточка мастерской способна хранить **8 таких записей,** ~~как минимум, 4 такие записи.~~

4.5.4.2.10 Места и местоположения, в которых начинаются и/или заканчиваются ежедневные периоды работы.

347) Карточка мастерской способна хранить записанные данные **о местах и местоположениях, в которых начале и/или окончании дневных периодов работы начинаются и/или заканчиваются** ежедневные периоды работы, таким же образом, как и карточка водителя.

348) Карточка мастерской способна хранить, ~~как минимум, 3~~ **4** пары таких записей.

4.5.4.2.11 Данные о сеансе использования карточки

349) Карточка мастерской способна хранить данные о сеансе использования карточки таким же образом, как и карточка водителя.

4.5.4.2.12 Данные о деятельности по контролю

350) Карточка мастерской способна хранить данные о деятельности по контролю таким же образом, как и карточка водителя.

4.5.4.2.13 Данные используемых бортовых устройств

351) Карточка мастерской способна хранить следующие данные, касающиеся различных бортовых устройств, в которых использовалась карточка:

- дата и время начала периода использования бортового устройства (т. е. первый ввод карточки в бортовое устройство в течение рассматриваемого периода);
- изготовитель бортового устройства;
- тип бортового устройства;
- номер версии программного обеспечения бортового устройства.

352) Карточка мастерской способна хранить **8 таких записей,** ~~как минимум, 4 такие записи.~~

4.5.4.2.14 Данные о местах ~~непрерывного~~ **накопленного** времени управления в течение трех часов

353) Карточка мастерской способна хранить следующие данные о местоположении транспортного средства, когда ~~непрерывное~~ **накопленное** время управления ~~водителем~~ достигает значения, кратного трем часам:

- дата и время, когда ~~непрерывное~~ **накопленное** время управления ~~держателя карточки~~ достигает значения, кратного трем часам;
- местоположение транспортного средства;
- точность ГНСС, дата и время, когда было определено данное местоположение;
- **показания счетчика пробега транспортного средства.**

354) Карточка мастерской способна хранить ~~24, как минимум, 18~~ **24** такие записи.

4.5.4.2.15 Данные, касающиеся особых условий

355) Карточка мастерской способна хранить данные, касающиеся особых условий, таким же образом, как и карточка водителя.

356) Карточка мастерской способна хранить, как минимум, ~~4~~ **2** такие записи.

4.5.4.2.16 Статус аутентификации в случае местоположений, связанных с местами, в которых начинаются и/или заканчиваются ежедневные периоды работы (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

356a) Карточка мастерской способна хранить дополнительные данные о местах, в которых начинаются и/или заканчиваются ежедневные периоды работы, таким же образом, как и карточка водителя.

356b) Карточка мастерской способна хранить 4 пары таких записей.

4.5.4.2.17 Статус аутентификации в случае местоположений, в которых накапливаются три часа управления (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

356c) Карточка мастерской способна хранить дополнительные данные, касающиеся местоположения транспортного средства, когда накопленное время управления достигает значения, кратного трем часам, таким же образом, как и карточка водителя.

356d) Карточка мастерской способна хранить, как минимум, **24** такие записи.

4.5.4.2.18 Статус пересечения границы (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

356e) Карточка мастерской способна хранить данные о пересечении границ таким же образом, как и карточка водителя.

356f) Блок памяти карточки мастерской способен хранить 4 такие записи.

4.5.4.2.19 Операции по загрузке/разгрузке (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

356g) Карточка мастерской способна хранить данные об операциях по загрузке/разгрузке таким же образом, как и карточка водителя.

356h) Карточка мастерской способна хранить данные о 8 операциях по загрузке, разгрузке или одновременной операции по загрузке/разгрузке.

4.5.4.2.20 Записи о типе груза (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

356i) Карточка мастерской способна хранить записи о типе груза таким же образом, как и карточка водителя.

356j) Карточка мастерской способна хранить 4 такие записи.

4.5.4.2.21 Дополнительные данные о калибровке (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

356k) Карточка мастерской способна хранить дополнительные данные о калибровке, применимые только к версии 2:

- старую дату и прежнее время, а также идентификационный номер транспортного средства, которые должны быть точно такими же, как и значения, сохраненные в папке «EF Calibration» в специальном файле «DF Tachograph_G2»;
- тип груза по умолчанию, введенный во время этой калибровки;
- страна, в которой была выполнена калибровка, а также дата и время, когда местоположение, использованное для определения этой страны, было установлено по приемнику ГНСС.

356l) Карточка мастерской способна хранить 255 таких записей.

4.5.4.2.22 Конфигурации БУ (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

356m) Карточка мастерской способна хранить конкретные настройки держателя карточки тахографа.

356n) Объем памяти карточки мастерской для хранения конкретных настроек держателя карточки тахографа составляет 3072 байта.

4.5.5 Карточка контролера

4.5.5.1 Приложение тахографа (доступно для бортовых устройств первого и второго поколений)

4.5.5.1.1 Идентификационные данные приложения

357) Карточка контролера способна хранить следующие идентификационные данные приложения:

- идентификационные данные приложения тахографа;
- идентификационные данные типа карточки тахографа.

4.5.5.1.2 Ключи и сертификаты

358) Карточка контролера способна хранить целый ряд криптографических ключей и сертификатов, как указано в части А приложения подраздела 11.

4.5.5.1.3 Идентификационные данные карточки

359) Карточка контролера способна хранить следующие идентификационные данные карточки:

- номер карточки;
- ~~выдавшее ее государство-член,~~ **Договаривающаяся сторона, выдавшая карточку**, название выдавшего компетентного органа, дата выдачи;
- дата начала срока действия карточки, дата истечения срока действия карточки (если указана).

4.5.5.1.4 Идентификационные данные держателя карточки

360) Карточка контролера способна хранить следующие идентификационные данные держателя карточки:

- название контрольного органа;
- адрес контрольного органа;
- фамилия держателя;
- имя (имена) держателя;
- предпочитаемый язык.

4.5.5.1.5 Данные о деятельности по контролю

361) Карточка контролера способна хранить следующие данные о деятельности по контролю:

- дата и время контроля;
- тип контроля (вывод на дисплей и/или на печать и/или загрузка данных с БУ) и/или загрузка с карточки ~~и/или проверка калибровки на дорогах~~;
- период, за который загружаются данные (в соответствующих случаях),
- VRN и регистрирующий орган ~~государства члена Договаривающейся стороны~~ контролируемого транспортного средства;
- номер карточки и ~~государство член, выдавший карточку, Договаривающаяся сторона, выдавшая~~ контролируемую карточку водителя.

362) Карточка контролера способна хранить, как минимум, 230 таких записей.

4.5.5.2 Приложение тахографа G2 (в случае бортовых устройств первого поколения эта функция недоступна)

4.5.5.2.1 Идентификационные данные приложения

363) Карточка контролера способна хранить следующие идентификационные данные приложения:

- идентификационные данные приложения тахографа,
- идентификационные данные типа карточки тахографа.

4.5.5.2.1.1 Дополнительные идентификационные данные приложения (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

363а) Карточка контролера способна хранить дополнительные идентификационные данные приложения, применимые только к версии 2.

4.5.5.2.2 Ключи и ~~Сертификаты~~ сертификаты

364) Карточка контролера способна хранить ряд криптографических ключей и сертификатов, как указано в части В приложения подраздела 11.

4.5.5.2.3 Идентификационные данные карточки

365) Карточка контролера способна хранить следующие идентификационные данные карточки:

- номер карточки;
- ~~выдавшее ее~~ **государство член, Договаривающаяся сторона, выдавшая карточку**, название выдавшего компетентного органа, дата выдачи;

- дата начала срока действия карточки, дата истечения срока действия карточки (если указана).

4.5.5.2.4 Идентификационные данные держателя карточки

366) Карточка контролера способна хранить следующие идентификационные данные держателя карточки:

- название контрольного органа;
- адрес контрольного органа;
- фамилия держателя;
- имя (имена) держателя;
- предпочитаемый язык.

4.5.5.2.5 Данные о деятельности по контролю

367) Карточка контролера способна хранить следующие данные о деятельности по контролю:

- дата и время контроля;
- тип контроля (вывод на дисплей и/или на печать и/или загрузка данных с БУ и/или загрузка данных с карточки и/или проверка калибровки на дорогах);
- период, за который загружаются данные (в соответствующих случаях);
- VRN и регистрирующий орган ~~государства-члена~~ **Договаривающейся стороны** контролируемого транспортного средства;
- номер карточки и ~~государство-член, выдавший карточку,~~ **Договаривающаяся сторона, выдавшая контролируемую карточку** водителя.

368) Карточка контролера способна хранить, как минимум, 230 таких записей.

4.5.5.2.6 Конфигурации БУ (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

368a) Карточка контролера способна хранить конкретные настройки тахографа держателя карточки.

368b) Объем памяти карточки контролера для хранения конкретных настроек держателя карточки тахографа составляет 3072 байта.

4.5.6 Карточка предприятия

4.5.6.1 Приложение тахографа (доступно для бортовых устройств первого и второго поколений)

4.5.6.1.1 Идентификационные данные приложения

369) Карточка предприятия способна хранить следующие идентификационные данные приложения:

- идентификационные данные приложения тахографа;
- идентификационные данные типа карточки тахографа.

4.5.6.1.2 Ключи и ~~Сертификаты~~ **сертификаты**

370) Карточка предприятия способна хранить целый ряд криптографических ключей и сертификатов, как указано в части А ~~приложения~~ **подраздела 11.**

4.5.6.1.3 Идентификационные данные карточки

371) Карточка предприятия способна хранить следующие идентификационные данные карточки:

- номер карточки;
- ~~выдавшее ее государство – член Договаривающаяся сторона,~~ **выдавшая карточку**, название выдавшего компетентного органа, дата выдачи;
- дата начала срока действия карточки, дата истечения срока действия карточки (если указана).

4.5.6.1.4 Идентификационные данные держателя карточки

372) Карточка предприятия способна хранить следующие идентификационные данные держателя карточки:

- название предприятия;
- адрес предприятия.

4.5.6.1.5 Данные о деятельности предприятия

373) Карточка предприятия способна хранить следующие данные о деятельности предприятия:

- дата и время деятельности;
- тип деятельности (блокировка и/или разблокировка БУ, и/или загрузка данных с БУ и/или загрузка данных с карточки);
- период, за который загружаются данные (в соответствующих случаях);
- VRN и регистрирующий орган **Договаривающейся стороны транспортного средства**;
- номер карточки и ~~государство – член, выдавший карточку,~~ **Договаривающаяся сторона, выдавшая карточку** (в случае загрузки данных карточки).

374) Карточка предприятия способна хранить, как минимум, 230 таких записей.

4.5.6.2 Приложение тахографа G2 (в случае бортовых устройств первого поколения эта функция недоступна)

4.5.6.2.1 Идентификационные данные приложения

375) Карточка предприятия способна хранить следующие идентификационные данные приложения:

- идентификационные данные приложения тахографа;
- идентификационные данные типа карточки тахографа.

4.5.6.2.1.1 Дополнительные идентификационные данные приложения (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

375a) Карточка предприятия способна хранить дополнительные идентификационные данные приложения, применимые только к версии 2.

4.5.6.2.2 Ключи и ~~Сертификаты~~ сертификаты

376) Карточка предприятия способна хранить ряд криптографических ключей и сертификатов, как указано в части В приложения подраздела 11.

4.5.6.2.3 Идентификационные данные карточки

377) Карточка предприятия способна хранить следующие идентификационные данные карточки:

- номер карточки;
- ~~выдавшее~~ ~~ее~~ ~~государство-член~~, **Договаривающаяся сторона, выдавшая карточку**, название выдавшего компетентного органа, дата выдачи;
- дата начала срока действия карточки, дата истечения срока действия карточки (если указана).

4.5.6.2.4 Идентификационные данные держателя карточки

378) Карточка предприятия способна хранить следующие идентификационные данные держателя карточки:

- название предприятия;
- адрес предприятия.

4.5.6.2.5 Данные о деятельности предприятия

379) Карточка предприятия способна хранить следующие данные о деятельности предприятия:

- дата и время деятельности;
- тип деятельности (блокировка и/или разблокировка БУ, и/или загрузка данных с БУ и/или загрузка данных с карточки);
- период, за который загружаются данные (в соответствующих случаях);
- VRN и регистрирующий орган ~~государства-члена~~ **Договаривающейся стороны** транспортного средства;
- номер карточки и ~~государство-член~~, ~~выдавшее~~ ~~карточку~~, **Договаривающаяся сторона, выдавшая карточку** (в случае загрузки данных карточки).

380) Карточка предприятия способна хранить, как минимум, 230 таких записей.

4.5.6.2.6 Конфигурации БУ (в случае версии 1 бортовых устройств второго поколения эта функция недоступна)

380а) Карточка предприятия способна хранить конкретные настройки тахографа владельца карточки.

380б) Объем памяти карточки предприятия для хранения конкретных настроек владельца карточки тахографа составляет 3072 байта.

5. Установка записывающего оборудования контрольного устройства

5.1 Установка

381) Новое ~~записывающее оборудование~~ **контрольное устройство** поставляется техникам или изготовителям транспортного средства неактивированным со всеми параметрами калибровки, перечисленными в главе 3.21, с установленными соответствующими и действительными значениями по умолчанию. Если конкретное значение не подходит, то буквенные параметры устанавливаются в виде строк «?», а числовые параметры устанавливаются на «0». Поставка соответствующих комплектующих ~~записывающего оборудования~~, **контрольного устройства**, имеющих

отношение к обеспечению безопасности, может быть ограничена, если это требуется в ходе процедуры сертификации безопасности.

382) До активации ~~записывающее—оборудование~~ **контрольное устройство** подключают к функции калибровки, даже если оно не находится в режиме калибровки.

383) До активации ~~записывающее—оборудование~~ **контрольное устройство** не регистрирует и не хранит данные, предусмотренные в **требованиях 102–133** ~~пунктах 3.12.3, 3.12.9 и 3.12.12–3.12.15~~, включительно. Тем не менее до своей активации **контрольное устройство может записывать и хранить данные о событиях, имеющих отношение к попыткам нарушения безопасности в соответствии с требованием 117, а также неисправности контрольного устройства в соответствии с требованием 118.**

384) В процессе установки изготовители транспортных средств предварительно устанавливают все известные параметры.

385) Изготовители транспортных средств или техники активируют установленное ~~записывающее—оборудование~~ **контрольное устройство** не позднее начала эксплуатации транспортного средства в соответствии с **Регламентом (ЕС) № 561/2006 настоящим Соглашением.**

386) Активация ~~записывающего—оборудования~~ **контрольного устройства** происходит автоматически в результате первого ввода действительной карточки мастерской в любое из считывающих устройств карточки.

387) Конкретные операции по соединению датчика движения и бортового устройства, если таковые требуются, производятся автоматически до или во время активации.

388) Аналогичным образом конкретные операции по подсоединению внешнего устройства ГНСС и бортового устройства, если таковые требуются, производятся автоматически до или во время активации.

389) После активации ~~записывающее—оборудование~~ **контрольное устройство** полностью вводит в действие функции и права доступа к данным.

390) После активации ~~записывающее—оборудование~~ **контрольное устройство** передает устройству удаленной связи защищенные данные, необходимые для целевых проверок на дорогах.

391) Функции регистрации и хранения ~~записывающего—оборудования~~ **контрольного устройства** после его активации полностью работоспособны.

392) После установки производится калибровка. Первая калибровка не обязательно должна включать в себя ввод регистрационного ~~номера идентификационного кода~~ транспортного средства (VRN и **Договаривающаяся страна**), если уполномоченной мастерской, которая проводит калибровку, он неизвестен. В этих обстоятельствах владельцу транспортного средства, и только в это время, предоставляется возможность ввести VRN и код **Договаривающейся стороны** с помощью своей карточки предприятия до использования транспортного средства на основании **Регламента (ЕС) № 561/2006 настоящего Соглашения** (например, с использованием команд, предусмотренных в соответствующем меню человеко-машинного интерфейса бортового устройства⁴⁹). Любое обновление или подтверждение такого ввода данных возможно только с помощью карточки мастерской.

393) Установка внешнего устройства ГНСС предполагает необходимость соединения с бортовым устройством и последующей проверки информации ГНСС о местоположении.

394) ~~Записывающее—оборудование~~ **Контрольное устройство** должно быть установлено в транспортном средстве таким образом, чтобы водитель имел доступ ко всем необходимым функциям со своего места.

¹⁰ OJL 11.4.2006, p1.

5.2 Установочная табличка

395) После проверки установленного ~~записывающего оборудования~~ **контрольного устройства** к нему крепится несъемная четко видимая и легко доступная установочная табличка с выгравированным или напечатанным нестираемым текстом, который четко виден и удобочитаем. Если это невозможно, табличка крепится к средней стойке транспортного средства таким образом, чтобы она была хорошо видна. Если в транспортном средстве средней стойки нет, то установочная табличка крепится **в районе двери** ~~дверной рамы~~ со стороны водителя транспортного средства, с тем чтобы она была хорошо заметной во всех случаях.

После каждой инспекции, проведенной уполномоченным техником или мастерской, на месте прежней таблички устанавливается новая.

396) На табличке указываются, по крайней мере, следующие сведения:

- название, адрес или фирменный знак уполномоченного техника или мастерской;
- характеристический коэффициент транспортного средства в виде « $w = \text{имп./км}$ »;
- постоянная величина ~~записывающего оборудования~~ **контрольного устройства** в виде « $k = \dots \text{имп./км}$ »;
- эффективная окружность шин колес в виде « $l = \dots \text{мм}$ »;
- размер шин;
- дата определения характеристического коэффициента транспортного средства и измерения эффективной окружности шин колес;
- идентификационный номер транспортного средства;
- наличие (или отсутствие) внешнего устройства ГНСС;
- серийный номер внешнего устройства ГНСС, **в случае применимости**;
- серийный номер устройства удаленной связи, **в случае наличия**;
- серийный номер всех имеющихся пломб;
- часть транспортного средства, в которой установлен адаптер, в случае наличия;
- часть транспортного средства, в которой установлен датчик движения, если он не соединен с коробкой передач или если не используется адаптер;
- описание цвета кабеля между адаптером и частью транспортного средства, из которой поступают входящие импульсы;
- серийный номер встроенного датчика движения адаптера;
- **тип груза по умолчанию, ассоциируемый с транспортным средством.**

397) Только для автомобилей M1 и N1, которые оснащены адаптером в соответствии с ~~Регламентом (ЕС) № 68/2009¹¹~~ ~~субприложение~~ **подразделом 16** с последними изменениями, и в том случае, если включить всю необходимую информацию, как описано в требовании 396, невозможно, то можно использовать вторую, дополнительную, табличку. В таких случаях на дополнительной табличке ~~присутствует~~ **предусмотрено** не менее четырех пунктов, как описано в требовании 396.

Если используется такая же вторая дополнительная табличка, то она крепится рядом или поблизости от первой основной таблички, как описано в требовании 396, с тем же уровнем защиты. Кроме того, на второй табличке также указываются название, адрес

¹¹ OJL 21.1.2009, p. 3.

или фирменный знак уполномоченного техника или мастерской, установившего или установившей данные таблички, и дата установки.

5.3 Наложение пломб

398) Пломбы накладываются на следующие части:

- любое соединение, которое в случае рассоединения повлечет за собой невыявляемые изменения или потерю данных (например, это может касаться установки датчика движения на коробке передач, адаптера для транспортных средств M1/N1, внешнего соединения ГНСС или бортового устройства);
- установочную табличку, если она не прикреплена таким образом, что ее нельзя снять, не повредив нанесенную на ней маркировку.

398a) Упомянутые выше пломбы сертифицируются в соответствии со стандартом EN 16882:2016¹².

399) Указанные выше пломбы могут быть сняты:

- в случае аварийной ситуации;
- в целях установки, регулировки или ремонта устройства ограничения скорости или любого иного устройства обеспечения безопасности дорожного движения, при условии что ~~записывающее оборудование~~ **контрольное устройство** продолжает функционировать надежно и правильно и снова опломбировано уполномоченным техником или мастерской (в соответствии с главой 6) сразу же после установки устройства ограничения скорости или любого иного устройства обеспечения безопасности дорожного движения или, в иных случаях, в течение семи дней.

400) Каждый случай повреждения пломб должен быть предметом письменного уведомления компетентного органа с указанием причин, по которым были произведены такие действия.

401) На пломбах указывается их идентификационный номер, присваиваемый им изготовителем. Этот номер должен быть уникальным и отличным от любого другого номера пломбы, присвоенного другим изготовителем пломб.

Такой уникальный идентификационный номер составляется следующим образом: нестираемая маркировка ~~MM NNNNNN~~ **MMNNNNNNNN**, где MM — уникальный идентификационный номер изготовителя (регистрация в базе данных, подчиненной ЕК), а ~~NNNNNN NNNNNNNN~~ — это буквенно-цифровой номер, уникальный для данного изготовителя.

402) На пломбах предусмотрено свободное пространство, на котором уполномоченные техники, мастерские или изготовители транспортных средств могут добавить особую метку ~~в соответствии со статьей 22.3 Регламента (ЕС) № 165/2014~~.

Такая метка не должна закрывать идентификационный номер пломбы.

403) Изготовители пломб регистрируются в специальной базе данных **в тот момент, когда они получают модель пломбы, сертифицированной в соответствии с EN 16882:2016**, и доводят свои идентификационные номера пломб до общего сведения ~~в соответствии с процедурой, установленной Европейской комиссией~~.

404) Уполномоченные мастерские и изготовители транспортных средств в рамках ~~Регламента (ЕС) № 165/2014~~ **настоящего Соглашения используют пломбы сертифицированные пломбы в соответствии с EN 16882:2016** только тех изготовителей пломб, которые перечислены в упомянутой базе данных.

¹² Переход на стандарт ИСО планируется осуществить в течение пяти лет.

405) Изготовители пломб и их распространители ведут записи, обеспечивающие полную отслеживаемость сбытых пломб, используемых в рамках ~~Регламента (ЕС) № 165/2014~~ **настоящего Соглашения**, и в случае необходимости готовы их предоставить компетентным национальным органам.

406) На установочной табличке уникальные идентификационные номера пломб должны быть видны.

6. Проверки, инспекции и ремонтные работы

Требования к обстоятельствам, в случае которых можно снять пломбы, ~~как указано в статье 22.5 Регламента (ЕС) № 165/2014~~, представлены в главе 5.3 **настоящего дополнения добавления**.

6.1 Утверждение техников, мастерских и изготовителей транспортных средств

~~Государства-члены~~ **Договаривающиеся стороны** утверждают, регулярно контролируют и аттестуют организации, которым поручены следующие задачи:

- установка;
- проверки;
- инспекции;
- ремонтные работы.

Карточки мастерской выдаются только тем техникам и/или мастерским, которые уполномочены активировать и/или калибровать ~~записывающее оборудование~~ **контрольное устройство** в соответствии с настоящим ~~дополнением~~ **добавлением** и в случае должного обоснования:

- тем, кто не имеет права на карточку предприятия;
- и иная профессиональная деятельность которых не может поставить под угрозу общую защиту системы в соответствии с требованиями ~~приложения~~ **подраздела 10**.

6.2 Проверка новых или отремонтированных ~~приборов~~ компонентов

407) Каждое отдельное устройство, новое или отремонтированное, проверяется на предмет его надлежащего функционирования и точности показаний и записей в пределах, указанных в главе 3.2.1, 3.2.2, 3.2.3 и 3.3, ~~посредством наложения пломб в соответствии с главой 5.3 и параметрами калибровки~~.

6.3 Инспекция установки

408) После установки на транспортное средство весь сборочный узел (включая ~~записывающее оборудование~~ **контрольное устройство**) соответствует положениям, регламентирующим максимальные допуски, указанные в главах 3.2.1, 3.2.2, 3.2.3 и 3.3. **Весь сборочный узел пломбируется в соответствии с главой 5.3 и включает калибровку.**

6.4 Периодические инспекции

409) Регулярные инспекции оборудования, установленного на транспортных средствах, производятся после любого ремонта такого оборудования или после любого изменения характеристического коэффициента транспортного средства или эффективной окружности шин, или в том случае, если часы, показывающие время

UTC, спешат или отстают более чем на ~~5~~ 20 минут, или в случае изменения VRN и не реже одного раза в два года (24 месяца) после последней инспекции.

410) Такие инспекции включают в себя следующие проверки с целью убедиться в том:

- что ~~записывающее оборудование~~ **контрольное устройство** работает должным образом, включая функцию хранения данных на карточках тахографов и связь со считывающими устройствами удаленной связи;
- что обеспечивается соблюдение положений главы 3.2.1 и 3.2.2 о максимальных допусках при установке;
- что обеспечивается соблюдение положений главы 3.2.3 и 3.3;
- что на ~~записывающем оборудовании~~ **контрольном устройстве** нанесен знак официального утверждения типа;
- что установочная табличка, как определено в требовании 396, **и** описательная табличка, как определено в требовании 225, **закреплены**;
- что размер шин и фактическая окружность шин колес соответствуют требованиям;
- что к оборудованию не прикреплены никакие средства манипулирования;
- что пломбы правильно размещены и находятся в хорошем состоянии, что их идентификационные номера действительны (присвоены изготовителем пломб в базе данных ЕК) и что их идентификационные номера соответствуют маркировке на установочной табличке (см. требование 401);
- **что идентификатор версии сохраненной цифровой карты является самым последним.**

410а) В случае обнаружения какой-либо манипуляции компетентными национальными органами, транспортное средство может быть отправлено в уполномоченную мастерскую для повторной калибровки контрольного устройства.

411) Если обнаруживается, что с момента последней инспекции произошло одно из событий, перечисленных в главе 3.9 (обнаружение событий и/или неисправностей), и изготовители тахографов и/или национальных органов считают, что оно может подвергнуть риску безопасность оборудования, мастерская:

a) сравнивает идентификационные данные датчика движения, подключенного к коробке передач, с данными спаренного датчика движения, зарегистрированного в бортовом устройстве;

b) проверяет, соответствует ли информация, указанная на установочной табличке, информации в записях бортового устройства;

c) проверяет, соответствуют ли серийный номер и номер официального утверждения датчика движения, если они нанесены на корпусе датчика движения, информации, хранящейся в блоке памяти ~~записывающего оборудования~~ **контрольного устройства**;

d) сравнивает идентификационные данные на описательной табличке внешнего устройства ГНСС, если оно есть, с данными, хранящимися в блоке памяти бортового устройства.

412) Мастерские в своих отчетах об инспекциях хранят любые установленные факты о поврежденных пломбах или устройствах для манипулирования. Такие отчеты хранятся в мастерских не менее 2 лет и предоставляются компетентным органам по их требованию.

413) Такие инспекции включают в себя калибровку и профилактическую замену пломб, за установку которых отвечают мастерские.

6.5 Измерение погрешностей

414) Измерение погрешностей при установке или в ходе эксплуатации осуществляется на следующих условиях, которые должны рассматриваться как стандартные условия испытаний:

- транспортное средство в снаряженном состоянии без груза;
- давление в шинах соответствует инструкциям изготовителя;
- износ шин в пределах, допускаемых национальным законодательством;
- движение транспортного средства:
- транспортное средство движется вперед своим ходом по прямой линии по ровной дороге на скорости 50 ± 5 км/ч. Измеряемое расстояние составляет не менее 1000 метров;
- при условии сопоставимой точности, для испытания можно использовать и альтернативные методы, например, подходящий испытательный стенд.

6.6 Ремонтные работы

415) Мастерские имеют возможность загружать данные с ~~записывающего оборудования~~ **контрольного устройства** для их передачи соответствующему транспортному предприятию.

416) Официально утвержденные мастерские выдают транспортным предприятиям свидетельство, подтверждающее невозможность загрузки данных в том случае, когда неисправность ~~записывающего оборудования~~ **контрольного устройства** не позволяет загрузить ранее записанные данные даже после ремонта, произведенного данной мастерской. Мастерские хранят копию каждого выданного свидетельства не менее двух лет.

7. Выдача карточек

Порядок выдачи карточек, установленный ~~государствами-членами Договаривающимися сторонами~~, соответствует следующим предписаниям:

417) В случае первой выдачи карточки тахографа присваиваемый заявителю номер карточки имеет порядковый индекс (в случае применимости), индекс замены и индекс возобновления, установленные на «0».

418) В случае всех неиндивидуальных карточек тахографа, выданных одному контрольному органу, или одной мастерской или одному транспортному предприятию, первые 13 цифр номеров карточек одинаковые, а порядковый индекс для всех разный.

419) Карточка тахографа, выданная в порядке замены существующей карточки, имеет тот же номер, что и номер замененной карточки, за исключением индекса замены, который увеличивается на «1» (в порядке 0, ..., 9, A, ..., Z).

420) Карточка тахографа, выданная в порядке замены существующей карточки, имеет ту же дату истечения срока действия, что и замененная карточка.

421) Карточка тахографа, выданная в порядке возобновления существующей карточки, имеет тот же номер, что и номер возобновляемой карточки, за исключением индекса замены, который устанавливается на «0», и индекса возобновления, который увеличивается на «1» (в порядке 0, ..., 9, A, ..., Z).

422) Обмен существующей карточки тахографа в целях изменения административной даты производится в соответствии с правилами возобновления, если это происходит в том же государстве-члене той же Договаривающейся стороне, или в соответствии с правилами первой выдачи карточки, если это происходит в другом государстве-члене другой Договаривающейся стороне.

423) В графе «фамилия держателя карточки» в случае неиндивидуальных карточек мастерской или карточек контролера, указывается название мастерской или контрольного органа, или фамилия техника или контролера, если государство-член принимает такое решение.

~~Государства-члены обмениваются данными в электронном виде, чтобы обеспечить уникальность карточек водителя, которые они выдают, в соответствии с Регламентом (ЕС) № 165/2014.~~

424) Зарезервирован.

8. Утверждение типа записывающего оборудования контрольного устройства и карточек тахографов

8.1 Общие вопросы

В настоящем разделе выражение ~~записывающее оборудование~~ «**контрольное устройство**» означает ~~записывающее оборудование~~ «**контрольное устройство** или его компоненты». Для кабеля (кабелей) соединения датчика движения с БУ, **внешнего устройства ГНСС с БУ или устройства удаленной связи с БУ** официальное утверждение типа не требуется. Бумага, используемая в ~~записывающем оборудовании~~ **контрольном устройстве**, считается компонентом ~~записывающего оборудования~~ **контрольного устройства**.

Любой изготовитель может обращаться за официальным утверждением типа компонента(ов) ~~его контрольного устройства~~ с любым(и) другим(и) компонентом(ами) его **контрольного устройства** ~~типом датчика движения, внешнего устройства ГНСС и наоборот~~, если каждый из этих компонентов соответствует требованиям настоящего добавления. В качестве варианта изготовители могут также обращаться за официальным утверждением типа ~~записывающего оборудования~~ **контрольных устройств**.

~~Записывающее оборудование~~ **Бортовые устройства** могут иметь свои варианты сборки компонентов. Независимо от сборки компонентов бортовых устройств **внешняя антенна и (если применимо) антенный разветвитель, подключенные к приемнику ГНСС или к средству удаленной связи, не являются частью официального утверждения типа бортового устройства.**

Тем не менее изготовители, получившие официальное утверждение типа **контрольного устройства**, ведут общедоступный перечень совместимых антенн и разветвителей с каждым официально утвержденным бортовым устройством, **внешним средством ГНСС и внешним средством удаленной связи.**

425) **Контрольное устройство** представляется на официальное утверждение в комплекте с любыми встроенными дополнительными устройствами.

426) Официальное утверждение типа ~~записывающего оборудования~~ **контрольного устройства** и карточек тахографа включает в себя испытания средств защиты, функциональные испытания и испытания на эксплуатационную совместимость. Положительные результаты каждого из таких испытаний подтверждаются соответствующим сертификатом.

427) Органы официального утверждения типа ~~государств-членов Договаривающихся сторон~~ не выдают сертификат официального утверждения типа, если нет:

- сертификата защиты (**если это предусмотрено настоящим подразделом**);
- сертификата функциональности;
- и сертификата эксплуатационной совместимости (**если это предусмотрено настоящим подразделом**).

428) Любое изменение программного обеспечения или аппаратного оборудования или характера материалов, использованных для его изготовления, доводится в предварительном порядке до сведения компетентного органа, который предоставил официальное утверждение данного типа оборудования. Такой орган подтверждает изготовителю факт продления действия утверждения типа или может потребовать обновления или подтверждения соответствующих сертификатов функциональности, защиты и/или эксплуатационной совместимости.

429) Процедуры ~~модернизации~~ **обновления** на месте программного обеспечения ~~записывающего оборудования~~ **контрольного устройства** утверждаются органом, который предоставил официальное утверждение типа ~~записывающего оборудования~~ **контрольного устройства**. При ~~модернизации~~ **обновлении** программного обеспечения нельзя изменять или удалять никакие данные о деятельности водителя, которые хранятся в памяти ~~записывающего оборудования~~ **контрольного устройства**. ~~Модернизация~~ **Обновление** программного обеспечения может производиться только под ответственность изготовителя оборудования.

430) Официальное утверждение типа изменений программного обеспечения в целях ~~модернизации~~ **обновления** ~~записывающего оборудования~~ **контрольного устройства** ранее утвержденного типа не может быть отклонено, если такие изменения относятся только к функциям, не указанным в настоящем ~~дополнении~~ добавлении. ~~Модернизация~~ **Обновление** программного обеспечения ~~записывающего оборудования~~ **контрольного устройства** может не включать введение новых наборов символов, если это технически неосуществимо.

8.2 Сертификат защиты

431) Сертификат защиты выдается в соответствии с положениями ~~приложения~~ **подраздела 10** настоящего **добавления**. Подлежащие сертификации компоненты **контрольного устройства** включают в себя бортовое устройство, датчик движения, внешнее устройство ГНСС и карточки тахографа.

432) В исключительных обстоятельствах, когда органы, сертифицирующие систему защиты, отказываются сертифицировать новое оборудование на том основании, что механизмы защиты устарели, практика официального утверждения продолжает тем не менее действовать в таких особых и исключительных обстоятельствах и только в том случае, если альтернативного решения, соответствующего ~~Регламенту~~ **настоящему Соглашению**, не существует.

433) В подобных случаях ~~соответствующее государство-член~~ **соответствующая Договаривающаяся сторона** незамедлительно информирует ~~Европейскую комиссию, которая~~ **другие Договаривающиеся стороны** о том, что в течение двенадцати календарных месяцев после предоставления официального утверждения типа **она не будет инициировать** процедуру восстановления уровня безопасности до исходного уровня.

8.3 Сертификат функциональности

434) Каждый претендент на получение официального утверждения типа направляет компетентному органу ~~государства-члена~~ **Договаривающейся стороны**,

предоставляющему официальное утверждение типа, все материалы и документацию, которые такой компетентный орган считает необходимыми.

435) Изготовители предоставляют соответствующие образцы изделий, претендующих на официальное утверждение типа, и связанные с ними документы, требуемые лабораториями, на которые возложена ответственность за проведение функциональных испытаний, в течение одного месяца с момента подачи заявки. Все расходы, связанные с этой заявкой, берет на себя подающий ее субъект. Лаборатории хранят конфиденциальность всей информации, представляющей собой коммерческую тайну.

436) Сертификат функциональности выдается изготовителю только по итогам всех успешно проведенных функциональных испытаний, предусмотренных, как минимум, в ~~приложении~~ **подразделе 9**.

437) Орган по официальному утверждению типа выдает сертификат функциональности. В таком сертификате, помимо названия его получателя и идентификационных данных образца, приводится подробный перечень проведенных испытаний и полученных результатов.

438) Сертификат функциональности любого компонента ~~записывающего оборудования~~ **контрольного устройства** также содержит номера официального утверждения типа компонентов другого совместимого ~~записывающего оборудования~~ **контрольного устройства** утвержденного типа, прошедших испытания для получения настоящего сертификата.

439) Сертификат функциональности любого компонента ~~записывающего оборудования~~ **контрольного устройства** также содержит ссылку на стандарт ИСО или ЕКС, на основании которого сертифицирован данный функциональный интерфейс.

8.4 Сертификат эксплуатационной совместимости

440) Испытания на эксплуатационную совместимость проводятся ~~одной лабораторией под руководством и при ответственности Европейской комиссии~~ **одним компетентным органом**.

441) Лаборатория регистрирует заявки на проведение проверок на эксплуатационную совместимость, подаваемые изготовителями, в хронологическом порядке их поступления.

442) Заявки официально регистрируются только в случае предоставления в распоряжение лаборатории:

- всего комплекта материалов и документов, необходимых для проведения таких испытаний на эксплуатационную совместимость;
- соответствующего сертификата защиты;
- соответствующего сертификата функциональности.

Дата регистрации заявки доводится до сведения изготовителя.

443) Лаборатория не проводит испытаний на эксплуатационную совместимость ~~записывающего оборудования~~ **контрольных устройств** или карточек тахографов, на которые ~~не прошли анализ на уязвимость в ходе их оценки~~ **выданы сертификат защиты и сертификат соответствующей оценки** функциональности, кроме как в случае исключительных обстоятельств, указанных в требовании 432.

444) Любой изготовитель, подавший заявку на проведение испытаний на эксплуатационную совместимость, берет на себя обязательство передать на хранение лаборатории, уполномоченной проводить эти испытания, весь комплект материалов и документов, которые он предоставил для проведения испытаний.

445) Испытания на эксплуатационную совместимость проводятся в соответствии с положениями ~~приложения~~ **подраздела 9** настоящего ~~дополнения~~ **добавления** в отношении всех типов ~~записывающего оборудования~~ **контрольного устройства** или карточек тахографа, в случае которых:

- срок действия официального утверждения типа еще не истек; или
- официальное утверждение типа еще не выдано, но выдан действительный сертификат эксплуатационной совместимости.

446) Испытания на эксплуатационную совместимость распространяются на все поколения ~~записывающего оборудования~~ **контрольного устройства** или карточек тахографов, которые еще используются.

447) Сертификат функциональной совместимости выдается и передается лабораторией изготовителю только после успешного прохождения всех требуемых испытаний на функциональную совместимость **и после того, как изготовитель подтвердит, что на данное изделие выдан как действительный сертификат функциональности, так и действительный сертификат защиты, кроме исключительных обстоятельств, изложенных в требовании 432.**

448) Если одна или несколько единиц ~~записывающего оборудования~~ **контрольного устройства** или карточек тахографа не прошли испытания на эксплуатационную совместимость, то сертификат эксплуатационной совместимости не выдается до тех пор, пока изготовитель, подавший соответствующую заявку, не внесет необходимые изменения и не проведет успешные испытания на эксплуатационную совместимость. Лаборатория определяет причину проблемы с помощью изготовителей, которых касается данное несоответствие требованиям к эксплуатационной совместимости, и стремится оказать изготовителю, подавшему заявку, помощь в поиске соответствующего технического решения. Если изготовитель модифицировал свое изделие, он обязан удостовериться в соответствующих компетентных органах в том, что срок действия сертификата защиты и сертификатов функциональности еще не истек.

449) Сертификат эксплуатационной совместимости действует в течение шести месяцев. Если изготовитель не получил соответствующий сертификат официального утверждения типа, то срок его действия в конце этого периода истекает. Изготовитель передает его компетентному органу ~~государства-члена~~, **Договаривающейся стороны, выдающему** официальное утверждение типа, который выдал данный сертификат функциональности.

450) Любой элемент, который может явиться причиной несоответствия требованиям к эксплуатационной совместимости, не должен использоваться в целях получения выгоды или приводить к созданию доминирующего положения.

8.5 Сертификат официального утверждения типа

451) Орган ~~государства-члена~~ **Договаривающейся стороны**, выдающий официальное утверждение типа, может выдавать сертификат официального утверждения типа после получения всех трех требуемых сертификатов.

452) Сертификат официального утверждения типа любого компонента ~~записывающего оборудования~~ **контрольного устройства** также содержит номера официального утверждения типа другого совместимого ~~записывающего оборудования~~ **контрольного устройства** официально утвержденного типа.

453) Копия сертификата официального утверждения типа направляется компетентным органом, выдающим официальное утверждение типа, лаборатории, уполномоченной проводить испытания на эксплуатационную совместимость, в момент его выдачи изготовителю.

454) Лаборатория, в компетенцию которой входят испытания на эксплуатационную совместимость, поддерживает общедоступный веб-сайт, на котором обновляется

перечень образцов записывающего оборудования контрольного устройства или карточек тахографа:

- в случае которых зарегистрирован запрос на проведение испытаний на эксплуатационную совместимость;
- которые получили сертификат эксплуатационной совместимости (даже временный);
- которые получили сертификат официального утверждения типа.

~~7.6 — Исключительная процедура: первые сертификаты эксплуатационной совместимости для записывающего оборудования и карточек тахографов второго поколения~~

~~455) До истечения четырех месяцев после подтверждения эксплуатационной совместимости первой пары записывающего оборудования и карточек тахографов второго поколения (карточек водителя, мастерской, карточки контролера и карточки предприятия), любой сертификат эксплуатационной совместимости (включая первые), выданный по запросам, зарегистрированным в течение этого периода, считается временным.~~

~~456) Если по окончании этого периода все изделия совместимы, все соответствующие сертификаты эксплуатационной совместимости становятся постоянными.~~

~~457) Если в течение этого периода обнаруживаются несоответствия требованиям эксплуатационной совместимости, лаборатория, ответственная за испытания на эксплуатационную совместимость, находит причины проблем с помощью всех заинтересованных изготовителей и предлагает им внести необходимые изменения.~~

~~458) Если по окончании этого периода проблемы эксплуатационной совместимости не устранены, лаборатория, ответственная за испытания эксплуатационной совместимости, в сотрудничестве с заинтересованными изготовителями и органами по официальному утверждению типа, выдавшими соответствующие сертификаты функциональности, устанавливает причины несоответствия требованиям эксплуатационной совместимости и принимают решение о том, какие изменения должен внести каждый заинтересованный изготовитель. Поиск технических решений длится не более двух месяцев, после чего, если общее решение не найдено, Комиссия, после консультации с лабораторией, ответственной за испытания эксплуатационной совместимости, принимает решение, на какое оборудование и на какие карточки выдать постоянные сертификаты эксплуатационной совместимости, и указывает причины своего решения.~~

~~459) Любые заявки на испытания в целях проверки эксплуатационной совместимости, регистрируемые лабораторией по истечении четырехмесячного периода после выдачи первого временного свидетельства на эксплуатационную совместимость и даты решения Комиссии, указанного в требовании 455, откладываются до разрешения начальных проблем с эксплуатационной совместимостью. Впоследствии такие заявки обрабатываются в хронологическом порядке их регистрации.~~

ПРИЛОЖЕНИЕ

ДОБАВЛЕНИЕ

ЗНАК ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ И СЕРТИФИКАТ

I. ЗНАК ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ

1. Знак официального утверждения состоит из:

а) прямоугольника, внутри которого изображена буква «е», за которой следует отличительный номер или буквенный код страны, выдавшей официальное утверждение, в соответствии со следующими условными знаками:

Редакционное примечание: В списке должны быть перечислены все Договаривающиеся стороны

Австрия	12,
Бельгия	6,
Болгария	34,
Венгрия	7,
Германия	1,
Греция	23,
Дания	18,
Ирландия	24,
Испания	9,
Италия	3,
Кипр	СУ
Латвия	32,
Литва	36,
Люксембург	13,
Мальта	МТ,
Нидерланды	4,
Польша	20,
Португалия	21,
Румыния	19,
Словакия	27,
Словения	26,
Соединенное Королевство	11,
Финляндия	17
Франция	2,
Хорватия	25,

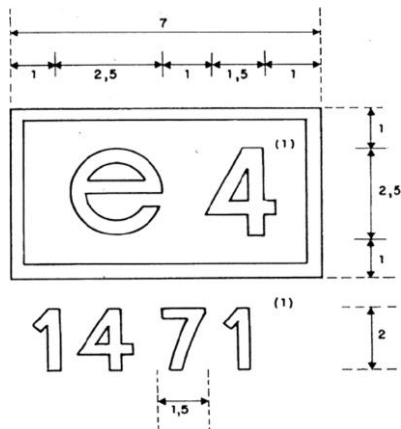
Чешская Республика	8,
Швеция	5,
Эстония	29.

а) прямоугольника, внутри которого изображена буква «е», за которой следует отличительный номер или буквенный код страны, выдавшей официальное утверждение, в соответствии со следующими условными знаками:

б) номера официального утверждения, соответствующего номеру сертификата официального утверждения, выданного на прототип регистрирующего оборудования **контрольного устройства**, или номеру регистрационного списка или номеру карточки тахографа, размещенного в любом месте в непосредственной близости от этого прямоугольника.

2. Знак официального утверждения указывается на описательной табличке каждого комплекта оборудования, в каждом регистрационном списке и на каждой карточке тахографа. Он должен быть нестираемым и всегда оставаться четким и разборчивым.

3. Размеры знака официального утверждения, изображенного ниже (1), выражены в миллиметрах, причем эти размеры являются минимальными. Соотношения между размерами должны сохраняться.



(1) Эти цифры приведены только в качестве рекомендации.

II. СЕРТИФИКАТ ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ АНАЛОГОВЫХ ТАХОГРАФОВ

~~Государство-член, предоставившее~~ Договаривающаяся сторона, предоставившая официальное утверждение, выдает заявителю сертификат официального утверждения, образец которого приведен ниже. В порядке информирования других ~~государств-членов Договаривающихся сторон~~ об официальных утверждениях, выданных или, в случае возникновения необходимости, отмененных, ~~государство-член~~ должен Договаривающаяся сторона использовать копии этого сертификата.

СЕРТИФИКАТ ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ

- Наименование компетентного административного органа
- Уведомление, касающееся⁽¹⁾:
- официальное утверждение типа ~~записывающего оборудования~~ **контрольного устройства**
- отмена официального утверждения типа ~~записывающего оборудования~~ **контрольного устройства**
- утверждение образца регистрационного списка
- изъятие образца регистрационного списка

Официальное утверждение №:.....

1. Торговое наименование или товарный знак
2. Название типа или модели
3. Название изготовителя
-
-
-
4. Адрес изготовителя
5. Представлено на официальное утверждение (дата)
6. Проверено на
7. Дата и номер испытания(ий)
8. Дата официального утверждения
9. Дата отмены официального утверждения
10. Тип или типы ~~записывающего оборудования~~ **контрольного устройства**, в случае которого следует использовать этот формуляр
11. Место
12. Дата
13. Прилагаемые описательные документы
14. Замечания (включая указание места наложения пломб, в случае применимости)
-

(Подпись)

⁽¹⁾ Неприменимые позиции исключить

III. СЕРТИФИКАТ ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ ЦИФРОВЫХ ТАХОГРАФОВ

Государство-член, предоставившее Договаривающаяся сторона, предоставившая официальное утверждение, выдает заявителю сертификат официального утверждения, образец которого приведен ниже. В порядке информирования других государств-членов Договаривающихся сторон об официальных утверждениях, выданных или, в случае возникновения необходимости, отмененных, государство-член Договаривающаяся сторона использует экземпляры этого сертификата.

СЕРТИФИКАТ ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ АНАЛОГОВЫХ ТАХОГРАФОВ

Наименование компетентного административного органа

Уведомление, касающееся⁽¹⁾:

- официального утверждения:
- отмены официального утверждения:
- образца записывающего оборудования **контрольного устройства**
- компонента⁽²⁾ образца записывающего оборудования **контрольного устройства**
- карточки водителя
- карточки мастерской
- карточки предприятия
- карточка контролера

Официальное утверждение №:

1. Торговое наименование или товарный знак
2. Название модели
3. Наименование изготовителя
4. Адрес изготовителя
5. Представлено на официальное утверждение (дата)
6. Лаборатория(и)
7. Дата и номер протокола испытания(ий)
8. Дата официального утверждения
9. Дата отмены официального утверждения
10. Модель записывающего оборудования **контрольного устройства (контрольных устройств)**, на котором следует использовать этот компонент
11. Место
12. Дата
13. Прилагаемые описательные документы
14. Примечания (включая указание места наложения пломб, в случае применимости)

(Подпись)

⁽¹⁾ Сделать отметку в соответствующих клетках.

⁽²⁾ Указать данный компонент, отраженный в уведомлении.

IV. СЕРТИФИКАТ ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ СМАРТ-ТАХОГРАФОВ

~~Государство-член, предоставившее~~ Договаривающаяся сторона, предоставившая официальное утверждение, выдает заявителю сертификат официального утверждения, которого приведен ниже. В порядке информирования других ~~государств-членов~~ Договаривающихся сторон об официальных утверждениях, выданных или, в случае возникновения необходимости, отмененных, ~~государство-член~~ Договаривающаяся сторона использует экземпляры этого сертификата.

СЕРТИФИКАТ ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ СМАРТ-ТАХОГРАФОВ

Наименование компетентного административного органа

Уведомление, касающееся⁽¹⁾:

- официального утверждения:
- отмены официального утверждения:
- модели ~~записывающего оборудования~~ **контрольного устройства**
- компонента ~~записывающего оборудования~~ **контрольного устройства**⁽²⁾
- карточки водителя
- карточки мастерской
- карточки предприятия
- карточка контролера

Официальное утверждение №:

1. Торговое наименование или товарный знак
2. Название модели
3. Наименование изготовителя
4. Адрес изготовителя
5. Представлено на официальное утверждение (дата)
6.
 - a Испытательная лаборатория для функциональной сертификации
 - b Испытательная лаборатория для сертификации безопасности
 - c Испытательная лаборатория для сертификации эксплуатационной совместимости
7.
 - a Дата и номер сертификата функциональности
 - b Дата и номер сертификата безопасности
 - c Дата и номер сертификата эксплуатационной совместимости
8. Дата официального утверждения
9. Дата отмены официального утверждения
10. Модель ~~записывающего оборудования~~ **контрольного устройства (контрольных устройств)**, в случае которого(ых) следует использовать этот компонент
11. Место
12. Дата
13. Прилагаемые описательные документы
14. Примечания (включая указание места наложения пломб, в случае применимости)

(Подпись)

⁽¹⁾ Сделать отметку в соответствующих клетках.

⁽²⁾ Указать данный компонент, отраженный в уведомлении.

Добавление Подраздел 1**Словарь данных****Содержание**

	<i>Стр.</i>
1. Введение	125
1.1 Метод определения типов данных	125
1.2 Справочные материалы	125
2. Определения типов данных	126
2.1 ActivityChangeInfo (данные об изменении вида деятельности)	126
2.2 Address (адрес)	128
2.3 AESKey (ключ AES)	128
2.4 AES128Key (ключ AES128)	128
2.5 AES192Key (ключ AES192)	129
2.6 AES256Key (ключ AES256)	129
2.7 BCDString (строка BCD)	129
2.8 CalibrationPurpose (цель калибровки)	129
2.9 CardActivityDailyRecord (запись вида деятельности на карточке)	130
2.10 CardActivityLengthRange (длина записи о деятельности на карточке)	131
2.11 CardApprovalNumber (номер официального утверждения карточки)	131
2.11a CardBorderCrossings (данные на карточке о пересечении границы)	131
2.11b CardBorderCrossingRecord (запись на карточке о пересечении границы)	131
2.12 CardCertificate (сертификат карточки)	132
2.13 CardChipIdentification (идентификация микросхемы карточки)	132
2.14 CardConsecutiveIndex (порядковый индекс карточки)	132
2.15 CardControlActivityDataRecord (запись данных на карточке о деятельности по контролю)	133
2.16 CardCurrentUse (текущее использование карточки)	133
2.17 CardDriverActivity (запись на карточке о деятельности водителя)	133
2.18 CardDrivingLicenceInformation (информация о водительском удостоверении на карточке)	134
2.19 CardEventData (данные о событиях на карточке)	135
2.20 CardEventRecord (запись о событиях на карточке)	135
2.21 CardFaultData (данные о сбоях в работе карточки)	136
2.22 CardFaultRecord (запись о сбоях в работе карточки)	136
2.23 CardIccIdentification (идентификация карточки ИС)	136
2.24 CardIdentification (идентификация карточки)	137
2.24a CardLoadTypeEntries (данные о типе груза на карточке)	137
2.24b CardLoadTypeEntryRecord (запись данных о типе груза на карточке)	138
2.24c CardLoadUnloadOperations (операции по загрузке/разгрузке на карточке)	138

2.24d	CardLoadUnloadRecord (запись об операциях загрузки/разгрузки на карточке)	139
2.25	CardMACertificate (сертификат карточки МА)	139
2.26	CardNumber (номер карточки)	139
2.26a	CardPlaceAuthDailyWorkPeriod (разрешенный ежедневный период работы и место, указанные на карточке)	140
2.27	CardPlaceDailyWorkPeriod (ежедневный период работы и место, указанные на карточке)	140
2.28	CardPrivateKey (закрытый ключ карточки)	141
2.29	CardPublicKey (открытый ключ карточки)	141
2.30	CardRenewalIndex (индекс возобновления карточки)	141
2.31	CardReplacementIndex (индекс замены карточки)	141
2.32	CardSignCertificate (сертификат подписи карточки)	141
2.33	CardSlotNumber (номер считывающего устройства карточки)	141
2.34	CardSlotsStatus (статус считывающих устройств карточки)	142
2.35	CardSlotsStatusRecordArray (статус считывающих устройств карточки и метаданные)	142
2.36	CardStructureVersion (версия структуры карточки)	142
2.37	CardVehicleRecord (запись использования транспортного средства на карточке)	143
2.38	CardVehiclesUsed (использованное транспортное средство)	144
2.39	CardVehicleUnitRecord (запись использованных единиц транспортных средств)	144
2.40	CardVehicleUnitsUsed (использованные единицы транспортных средств)	145
2.41	Certificate (сертификат)	145
2.42	CertificateContent (содержание сертификата)	145
2.43	CertificateHolderAuthorisation (идентификатор прав держателя сертификата)	146
2.44	CertificateRequestID (идентификатор запроса на сертификат)	146
2.45	CertificationAuthorityKID (сертификационный орган KID)	147
2.46	CompanyActivityData (данные об операциях с карточкой предприятия)	147
2.47	CompanyActivityType (тип операции, произведенной предприятием)	148
2.48	CompanyCardApplicationIdentification (идентификация приложения карточки предприятия)	149
2.48a	CompanyCardApplicationIdentificationV2 (идентификация приложения карточки предприятияV2)	149
2.49	CompanyCardHolderIdentification (идентификация держателя карточки предприятия)	149
2.50	ControlCardApplicationIdentification (идентификация приложения карточки контролера)	150
2.50a	ControlCardApplicationIdentificationV2 (идентификация приложения карточки контролераV2)	150
2.51	ControlCardControlActivityData (данные о проверочных операциях на карточке контролера)	150

2.52	ControlCardHolderIdentification (идентификация держателя карточки контролера)	151
2.53	ControlType (тип контроля)	151
2.54	CurrentDateTime (текущая дата/время)	153
2.55	CurrentDateTimeRecordArray (данные о текущей дате/времени и метаданные)	153
2.56	DailyPresenceCounter (счетчик ежедневного присутствия)	153
2.57	Datef (формат даты)	154
2.58	DateOfDayDownloaded (дата и время загрузки)	154
2.59	DateOfDayDownloadedRecordArray (данные о дне и времени загрузки и метаданные)	154
2.60	Distance (расстояние)	155
2.60a	DownloadInterfaceVersion(версия загрузочного интерфейса)	155
2.61	DriverCardApplicationIdentification (идентификация приложения карточки водителя)	155
2.61a	DriverCardApplicationIdentificationV2 (идентификация приложения карточки водителяV2)	156
2.62	DriverCardHolderIdentification (идентификация держателя карточки водителя)	157
2.63	DSRCSecurityData (система защиты данных DSRCs)	157
2.64	EGFCertificate (сертификат EGF)	158
2.65	EmbedderIcAssemblerId (идентификатор монтажного/сборочного предприятия)	158
2.66	EntryTypeDailyWorkPeriod (ввод данных о периоде и типе ежедневной работы)	158
2.67	EquipmentType (тип оборудования)	159
2.68	EuropeanPublicKey (европейский открытый ключ)	160
2.69	EventFaultRecordPurpose (цель регистрации события или неисправности)	160
2.70	EventFaultType (событие: тип неисправности)	161
2.71	ExtendedSealIdentifier (расширенный идентификатор пломбы)	166
2.72	ExtendedSerialNumber (расширенный серийный номер)	166
2.73	FullCardNumber (полный номер карточки)	167
2.74	FullCardNumberAndGeneration (полный номер и поколение карточки)	167
2.75	Generation (поколение)	168
2.76	GeoCoordinates (геокоординаты)	168
2.77	GNSSAccuracy (точность ГНСС)	168
2.78	GNSSAccumulatedDriving (накопленное время управления по ГНСС)	168
2.79	GNSSAccumulatedDrivingRecord (запись накопленного времени управления по ГНСС)	169
2.79a	GNSSAuthAccumulatedDriving (разрешенное накопленное время управления по ГНСС)	169
2.79b	GNSSAuthStatusADRecord (запись данных в БУ о НакБУ по ГНСС)	170
2.79c	GNSSPlaceAuthRecord (запись аутентифицированного места по ГНСС)	170
2.80	GNSSPlaceRecord (запись названия места по ГНСС)	171

2.81	HighResOdometer (счетчик пробега с высоким разрешением)	171
2.82	HighResTripDistance (расстояние, пройденное за рейс, с высоким разрешением)	171
2.83	HolderName (фамилия и имя (имена) держателя)	171
2.84	Зарезервировано для будущего использования	172
2.85	K-ConstantOfRecordingEquipment (постоянная К записывающего оборудования)	172
2.86	KeyIdentifier (идентификатор ключа)	172
2.87	KMWCKey (ключ KMWC)	172
2.88	Language (язык)	173
2.89	LastCardDownload (последняя дата загрузки с карточки)	173
2.89a	LengthOfFollowingData (длина следующих данных)	173
2.90	LinkCertificate (связывающий сертификат)	173
2.90a	LoadType (тип груза)	173
2.91	L-TyreCircumference (окружность шины L)	173
2.92	MAC (MAC)	174
2.93	ManualInputFlag (метка ручного ввода)	174
2.94	ManufacturerCode (код изготовителя)	174
2.95	ManufacturerSpecificEventFaultData (данные о неисправности, связанной с конкретным изготовителем)	174
2.96	MemberStateCertificate (сертификат государства-члена)	175
2.97	MemberStateCertificateRecordArray (записи о сертификате государства-члена и метаданные)	175
2.98	MemberStatePublicKey (открытый ключ государства-члена)	175
2.99	Name (название)	175
2.100	NationAlpha (буквенный код страны)	176
2.101	NationNumeric (цифровой код страны)	176
2.101a	NoOfBorderCrossingRecords (число записей о пересечении границы)	176
2.102	NoOfCalibrationRecords (число записей о калибровках)	176
2.103	NoOfCalibrationsSinceDownload (число калибровок после загрузки данных)	176
2.104	NoOfCardPlaceRecords (число записей на карточке, касающихся мест)	177
2.105	NoOfCardVehicleRecords (число записей, касающихся транспортных средств, на карточке)	177
2.106	NoOfCardVehicleUnitRecords (число записей на карточке, касающихся единиц транспортных средств)	177
2.107	NoOfCompanyActivityRecords (число записей, касающихся операций предприятия)	177
2.108	NoOfControlActivityRecords (число записей, касающихся операций по контролю)	177
2.109	NoOfEventsPerType (число событий по типу)	178
2.110	NoOfFaultsPerType (число неисправностей по типу)	178
2.111	NoOfGNSSADRecords (число записей ГНСС, касающихся НакВУ)	178

2.111a	NoOfLoadUnloadRecords (число записей, касающихся загрузки/разгрузки)	178
2.112	NoOfSpecificConditionRecords (число записей, касающихся особых условий)	178
2.112a	NoOfLoadTypeEntryRecords (число записей о типе поступившего груза)	178
2.113	OdometerShort (показания счетчика пробега)	179
2.114	OdometerValueMidnight (показания счетчика пробега в полночь)	179
2.114a	OperationType (тип операции)	179
2.115	OdometerValueMidnightRecordArray (показания счетчика пробега в полночь и метаданные)	179
2.116	OverspeedNumber (число превышений скорости)	180
2.116a	PlaceAuthRecord (запись аутентификации места)	180
2.116b	PlaceAuthStatusRecord (запись статуса аутентификации места)	180
2.117	PlaceRecord (место, в котором начинается или заканчивается ежедневный период работы)	181
2.117a	PositionAuthenticationStatus (статус аутентификации местоположения)	182
2.118	PreviousVehicleInfo (информация о предыдущем транспортном средстве)	182
2.119	PublicKey (открытый ключ)	182
2.120	RecordType (тип записи)	183
2.121	RegionAlpha (буквенный код региона)	184
2.122	RegionNumeric (числовой код района)	184
2.123	RemoteCommunicationModuleSerialNumber (серийный номер модуля удаленной связи)	185
2.124	RSAPublicModulus (модуль ключа RSA)	185
2.125	RSAPrivateExponent (закрытая экспонента ключа RSA)	186
2.126	RSAPublicExponent (открытая экспонента ключа RSA)	186
2.127	RtmData (данные удаленного мониторинга тахографа)	186
2.128	SealDataCard (данные, касающиеся пломб, указанных на карточке)	186
2.129	SealDataVu (данные, касающиеся пломб, в БУ)	186
2.130	SealRecord (запись, касающаяся пломб)	187
2.131	SensorApprovalNumber (номер официального утверждения датчика)	187
2.132	SensorExternalGNSSApprovalNumber (номер официального утверждения внешнего датчика ГНСС)	187
2.133	SensorExternalGNSSCoupledRecord (запись о соединении внешнего датчика ГНСС)	188
2.134	SensorExternalGNSSIdentification (идентификационные данные внешнего датчика ГНСС)	188
2.135	SensorExternalGNSSInstallation (данные, касающиеся установки внешнего датчика ГНСС)	188
2.136	SensorExternalGNSSOSIdentifier (идентификатор внешнего датчика ОС ГНСС)	189
2.137	SensorExternalGNSSK3Identifier (идентификатор внешнего датчика КЗ ГНСС)	189
2.138	SensorGNSSCouplingDate (дата соединения датчика ГНСС с БУ)	189
2.139	SensorGNSSSerialNumber (серийный номер датчика ГНСС)	190

2.140	SensorIdentification (идентификация датчика)	190
2.141	SensorInstallation (установка датчика)	190
2.142	SensorInstallationSecData (данные, касающиеся защиты при установке датчика)	191
2.143	SensorOSIdentifier (идентификатор ОС датчика)	191
2.144	SensorPaired (подсоединенный датчик)	191
2.145	SensorPairedRecord (запись данных о подсоединении датчика)	192
2.146	SensorPairingDate (дата подсоединения датчика)	192
2.147	SensorSCIdentifier (идентификатор КЗ датчика)	192
2.148	SensorSerialNumber (серийный номер датчика)	192
2.149	Signature (подпись)	192
2.150	SignatureRecordArray (набор подписей и метаданные)	193
2.151	SimilarEventsNumber (число похожих событий)	193
2.152	SpecificConditionRecord (запись особых условий)	193
2.153	SpecificConditions (особые условия)	194
2.154	SpecificConditionType (тип особых условий)	194
2.155	Speed (скорость)	194
2.156	SpeedAuthorised (разрешенная скорость)	195
2.157	SpeedAverage (средняя скорость)	195
2.158	SpeedMax (максимальная скорость)	195
2.158a	TachographCardsGenI Suppression (отмена карточек тахографа первого поколения)	195
2.159	TachographPayload (пакет данных тахографа)	195
2.160	Reserved for future use (зарезервировано для использования в будущем)	195
2.161	TDesSessionKey (тройной ключ сеанса в системе TDes)	196
2.162	TimeReal (реальное время)	196
2.163	TyreSize (размер шин)	196
2.164	VehicleIdentificationNumber (идентификационный номер транспортного средства)	196
2.165	VehicleIdentificationNumberRecordArray (идентификационный номер транспортного средства и метаданные)	197
2.166	VehicleRegistrationIdentification (идентификация регистрации транспортного средства)	197
2.166a	VehicleRegistrationIdentificationRecordArray (идентификация регистрации транспортного средства и метаданные)	197
2.167	VehicleRegistrationNumber (регистрационный номер транспортного средства)	198
2.168	VehicleRegistrationNumberRecordArray (регистрационный номер транспортного средства и метаданные)	198
2.169	VuAbility (характеристики БУ)	198
2.170	VuActivityDailyData (данные в БУ о деятельности за данный день)	199
2.171	VuActivityDailyRecordArray (данные в БУ о деятельности или статусе и метаданные)	199

2.172	VuApprovalNumber (номер официального утверждения БУ)	200
2.173	VuCalibrationData (данные в БУ о калибровке)	200
2.174	VuCalibrationRecord (запись в БУ о калибровке)	200
2.175	VuCalibrationRecordArray (данные в БУ о калибровке и метаданные)	203
2.176	VuCardIWData (данные в БУ о циклах ввода и извлечения карточек)	204
2.177	VuCardIWRecord (запись данных в БУ о циклах ввода и извлечения карточек)	204
2.178	VuCardIWRecordArray (данные о циклах ввода и извлечения карточек и метаданные)	205
2.179	VuCardRecord (запись данных в БУ об используемой карточке)	206
2.180	VuCardRecordArray (данные об используемых карточках и метаданные)	206
2.181	VuCertificate (сертификат БУ)	207
2.182	VuCertificateRecordArray (сертификат БУ и метаданные)	207
2.183	VuCompanyLocksData (данные в БУ о блокировке предприятием)	207
2.184	VuCompanyLocksRecord (запись данных в БУ о блокировке предприятием)	208
2.185	VuCompanyLocksRecordArray (запись данных в БУ о блокировке предприятием и метаданные)	208
2.185a	VuConfigurationLengthRange (длина данных о конфигурации БУ)	209
2.186	VuControlActivityData (данные в БУ о контроле за деятельностью)	209
2.187	VuControlActivityRecord (запись данных в БУ о контроле за деятельностью)	209
2.188	VuControlActivityRecordArray (запись данных в БУ о контроле за деятельностью и метаданные)	210
2.189	VuDataBlockCounter (счетчик нумерации циклов ввода и извлечения карточек в БУ)	210
2.190	VuDetailedSpeedBlock (данные в БУ о скорости транспортного средства)	211
2.191	VuDetailedSpeedBlockRecordArray (данные в БУ о скорости транспортного средства и метаданные)	211
2.192	VuDetailedSpeedData (детальные данные в БУ о скорости транспортного средства)	211
2.192a	VuDigitalMapVersion (версия цифровой карты в БУ)	212
2.193	VuDownloadablePeriod (сроки хранения данных в БУ)	212
2.194	VuDownloadablePeriodRecordArray (сроки хранения записей данных в БУ и метаданные)	212
2.195	VuDownloadActivityData (данные в БУ о загрузке)	213
2.196	VuDownloadActivityDataRecordArray (данные в БУ о загрузке и метаданные)	213
2.197	VuEventData (данные в БУ о событиях)	214
2.198	VuEventRecord (запись данных в БУ о событиях)	214
2.199	VuEventRecordArray (запись данных в БУ о событиях и метаданные)	216
2.200	VuFaultData (данные в БУ о неисправностях)	216
2.201	VuFaultRecord (запись данных в БУ о неисправностях)	216
2.202	VuFaultRecordArray (запись данных в БУ о неисправностях и метаданные)	218
2.203	VuGNSSCDRECORDVuGNSSADRecord (запись данных в БУ о НаКБУ по ГНСС)	218

2.203a	VuBorderCrossingRecord (запись данных в БУ о пересечении границы)	219
2.203b	VuBorderCrossingRecordArray (запись данных в БУ о пересечении границы и метаданные)	220
2.204	VuGNSSCDRecordArray (запись данных в БУ о НакВУ по ГНСС и метаданные)	220
2.204a	VuGnssMaximalTimeDifference (данные в БУ о максимальной разнице во времени по ГНСС)	221
2.205	VuIdentification (идентификация бортового устройства)	221
2.206	VuIdentificationRecordArray (идентификация БУ и метаданные)	222
2.207	VuITSConsentRecord (запись в БУ о согласии водителя использовать ИТС)	222
2.208	VuITSConsentRecordArray (запись в БУ о согласии водителя использовать ИТС и метаданные)	223
2.208a	VuLoadUnloadRecord (запись данных в БУ о загрузке/разгрузке)	223
2.208b	VuLoadUnloadRecordArray (запись данных в БУ о загрузке/ разгрузке и метаданные)	224
2.209	VuManufacturerAddress (адрес изготовителя БУ)	224
2.210	VuManufacturerName (наименование изготовителя БУ)	224
2.211	VuManufacturingDate (дата изготовления БУ)	225
2.212	VuOverSpeedingControlData (данные в БУ о превышении скорости)	225
2.213	VuOverSpeedingControlDataRecordArray (данные в БУ о превышении скорости и метаданные)	225
2.214	VuOverSpeedingEventData (данные в БУ о событиях превышения скорости)	226
2.215	VuOverSpeedingEventRecord (запись данных в БУ о событиях превышения скорости)	226
2.216	VuOverSpeedingEventRecordArray (запись данных в БУ о событиях превышения скорости и метаданные)	227
2.217	VuPartNumber (номер детали БУ)	227
2.218	VuPlaceDailyWorkPeriodData (данные в БУ о месте, где начинается и заканчивается ежедневный период работы)	228
2.219	VuPlaceDailyWorkPeriodRecord (запись данных в БУ о месте, где начинается и заканчивается ежедневный период работы)	228
2.220	VuPlaceDailyWorkPeriodRecordArray (запись данных в БУ о месте, где начинается и заканчивается ежедневный период работы, и метаданные)	229
2.221	VuPrivateKey (закрытый ключ БУ)	229
2.222	VuPublicKey (открытый ключ БУ)	230
2.222a	VuRtcTime (время в БУ по часам реального времени)	230
2.223	VuSerialNumber (серийный номер БУ)	230
2.224	VuSoftInstallationDate (дата установки программного обеспечения БУ)	230
2.225	VuSoftwareIdentification (идентификация программного обеспечения БУ)	230
2.226	VuSoftwareVersion (версия программного обеспечения БУ)	230
2.227	VuSpecificConditionData (данные об особых условиях в БУ)	231
2.228	VuSpecificConditionRecordArray (данные об особых условиях в БУ и метаданные)	231
2.229	VuTimeAdjustmentData (данные в БУ о корректировке времени)	231

2.230	Reserved for future use (зарезервирован для использования в будущем)	232
2.231	Reserved for future use (зарезервирован для использования в будущем)	232
2.232	VuTimeAdjustmentRecord (запись данных в БУ о корректировке времени)	232
2.233	VuTimeAdjustmentRecordArray (запись данных в БУ о корректировке времени и метаданные)	233
2.234	WorkshopCardApplicationIdentification (идентификация приложения карточки мастерской)	234
2.234a	WorkshopCardApplicationIdentificationV2 (идентификация приложения карточки мастерскойV2)	235
2.234b	WorkshopCardCalibrationAddData (запись дополнительных данных калибровки карточки мастерской)	235
2.234c	WorkshopCardCalibrationAddDataRecord (запись дополнительных данных калибровки карточки мастерской)	236
2.235	WorkshopCardCalibrationData (данные калибровки карточки мастерской)	236
2.236	WorkshopCardCalibrationRecord (запись данных калибровки карточки мастерской)	237
2.237	WorkshopCardHolderIdentification (идентификация держателя карточки мастерской)	239
2.238	WorkshopCardPIN (ПИН-код карточки мастерской)	239
2.239	W-VehicleCharacteristicConstant (характеристическая постоянная W транспортного средства)	239
2.240	VuPowerSupplyInterruptionRecord (запись данных в БУ о прекращении электропитания)	239
2.241	VuPowerSupplyInterruptionRecordArray (запись данных в БУ о прекращении электропитания и метаданные)	240
2.242	VuSensorExternalGNSSCoupledRecordArray (запись данных в БУ о соединении с внешним датчиком ГНСС и метаданные)	241
2.243	VuSensorPairedRecordArray (запись данных о спаренном датчике БУ и метаданные)	241
3.	Определения диапазона значений и размеров	241
4.	Наборы символов	242
5.	Кодирование	242
6.	Идентификаторы объектов и идентификаторы приложений	243
6.1	Идентификаторы объектов	243
6.2	Идентификаторы приложений	244

1. Введение

В настоящем **подразделе** уточняются форматы данных, элементы данных и структуры данных, подлежащие использованию в ~~записывающем оборудовании~~ **контрольном устройстве** и карточках тахографа.

1.1 Метод определения типов данных

Для определения типов данных в настоящем **подразделе** используется абстрактное описание синтаксиса версии 1 (ASN.1). Эта система позволяет определить простые и структурированные данные, не прибегая к помощи какого-либо конкретного синтаксиса передачи (правил кодирования), который зависит от приложения и операционной среды.

Правила присвоения названий типа ASN.1 соответствуют стандарту ISO/IEC 8824.1. Это предполагает, что:

- при возможности, смысл соответствующего типа данных косвенно заложен в выбранных названиях;
- если какой-либо тип данных состоит из других типов данных, название этого типа данных и в этом случае представляет собой простую последовательность буквенных знаков, которая начинается с заглавной буквы; вместе с тем заглавные буквы используются и в названии с целью придать данным соответствующий смысл;
- в целом, название типов данных соотносится с названием тех типов данных, с помощью которых они построены, с оборудованием, в которых хранятся данные, и с функцией, имеющей отношение к этим данным.

Если какой-либо тип ASN.1 уже определен в качестве того или иного стандарта и если он подходит для использования в ~~записывающем оборудовании~~ **контрольном устройстве**, то в данном приложении будет определен и этот тип ASN.1.

Для того чтобы можно было использовать несколько типов правил кодирования, некоторые типы ASN.1 в настоящем ~~приложении~~ **подразделе** ограничиваются соответствующими идентификаторами диапазона значений. Идентификаторы диапазона значений определяются в пункте 3 и **подразделе добавления** 2.

1.2 Справочные материалы

В настоящем **подразделе** ~~приложении~~ используются следующие источники:

ISO 639	Код отображения названий языков. Первое издание: 1988 год
ISO 3166	Коды стран ИСО, отображающие их названия и административно-территориальные единицы — Часть 1: Коды стран, 2013 год
ISO 3779	Транспорт дорожный — Идентификационный номер транспортного средства (VIN) — Содержание и структура. 2009 год
ISO/IEC 7816-5	Идентификационные карточки — карточки на интегральной микросхеме — Часть 5: Регистрация подателей заявок. Второе издание: 2004 год
ISO/IEC 7816-6	Идентификационные карточки — карточки на интегральной микросхеме — Часть 6: Межотраслевые элементы данных для обмена, 2004 год + техническая поправка 1: 2006 год
ISO/IEC 8824-1	Информационные технологии — Абстрактное описание синтаксиса версии 1 (ASN.1): Спецификация основных описаний. 2008 год + техническая поправка 1: 2012 год и техническая поправка 2: 2014 год

ISO/IEC 8825-2	Информационные технологии. Правила кодирования ASN.1: спецификация правил уплотненного кодирования (PER). Издание 2: 2008 год
ISO/IEC 8859-1	Информационные технологии. 8-битные однобайтовые кодированные наборы графических символов — Часть 1: Латинский алфавит № 1. Первое издание: 1998 год
ISO/IEC 8859-7	Информационные технологии. 8-битные однобайтовые кодированные наборы графических символов — Часть 7: Латинский/греческий алфавит. 2003 год
ISO 16844-3	Транспорт дорожный. Системы тахографов. Интерфейс датчика движения. 2004 + Техническая поправка 1: 2006 год
TR-03110-3	Технические руководящие принципы BSI/ANSSI TR-03110-3, механизмы повышенной безопасности для машиночитываемых проездных документов и идентификатор eIDAS — Часть 3: общие спецификации, версия 2.20, 3. Февраль 2015 года

2. Определения типов данных ~~Определения типов~~

В случае любого из следующих типов данных значение по умолчанию позиции «нет данных» или «неприменимо» определяется посредством заполнения соответствующего элемента данных с помощью **шестнадцатиричных** байтов FF, если не указано иное.

Все типы данных используются для приложений первого и второго поколений, если не указано иначе.

В случае типов карточек данных, используемых только для поколения 2, предлагается использовать приложения версии 2. В случае типов данных, используемых для приложений поколения 1 и поколения 2, размер, указанный в данном подразделе, является размером, предусмотренным для приложения поколения 2. Предполагается, что размер для приложения поколения 1 читателю уже известен. Номера требований в приложении 1С, относящиеся к таким типам данных, охватывают приложения как поколения 1, так и поколения 2.

Типы карточек данных, не определенные для карточек поколения 1, в приложении поколения 1 к карточкам поколения 2 не хранятся. В частности:

- номера официального утверждения типа, хранящиеся в приложении поколения 1 карточек поколения 2, при необходимости усекаются до 8 первых знаков;
- в приложении поколения 1 карточек поколения 2 сохраняется только конкретное состояние «FERRY/TRAIN CROSSING begin» (начало ПЕРЕЕЗДА НА ПАРОМЕ/ПОЕЗДЕ) в позиции «FERRY/TRAIN CROSSING» (ПЕРЕЕЗД НА ПАРОМЕ/ПОЕЗДЕ).

2.1 ActivityChangeInfo (данные об изменении вида деятельности)

Этот тип данных позволяет кодировать с помощью слова из двух байтов состояние считывающего устройства в 00:00 часов и/или статус водителя в 00:00 часов и/или изменение вида деятельности и/или изменение статуса управления и/или изменение статуса карточки водителя или второго водителя. Данный тип данных связан с требованиями 105, 266, 291, 320, 321, 343 и 344 в ~~приложении~~ **добавлении 1С**.

ActivityChangeInfo ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(2))

Присвоенное значение — выровненный октет: ‘scpaatttttttt’В (16 бит)

В случае записи данных в блок памяти (или статуса считывающего устройства):

's'В	Считывающее устройство: '0'В: DRIVER (ВОДИТЕЛЬ) '1'В: CO-DRIVER (ВТОРОЙ ВОДИТЕЛЬ)
'с'В	Статус управления: '0'В: SINGLE (ОДИН) '1'В: CREW (ЭКИПАЖ)
'р'В	Статус карточки водителя (или мастерской) в соответствующем считывающем устройстве: '0'В: INSERTED, карточка введена 1'В: NOT INSERTED, карточка не введена (или карточка извлечена)
'aa'В	Деятельность: '00'В: BREAK/REST (перерыв, отдых) '01'В: AVAILABILITY (готовность) '10'В: WORK (работа) '11'В: DRIVING, (управление)
'tttttttt'В	Время изменения: число минут, начиная с 00:00 часов на данный день

Для записи данных на карточку водителя (или мастерской) (и статуса водителя):

's'В	Считывающее устройство (неприменимо, если 'р'=1, за исключением случая, указанного ниже): '0'В: DRIVER (водитель) '1'В: CO-DRIVER (второй водитель)
'с'В	Статус управления (случай 'р'=0) или статус следующего вида деятельности (случай 'р'=1): '0'В: SINGLE (один) '0'В: UNKNOWN (нет данных) '1'В: CREW (экипаж) '1'В: KNOWN (= введено вручную)
'р'В	Статус карточки: '0'В: INSERTED, карточка введена в записывающее оборудование контрольное устройство '1'В: NOT INSERTED, карточка не введена (или извлечена)
'aa'В	Считывающее устройство (неприменимо, если 'р'=1 и 'с'=0, за исключением примечания ниже): '00'В: BREAK/REST (перерыв, отдых) '01'В: AVAILABILITY (готовность) '10'В: WORK (работа) '11'В: DRIVING (управление)
'tttttttt'В	Время изменения: число минут, начиная с 00:00 часов на данный день

Примечание на случай «извлечение карточки»:

Когда карточка извлечена:

- знак 's' применим и указывает на считывающее устройство, из которого извлечена карточка;
- 'с' должно быть установлено на 0;

- ‘p’ должно быть установлено на 1;
- ‘aa’ должно кодировать текущий вид деятельности, выбранный в указанное время.

В результате ручного ввода биты ‘с’ и ‘aa’ в составе слова (хранящиеся в памяти карточки) позднее могут быть удалены и на их место записаны другие данные, отражающие факт этого ввода.

2.2 Address (адрес)

Адрес.

```
Address ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
codePage    ЦЕЛОЕ ЧИСЛО (0..255)
address     ОКТЕТНАЯ СТРОКА (РАЗМЕР35))
}
```

codePage определяет набор символов, указанный в главе 4

address — адрес, закодированный с помощью указанного набора символов

2.3 AESKey (ключ AES)

Поколение 2:

Ключ AES длиной 128, 192 или 256 битов.

```
AESKey ::= ВЫБОР {
aes128Key  AES128Key
aes192Key  AES192Key
aes256Key  AES256Key
}
```

Присвоение значения: дополнительно не указывается.

2.4 AES128Key (ключ AES128)

Поколение 2:

Ключ AES128.

```
AES128Key ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
длина      ЦЕЛОЕ ЧИСЛО (0..255)
aes128Key  ОКТЕТНАЯ СТРОКА (РАЗМЕР(16))
}
```

length обозначает длину ключа AES128 в октетах. **aes128Key** — ключ AES длиной 128 битов.

Присвоение значения:

Значение длины — 16.

2.5 AES192Key (ключ AES192)

Поколение 2:

Ключ AES192.

```
AES128Key ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
длина      ЦЕЛОЕ ЧИСЛО (0..255)
aes192Key  ОКТЕТНАЯ СТРОКА (РАЗМЕР(24))
}
```

length обозначает октетную длину ключа AES192.

aes192Key — ключ AES длиной 192 бита.

Присвоение значения:

Длина должна иметь значение 24.

2.6 AES256Key (ключ AES256)

Поколение 2:

Ключ AES256.

```
AES256Key ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
длина      ЦЕЛОЕ ЧИСЛО (0..255)
aes256Key  ОКТЕТНАЯ СТРОКА (РАЗМЕР(32))
}
```

length обозначает октетную длину ключа AES256.

aes256Key — ключ AES длиной 256 битов.

Присвоение значения:

Длина должна иметь значение 32.

2.7 BCDSString (строка BCD)

BCDSString используется для отображения десятичного числа в двоичном коде (BCD). Этот тип данных используется для отображения одного десятичного знака в одном полуоктете 4 бита). BCDSString определяется в соответствии со стандартом ISO/IEC 8824-1 (тип знаковой строки).

```
BCDSString ::= ЗНАКОВАЯ СТРОКА (С КОМПОНЕНТАМИ {
идентификация (С КОМПОНЕНТАМИ {
устанавливает ПРИСУТСТВИЕ }) })
```

BCDSString использует для описания нотацию “hstring”. Крайняя левая шестнадцатеричная цифра представляет собой самый значимый полуоктет первого октета. Для получения нескольких октетов после крайнего левого полуоктета первого октета включается, при необходимости, соответствующее число нулевых полуоктетов.

Допустимые цифры: 0, 1, .. 9.

2.8 CalibrationPurpose (цель калибровки)

Данный код указывает причину регистрации набора параметров калибровки. Этот тип данных связан с требованиями 097 и 098 приложения добавления 1С и требованиями требованием 119.

CalibrationPurpose ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))

Присвоение значения:

Поколение 1:

- '00'Н зарезервированное значение,
- '01'Н активация: регистрация известных параметров калибровки в момент активации БУ,
- '02'Н первая установка: первая калибровка БУ после его активации,
- '03'Н установка: первая калибровка БУ в данном транспортном средстве,
- '04'Н регулярная проверка,

Поколение 2:

В дополнение к поколению 1, используются следующие значения:

- '05'Н ввод VRN предприятием,
- '06'Н корректировка времени без калибровки,
- '07'Н — '7F'Н RFU, '80'Н — 'FF'Н по усмотрению изготовителя.

2.9 CardActivityDailyRecord (запись вида деятельности на карточке)

Информация, которая хранится на карточке, относится к деятельности водителя за конкретный календарный день. Этот тип данных связан с требованиями 266, 291, 320 и 343 в ~~приложении~~ **добавлении 1С**.

```
CardActivityDailyRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
activityPreviousRecordLength ЦЕЛОЕ ЧИСЛО (0..CardActivityLengthRange)
activityRecordLength ЦЕЛОЕ ЧИСЛО (0..CardActivityLengthRange)
activityRecordDate Реальное время
activityDailyPresenceCounter Счетчик ежедневного присутствия
activityDayDistance Расстояние
activityChangeInfo УСТАНОВЛЕННЫЙ РАЗМЕР (1..1440) ПАРАМЕТРА
ActivityChangeInfo
}
```

activityPreviousRecordLength — общая длина предыдущей ежедневной записи в байтах. Максимальное значение определяется в виде длины ОКТЕТНОЙ СТРОКИ, содержащей эти записи (см. CardActivityLengthRange, ~~приложение~~ **подраздел 2**, пункт 4). Когда эта запись становится самой старой ежедневной записью, значение activityPreviousRecordLength должно устанавливаться на 0.

activityRecordLength — общая длина ежедневной записи в байтах. Максимальное значение определяется в виде длины ОКТЕТНОЙ СТРОКИ, содержащей эти записи.

activityRecordDate — дата записи.

activityDailyPresenceCounter — счетчик ежедневного наличия карточки на данный день.

activityDayDistance — общее расстояние, пройденное за данный день.

activityChangeInfo — набор данных ActivityChangeInfo, относящихся к водителю на данный день. Он может содержать максимум 1440 значений (изменение вида деятельности 1 раз в минуту). Этот набор данных всегда включает кодирование статуса водителя activityChangeInfo на 00:00 часов.

2.10 CardActivityLengthRange (длина записи о деятельности на карточке)

Число байтов на карточке водителя или мастерской, которые предусмотрены для хранения записей, касающихся деятельности водителя.

CardActivityLengthRange ::= ЦЕЛОЕ ЧИСЛО (0..2¹⁶−1)

Присвоение значения: см. приложение подраздел 2.

2.11 CardApprovalNumber (номер официального утверждения карточки)

Номер официального утверждения типа карточки.

CardApprovalNumber ::= Строка IA5 (РАЗМЕР(8))

Присвоение значения:

Номер официального утверждения указывается в том виде, в каком он опубликован на соответствующем ~~веб-сайте Европейской комиссии, т. е. на веб-сайте лаборатории, уполномоченной проводить испытания на эксплуатационную совместимость,~~ т. е., например, включать дефисы, если они нужны. Номер официального утверждения смещается влево.

2.11a CardBorderCrossings (данные на карточке о пересечении границы)

Поколение 2, версия 2:

Информация, хранящаяся на карточке водителя или мастерской, связанная с пересечением границы транспортным средством, когда оно пересекло границу соответствующей страны (требования 306f и 356f добавления 1С).

```
CardBorderCrossings ::=          ПОСЛЕДОВАТЕЛЬНОСТЬ {
borderCrossingPointerNewestRecord ЦЕЛОЕ ЧИСЛО (0..NoOfBorderCrossingRecords−1),
cardBorderCrossingRecords        УСТАНОВЛЕННЫЙ РАЗМЕР
                                   (NoOfBorderCrossingRecords)
                                   ПАРАМЕТРА CardBorderCrossingRecord
}
```

borderCrossingPointerNewestRecord — индекс последней обновленной записи в карточке о пересечении границы.

Присвоение значения — число, соответствующее числителю записи о пересечении границы на карточке, начиная с '0' для первого появления записи о пересечении границы на карточке в структуре данных.

cardBorderCrossingRecords — записи на карточке о пересечении границы.

2.11b CardBorderCrossingRecord (запись на карточке о пересечении границы)

Поколение 2, версия 2:

Информация, хранящаяся на карточке водителя или мастерской, связанная с пересечением границы транспортным средством, когда оно пересекло границу соответствующей страны (требования 147b, 306e и 356e добавления 1С).

```
CardBorderCrossingRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
countryLeft                  Числовой код страны
```

countryEntered	Числовой код страны
gnssPlaceAuthRecord	Запись аутентифицированного места по ГНСС
vehicleOdometerValue	Счетчик пробега
}	

countryLeft — страна, которую покинуло транспортное средство, или «информация отсутствует» в соответствии с требованием 147b добавления 1С. «Остальная часть мира» (числовой код страны 'FF'Н) используется в том случае, когда бортовое устройство не может определить страну, в которой находится транспортное средство (например, данная страна не находит отражения в сохраненных цифровых картах).

countryEntered — страна, в которую въехало транспортное средство, или страна, в которой находится транспортное средство в момент введения карточки. «Остальная часть мира» (числовой код страны 'FF'Н) используется в том случае, когда бортовое устройство не может определить страну, в которой находится транспортное средство (например, данная страна не находит отражения в сохраненных цифровых картах).

gnssPlaceAuthRecord содержит информацию, связанную с местоположением транспортного средства, когда бортовое устройство обнаружило, что транспортное средство пересекло границу страны, или «информация отсутствует» в соответствии с требованием 147b добавления 1С, и его статус аутентификации.

vehicleOdometerValue — показание счетчика пробега, когда бортовое устройство обнаружило, что транспортное средство пересекло границу страны, или «информация отсутствует» в соответствии с требованием 147b добавления 1С.

2.12 CardCertificate (сертификат карточки)

Поколение 1:

Сертификат открытого ключа соответствующей карточки.

CardCertificate ::= Certificate

2.13 CardChipIdentification (идентификация микросхемы карточки)

Информация, записанная на карточке, которая относится к идентификации интегральной микросхемы карточки (ИС) (требование 249 приложения добавления 1С). icSerialNumber вместе с icManufacturingReferences однозначно идентифицирует микросхему карточки. Атрибут icSerialNumber сам по себе не является уникальным идентификатором микросхемы карточки.

```
CardChipIdentification ::=      ПОСЛЕДОВАТЕЛЬНОСТЬ {
icSerialNumber                  ОКТЕТНАЯ СТРОКА (РАЗМЕР4))
icManufacturingReferences       ОКТЕТНАЯ СТРОКА (РАЗМЕР4))
                                }
```

icSerialNumber — серийный номер ИС.

icManufacturingReferences — конкретный идентификатор изготовителя ИС.

2.14 CardConsecutiveIndex (порядковый индекс карточки)

Порядковый индекс карточки (определение h)).

CardConsecutiveIndex ::= строка IA5 (РАЗМЕР(1))

Присвоение значения: (см. приложение добавление 1С, глава 7)

Порядок увеличения: ‘0 , ..., 9, A, ..., Z, a, ..., z’

2.15 CardControlActivityDataRecord (запись данных на карточке о деятельности по контролю)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к последней проверке, которой подвергся водитель (приложение добавление 1С, требования 274, 299, 327 и 350).

```
CardControlActivityDataRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
controlType                Тип проверки
controlTime                Реальное время
controlCardNumber          Номер контрольной карточки
FullCardNumber,           Полный номер карточки
controlVehicleRegistration Идентификационный номер регистрации
                           транспортного средства,
controlDownloadPeriodBegin Реальное время
controlDownloadPeriodEnd   Реальное время }

```

controlType — тип проверки.

controlTime — дата и время проверки.

controlCardNumber — полный номер карточки контролера, проводившего проверку.

controlVehicleRegistration — регистрационный номер транспортного средства (VRN) и название государства-члена Договаривающейся стороны регистрации транспортного средства, в которой была произведена проверка.

controlDownloadPeriodBegin и **controlDownloadPeriodEnd** — период, за который загружаются данные, в случае загрузки.

2.16 CardCurrentUse (текущее использование карточки)

Информация о фактическом пользовании карточки (приложение добавление 1С, требования 273, 298, 326 и 349).

```
CardCurrentUse ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
sessionOpenTime    Реальное время
sessionOpenVehicle Идентификационный номер регистрации транспортного средства
}

```

sessionOpenTime — время, когда карточка была введена для текущего использования. При извлечении карточки данный элемент устанавливается на ноль.

sessionOpenVehicle — идентификация используемого в данный момент транспортного средства, установленная при вводе карточки. При извлечении карточки данный элемент устанавливается на ноль.

2.17 CardDriverActivity (запись на карточке о деятельности водителя)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к деятельности водителя (приложение добавление 1С, требования 267, 268, 292, 293, 321 и 344).

```

CardDriverActivity ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
activityPointerOldestDayRecord  ЦЕЛОЕ ЧИСЛО (0..CardActivityLengthRange-1)
activityPointerNewestRecord     ЦЕЛОЕ ЧИСЛО (0..CardActivityLengthRange-1)
activityDailyRecords           ОКТЕТНАЯ СТРОКА
                               (РАЗМЕР(CardActivityLengthRange))
}

```

activityPointerOldestDayRecord — спецификация начала места хранения (число байтов с начала строки) самой давней записи о полном дне в строке activityDailyRecords. Максимальное значение определяется в виде длины строки.

activityPointerNewestRecord — спецификация начала места хранения (число байтов с начала строки) самой новой дневной записи в строке activityDailyRecords. Максимальное значение определяется в виде длины строки.

activityDailyRecords — место для хранения данных о деятельности водителя (структура данных: CardActivityDailyRecord) за каждый календарный день, когда использовалась карточка.

Присвоение значения: данная октетная строка периодически заполняется записями типа CardActivityDailyRecord. При первом использовании хранение данных производится с начала первого байта строки. Все новые записи включаются в конце предыдущей. Когда вся строка заполняется, процесс хранения продолжается с первого байта строки, независимо от наличия разрыва в том или ином элементе данных. До включения в строку данных о новом виде деятельности (посредством расширения текущей позиции activityDailyRecord или включения новой позиции activityDailyRecord), которые записываются вместо прежних данных о деятельности, указатель activityPointerOldestDayRecord должен быть обновлен с целью отразить новое место хранения самой давней полной ежедневной записи, а указатель activityPreviousRecordLength этой (новой) самой давней полной дневной записи должен быть установлен на 0.

2.18 CardDrivingLicenceInformation (информация о водительском удостоверении на карточке)

Информация, записанная на карточке водителя, которая относится к данным о водительском удостоверении держателя карточки (~~приложение~~ **добавление 1С**, требования 259 и 284).

```

CardDrivingLicenceInformation ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
drivingLicenceIssuingAuthority  Название органа, выдавшего водительское
                               удостоверение
drivingLicenceIssuing          Выдача водительского удостоверения  Страна
                               Числовой код страны
drivingLicenceNumber           Номер водительского удостоверения  Октетная
                               строка IA5(РАЗМЕР(16))
}

```

drivingLicenceIssuingAuthority — орган, ответственный за выдачу водительского удостоверения.

drivingLicenceIssuingNation — национальная принадлежность органа, выдавшего водительское удостоверение.

drivingLicenceNumber — номер водительского удостоверения.

2.19 CardEventData (данные о событиях на карточке)

Поколение 1:

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к событиям, связанным с держателем карточки (~~приложение добавление~~ 1С, требования 260, ~~285, 318~~ и ~~341 318~~).

```
CardEventData ::= РАЗМЕР ПОСЛЕДОВАТЕЛЬНОСТИ (6) {
cardEventRecords          УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfEventsPerType)
                           ПАРАМЕТРА CardEventRecord
}
```

CardEventData — последовательность записей **cardEventRecords**, записанная в порядке возрастания значения элемента **EventFaultType** (за исключением записей, касающихся нарушения защиты, которые группируются в последнем массиве данных этой последовательности).

cardEventRecords — набор записей о событиях данного типа (или категория событий, имеющих отношение к попыткам нарушения защиты).

Поколение 2:

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к событиям, связанным с держателем карточки (добавление 1С, требования 285 и 341).

```
CardEventData ::= РАЗМЕР ПОСЛЕДОВАТЕЛЬНОСТИ (11) {
cardEventRecords          УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfEventsPerType)
                           CardEventRecord
}
```

CardEventData — последовательность записей **cardEventRecords**, записанная в порядке возрастания значения элемента **EventFaultType** (за исключением записей, касающихся нарушения защиты, которые группируются в последнем массиве данных).

cardEventRecords — набор записей о событиях данного типа (или категория событий, имеющих отношение к попыткам нарушения защиты).

2.20 CardEventRecord (запись о событиях на карточке)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к событию, связанному с держателем карточки (добавление 1С, требования 261, 286, 318 и 341).

```
CardEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
eventType                 Тип события — неисправность
eventBeginTime            Реальное время
eventEndTime              Реальное время
eventVehicleRegistration  Идентификация регистрации транспортного средства
}
```

eventType — тип события.

eventBeginTime — дата и время начала события.

eventEndTime — дата и время окончания события.

eventVehicleRegistration — VRN и государство-член Договаривающаяся сторона регистрации транспортного средства, в котором произошло данное событие.

2.21 CardFaultData (данные о сбоях в работе карточки)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к событию, связанному с владельцем карточки (~~приложение добавление~~ 1С, требования 261, 286, 318 и 341).

```
CardFaultData ::= РАЗМЕР ПОСЛЕДОВАТЕЛЬНОСТИ(2) {
cardFaultRecords          УСТАНОВЛЕННЫЙ РАЗМЕР(NoOfFaultsPerType)
                           ПАРАМЕТРА CardFaultRecord
}
```

CardFaultData — последовательность совокупности записей, отражающих неисправности ~~записывающего оборудования~~ **контрольного устройства**, за которой следует совокупность записей, отражающих сбой в работе карточек.

cardFaultRecords — совокупность записей о неисправностях, сгруппированных по данной категории неисправностей (~~записывающего оборудования~~ **контрольного устройства** или карточки).

2.22 CardFaultRecord (запись о сбоях в работе карточки)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к событию, связанному с держателем карточки (~~приложение добавление~~ 1С, требования 261, 286, 318 и 341).

```
CardFaultRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
faultType                  Тип события — неисправность
faultBegin                 Реальное время
faultEndTime               Реальное время
faultVehicleRegistration  Идентификация регистрации транспортного средства
}
```

faultType — тип неисправности.

faultBeginTime — дата и время начала неисправности.

faultEndTime — дата и время окончания неисправности.

faultVehicleRegistration — VRN и ~~государство-член~~ **Договаривающаяся сторона** регистрации транспортного средства, в котором произошла данная неисправность.

2.23 CardIccIdentification (идентификация карточки ИС)

Информация, записанная на карточке, которая относится к идентификации интегральной микросхемы карточки (ИС) (~~приложение добавление~~ 1С, требование 248).

```
CardIccIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
clockStop                  ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))
cardExtendedSerialNumber  Расширенный серийный номер
cardApprovalNumber        Номер официального утверждения карточки
cardPersonaliserID        Идентификатор персонализации карточки
EmbedderIcAssemblerId     Идентификатор монтажного/сборочного предприятия
iccIdentifier              ОКТЕТНАЯ СТРОКА (РАЗМЕР(2))
}
```


clockStop — режим остановки часов, определенный в подразделе 2.

cardExtendedSerialNumber — расширенный серийный номер карточки на микросхеме ИС, как указано далее для типа данных ExtendedSerialNumber.

cardApprovalNumber — номер официального утверждения карточки.

cardPersonaliserID — идентификационные данные персонализации карточки, закодированные в виде кода изготовителя.

embedderIcAssemblerId — информация о монтажном/сборочном предприятии ИС.

icIdentifier — идентификатор ИС на карточке и изготовителя ИС, как указано в стандарте ISO/IEC 7816-6.

2.24 CardIdentification (идентификация карточки)

Информация, записанная на карточке, которая имеет отношение к идентификационным данным карточки (~~приложение~~ **добавление** 1С, требования 255, 280, 310, 333, 359, 365, 371 и 377).

CardIccIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

cardIssuingMemberState Числовой код страны

cardNumber Номер карточки

cardIssuingAuthorityName Название,

cardIssueDate Реальное время

cardValidityBegin Реальное время

cardExpiryDate Реальное время

}

cardIssuingMemberState — код государства-члена, выдающего Договаривающейся стороны, выдавшей карточку

cardNumber — номер карточки.

cardIssuingAuthorityName — название органа, выдавшего карточку.

cardIssueDate — дата выдачи карточки нынешнему держателю.

cardValidityBegin — первая дата действия карточки.

cardExpiryDate — дата истечения срока действия карточки.

2.24a CardLoadTypeEntries (данные о типе груза на карточке)

Поколение 2, версия 2:

Информация, записанная на карточке водителя или мастерской, которая относится к данным о типе груза, выдаваемым бортовым устройством при вводе карточки в бортовое устройство (приложение 1С, требования 306j и 356j).

CardLoadTypeEntries ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

loadTypeEntryPointerNewestRecord ЦЕЛОЕ ЧИСЛО (0..NoOfLoadTypeEntryRecords-1)

cardLoadTypeEntryRecords УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfLoadTypeEntryRecords)
ПАРАМЕТРА CardLoadTypeEntryRecord

}

loadTypeEntryPointerNewestRecord — индекс последней обновленной записи о типе груза.

Присвоение значения: число, соответствующее счетчику записи о типе груза начиная с '0' для первого случая внесения записи о типе груза на карточке в структуре данных.

cardLoadTypeEntryRecords — набор записей, содержащих дату и время записи и внесенный тип груза.

2.24b CardLoadTypeEntryRecord (записи данных о типе груза на карточке)

Поколение 2, версия 2:

Информация, записанная на карточке водителя или мастерской, которая относится к изменениям внесенных данных о типе груза, выдаваемым бортовым устройством при вводе карточки в бортовое устройство (приложение 1С, требования 306i и 356i).

CardLoadType Record ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

timeStamp Реальное время

loadTypeEntered Тип груза

}

timeStamp — дата и время, когда были введены данные о типе груза.

loadTypeEntered — введенные данные о типе груза.

2.24c CardLoadUnloadOperations (операции по загрузке/разгрузке на карточке)

Поколение 2, версия 2:

Информация, записанная на карточке водителя или мастерской, которая относится к операциям по загрузке/разгрузке транспортного средства (Добавление 1С, требования 306h и 356h).

CardLoadUnloadOperations ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

loadUnloadPointerNewestRecord ЦЕЛОЕ ЧИСЛО (0..NoOfLoadUnloadRecords-1)

cardLoadUnloadRecords УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfLoadUnloadRecords)
ПАРАМЕТРА CardLoadUnloadRecord

}

loadUnloadPointerNewestRecord — последняя запись указателя на последнюю обновленную запись о загрузке/разгрузке.

Присвоение значения: число, соответствующее счетчику записи «загрузка/разгрузка» на карточке, начиная с '0' для первого случая внесения записи о разгрузке на карточке в структуре данных.

cardLoadUnloadRecords — набор записей, содержащих указание на тип выполненной операции (загрузка, разгрузка или одновременная загрузка и разгрузка), дату и время ввода операции загрузки/разгрузки, информацию о местоположении транспортного средства и показания счетчика пробега транспортного средства.

2.24d CardLoadUnloadRecord (запись об операциях загрузки/разгрузки на карточке)

Поколение 2, вариант 2:

Информация, записанная на карточке водителя или мастерской, которая относится к операциям по загрузке/разгрузке транспортного средства (добавление 1С, требования 306g и 356g).

CardLoadUnloadRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

timeStamp	Реальное время,
operationType	Тип операции
gnssPlaceAuthRecord	Запись аутентифицированного места по ГНСС
vehicleOdometerValue	Показания счетчика пробега

}

timestamp — дата и время начала операции по загрузке, разгрузке и одновременной загрузке/разгрузке.

operationType — тип введенных данных по проведенной операции (загрузка, разгрузка или одновременная загрузка/разгрузка).

gnssPlaceRecord содержит информацию, связанную с местоположением транспортного средства.

vehicleOdometerValue — показания счетчика пробега, относящиеся к началу операции загрузки/разгрузки.

2.25 CardMACertificate (сертификат карточки МА)

Поколение 2:

Сертификат открытого ключа карточки для взаимной аутентификации с БУ. Структура данного сертификата представлена в ~~приложении~~ подразделе 11.

CardMACertificate ::= сертификат

2.26 CardNumber (номер карточки)

Номер карточки в соответствии с определением g.

CardNumber ::= ВЫБОР {

ПОСЛЕДОВАТЕЛЬНОСТЬ {

driverIdentification	СтрокаIA5(РАЗМЕР(14))
cardReplacementIndex	Индекс замены карточки
cardRenewalIndex	Индекс возобновления карточки

}

ПОСЛЕДОВАТЕЛЬНОСТЬ {

ownerIdentification	СтрокаIA5(РАЗМЕР(13))
cardConsecutiveIndex	Порядковый индекс карточки
cardReplacementIndex	Индекс замены карточки
cardRenewalIndex	Индекс возобновления карточки

}

}

driverIdentification — уникальная идентификация водителя в государстве-члене Договаривающейся стороне.

ownerIdentification — уникальная идентификация владельца в государстве-члене Договаривающейся стороне.

cardConsecutiveIndex — порядковый индекс карточки.

cardReplacementIndex — индекс замены карточки.

cardRenewalIndex — индекс возобновления карточки.

Первая последовательность выбора подходит для кодирования номера карточки водителя, вторая последовательность выбора подходит для кодирования номеров карточки мастерской, карточки контролера и карточки предприятия.

2.26a CardPlaceAuthDailyWorkPeriod (разрешенный ежедневный период работы и место, указанные на карточке)

Поколение 2, вариант 2:

Информация, записанная на карточке водителя или мастерской, которая относится к аутентификации статуса мест, в которых начинаются и/или заканчиваются ежедневные периоды работы (добавление 1С, требования 306b и 356b).

CardPlaceAuthDailyWorkPeriod ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

placeAuthPointerNewestRecord ЦЕЛОЕ ЧИСЛО (0 .. NoOfCardPlaceRecords-1)

placeAuthStatusRecords УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfCardPlaceRecords)
ПАРАМЕТРА PlaceAuthStatusRecord

}

placeAuthPointerNewestRecord — индекс последней обновленной записи аутентификации данных о месте.

Присвоение значения: число, соответствующее счетчику записей о статусе аутентификации места, которое начинается с '0' в случае первой регистрации записей о статусе аутентификации места в структуре данных.

placeAuthStatusRecords — набор записей, содержащих данные о статусе аутентификации места въезда.

2.27 CardPlaceDailyWorkPeriod (ежедневный период работы и место, указанные на карточке)

Информация, записанная на карточке водителя или мастерской, которая относится к местам, в которых начинаются и/или заканчиваются ежедневные периоды работы (приложение добавление 1С, требования 272, 297, 325 и 348).

CardPlaceDailyWorkPeriod ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

placePointerNewestRecord ЦЕЛОЕ ЧИСЛО(0 .. NoOfCardPlaceRecords-1),
УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfCardPlaceRecords)
ПАРАМЕТРА PlaceRecord

}

placePointerNewestRecord — индекс последней обновленной записи данных о названии мест.

Присвоение значения: число, соответствующее счетчику записи о статусе места, которое начинается с '0' в случае первой регистрации записей, касающихся статуса данного места, в структуре данных.

placeRecords — совокупность записей, содержащих информацию о введенных названиях мест.

2.28 CardPrivateKey (закрытый ключ карточки)

Поколение 1:

Закрытый ключ карточки.

CardPrivateKey ::= RSAKeyPrivateExponent

2.29 CardPublicKey (открытый ключ карточки)

Открытый ключ карточки.

CardPublicKey ::= PublicKey

2.30 CardRenewalIndex (индекс возобновления карточки)

Индекс возобновления карточки (определение i).

CardRenewalIndex ::= СтрокаIA5(РАЗМЕР(1))

Присвоение значения: (см. настоящее приложение добавление, глава VII 7).

‘0’ Первый выпуск.

Порядок возрастания: ‘0 , ... , 9 , A , ... , Z’

2.31 CardReplacementIndex (индекс замены карточки)

Индекс возобновления карточки (определение j)).

CardReplacementIndex ::= СтрокаIA5(РАЗМЕР(1))

Присвоение значения: (см. настоящее приложение добавление, глава VII).

‘0’ Первоначальная карточка.

Порядок возрастания: ‘0 , ... , 9 , A , ... , Z’

2.32 CardSignCertificate (сертификат подписи карточки)

Поколение 2:

Сертификат открытого ключа карточки для подписания. Структура данного сертификата представлена в приложении подразделе 11.

CardSignCertificate ::= Certificate

2.33 CardSlotNumber (номер считывающего устройства карточки)

Код, позволяющий проводить различие между двумя считывающими устройствами бортового устройства.

CardSlotNumber ::= ЦЕЛОЕ ЧИСЛО {

driverSlot (считывающее устройство водителя) (0),

co-driverSlot (считывающее устройство второго водителя) (1)

}

Присвоение значения: дополнительно не указывается.

2.34 CardSlotsStatus (статус считывающих устройств карточки)

Код, указывающий тип карточек, введенных в два считывающих устройства бортового устройства.

CardSlotsStatus ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))

Присвоение значения — выровненный октет: 'ccccddd'B

'cccc'B Идентификационные данные типа карточки, вставленной в считывающее устройство второго водителя,

'ddd'B Идентификационные данные типа карточки, вставленной в считывающее устройство водителя,

со следующими идентификационными кодами:

'0000'B карточка не вставлена,

'0001'B вставлена карточка водителя,

'0010'B вставлена карточка мастерской,

'0011'B вставлена карточка контролера,

'0100'B вставлена карточка предприятия.

2.35 CardSlotsStatusRecordArray (статус считывающих устройств карточки и метаданные)

Поколение 2:

CardSlotsStatus плюс метаданные, используемые в протоколе загрузки.

CardSlotsStatusRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType	Тип записи
recordSize	ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords	ЦЕЛОЕ ЧИСЛО(0..65535)
records	УСТАНОВЛЕННЫЙ РАЗМЕР(noOfRecords) ПАРАМЕТРА CardSlotsStatus

}

recordType указывает на тип записи (CardSlotsStatus).

Присвоение значения: см. RecordType

recordSize — размер CardSlotsStatus в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей CardSlotsStatus.

2.36 CardStructureVersion (версия структуры карточки)

Код, указывающий на версию реализованной структуры на карточке тахографа.

CardStructureVersion ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(2))

Присвоение значения: 'aabb'N:

'aa'N индекс изменений структуры.

'00'N для приложений поколения 1

'01'N для приложений поколения 2

'bb'Н индекс изменений применительно к использованию элементов данных, определенных в структуре, заданной стартовым байтом.

'00'Н для ~~настоящей версии~~ приложений поколения 1

'00'Н для ~~настоящей~~ версии 1 приложений поколения 2

'01'Н для версии 2 приложений поколения 2

2.37 CardVehicleRecord (запись использования транспортного средства на карточке)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к периоду использования транспортного средства в течение календарного дня (~~приложение~~ **добавление 1С**, требования 269, 294, 322 и 345).

Поколение 1:

```
CardEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
vehicleOdometerBegin    Показания счетчика пробега
vehicleOdometerEnd      Показания счетчика пробега
vehicleFirstUse         Реальное время
vehicleLastUse          Реальное время
vehicleRegistration     Идентификация регистрации транспортного средства
vuDataBlockCounter     счетчик нумерации циклов ввода и извлечения карточек в БУ
}
```

vehicleOdometerBegin — показания счетчика пробега транспортного средства на начало периода эксплуатации транспортного средства.

vehicleOdometerEnd — показания счетчика пробега транспортного средства на конец периода эксплуатации транспортного средства.

vehicleFirstUse — дата и время начала периода эксплуатации транспортного средства.

vehicleLastUse — дата и время окончания периода эксплуатации транспортного средства.

VehicleRegistration — VRN и ~~государство-член~~ **Договаривающаяся сторона** регистрации транспортного средства, на котором произошел данный сбой.

vuDataBlockCounter — показания VuDataBlockCounter на момент последнего извлечения информации за данный период эксплуатации транспортного средства.

Поколение 2:

```
CardEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
vehicleOdometerBegin    Показания счетчика пробега
vehicleOdometerEnd      Показания счетчика пробега
vehicleFirstUse         Реальное время
vehicleLastUse          Реальное время
vehicleRegistration     Идентификация регистрации транспортного средства
vuDataBlockCounter     Счетчик нумерации циклов ввода и извлечения карточек в БУ
vehicleIdentificationNumber  Идентификационный номер транспортного средства
}
```

В дополнение к первому поколению используется следующий элемент данных:

VehicleIdentificationNumber — идентификационный номер транспортного средства, относящийся ко всему транспортному средству.

2.38 CardVehiclesUsed (использованное транспортное средство)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к событию, связанному с держателем карточки (~~приложение добавление~~ 1С, требования 270, 295, 323 и 346).

```
CardVehiclesUsed ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
vehiclePointerNewestRecord  ЦЕЛОЕ ЧИСЛО (0..NoOfLoadTypeEntryRecords -1)
                               УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfCardPlaceRecords)
                               ПАРАМЕТРА cardVehicleRecords
}
```

vehiclePointerNewestRecord — последняя запись указателя на последнюю обновленную запись.

Присвоение значения: число, соответствующее показанию счетчика записи, касающейся транспортного средства, начиная с '0' для первого случая внесения записи, касающейся транспортного средства, в структуру данных.

cardVehicleRecords — совокупность записей, содержащих информацию об использованных транспортных средствах.

2.39 CardVehicleUnitRecord (запись использованных единиц транспортных средств)

Поколение 2:

~~Поколение 2:~~

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к соответствующему использованному транспортному средству (~~приложение добавление~~ 1С, требования 303 и 351).

```
CardVehicleUnitRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
timeStamp                    Реальное время
ManufacturerCode             Код изготовителя
deviceID                     ЦЕЛОЕ ЧИСЛО(0..255)
VuSoftwareVersion           Версия программного обеспечения БУ
}
```

timeStamp — начало периода использования бортового устройства (т. е. первый ввод карточки в бортовое устройство в течение рассматриваемого периода).

manufacturerCode идентифицирует изготовителя бортового устройства.

deviceID идентифицирует тип бортового устройства изготовителя. Принятое значение устанавливается по усмотрению изготовителя.

vuSoftwareVersion — номер версии программного обеспечения бортового устройства.

2.40 CardVehicleUnitsUsed (использованные единицы транспортных средств)

Поколение 2:

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к событию, связанному с держателем карточки (**приложение добавление 1С**, требования 3046 и 352).

```
CardVehicleUnitsUsed ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
vehicleUnitPointerNewestRecord ЦЕЛОЕ ЧИСЛО (0..NoOfLoadTypeEntryRecords-1)
cardVehicleUnitRecords УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfCardPlaceRecords)
ПАРАМЕТРА CardVehicleUnitRecords.
}
```

vehicleUnitPointerNewestRecord — указатель на последнюю обновленную запись по данной единице транспортного средства.

Присвоение значения: число, соответствующее показанию счетчика записей о единице транспортного средства, начиная с '0' для первого случая внесения записи о единице транспортного средства на карточке в структуре данных

cardVehicleRecords — совокупность записей, содержащих информацию об использованных единицах транспортных средств.

2.41 Certificate (сертификат)

Сертификат открытого ключа, выданный сертификационным органом.

Поколение 1:

Certificate ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(194))

Присвоение значения: цифровая подпись с частичным восстановлением содержания сертификата в соответствии с общими механизмами защиты, описанными в **приложении подразделе 11: Подпись (128 байтов) ||** Остальная часть открытого ключа (58 байтов) **||** Код сертификационного органа (8 байтов).

Поколение 2:

Сертификат ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(204..341))

Присвоение значения: См. **приложение подраздел 11** добавления.

2.42 CertificateContent (содержание сертификата)

Поколение 1:

(Четкое) содержание сертификата открытого ключа в соответствии с общими механизмами защиты, изложенными в **приложении подразделе 11**.

```
CertificateContent ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
certificateProfileIdentifier ЦЕЛОЕ ЧИСЛО(0..255)
certificationAuthorityReference Идентификатор ключа
certificateHolderAuthorisation Идентификатор прав держателя сертификата
certificateEndOfValidity Реальное время
certificateHolderReference Ссылка на держателя сертификата
publicKey Открытый ключ
}
```

certificateProfileIdentifier — версия соответствующего сертификата.

Присвоение значения: ‘01h’ для данной версии.

certificationAuthorityReference — идентификатор сертификационного органа, выдавшего сертификат. Он также включает в себя ссылку на открытый ключ данного сертификационного органа.

certificateHolderAuthorisation — идентификатор прав держателя сертификата.

certificateEndOfValidity — дата, когда истекает срок административного действия сертификата.

certificateHolderReference — ссылка на держателя сертификата. Он также включает в себя ссылку на его открытый ключ.

publicKey — открытый ключ, подтверждающий данный сертификат.

2.43 CertificateHolderAuthorisation (идентификатор прав держателя сертификата)

Идентификатор прав держателя сертификата.

```
certificateHolderAuthorisation ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
tachographApplicationID    ОКТЕТНАЯ СТРОКА (РАЗМЕР(6))
equipmentType              Тип оборудования
}
```

Поколение 1:

tachographApplicationID — идентификатор приложения для прикладной программы тахографа.

Присвоение значения: ‘FFh’ ‘54h’ ‘41h’ ‘43h’ ‘48h’ ‘4Fh’. Этот AID является фирменным незарегистрированным идентификатором приложения в соответствии со стандартом ISO/IEC 7816-5.

equipmentType — идентификатор типа оборудования, на который выдан данный сертификат.

Присвоение значения: в соответствии с типом данных EquipmentType. **0** — если это сертификат ~~какого-либо государства-члена~~ **какой-либо Договаривающейся стороны.**

Поколение 2:

tachographApplicationID обозначает 6 наиболее значимых байтов идентификатора (AID) приложения карточки тахографа второго поколения. AID приложения карточки тахографа указан в главе 6.2.

Присвоение значения: ‘FF 53 4D 52 44 54’.

equipmentType — идентификатор типа оборудования второго поколения, для которого предназначен этот сертификат.

Присвоение значения: в соответствии с типом данных EquipmentType.

2.44 CertificateRequestID (идентификатор запроса на сертификат)

Уникальный идентификатор запроса на получение сертификата. Он может также использоваться в качестве идентификатора открытого ключа бортового устройства, если серийный номер бортового устройства, для которого предназначен данный ключ, в момент создания сертификата неизвестен.

CertificateRequestID ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
~~requestSerialNumber~~**requestSerialNumber** ЦЕЛОЕ ЧИСЛО(0..2³²-1)
 requestMonthYearСтрока ВCD(РАЗМЕР(2))
 crIdentifier ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))
 ManufacturerCode код изготовителя
 }

requestSerialNumber — серийный номер запроса на сертификат, уникальный для данного изготовителя и относящийся к месяцу, указанному ниже.

requestMonthYear — идентификация месяца и года запроса на сертификат.

Присвоение значения: код ВCD месяца (две цифры) и года (две последние цифры).

crIdentifier — идентификатор, позволяющий проводить различие между запросом на сертификат и расширенным серийным номером.

Присвоение значения: 'FFh'.

manufacturerCode — цифровой код изготовителя, подающего заявку на сертификат.

2.45 CertificationAuthorityKID (сертификационный орган KID)

Идентификатор открытого ключа сертификационного центра (~~государства-члена Договаривающейся стороны~~ или Европейского корневого сертификационного центра).

CertificationAuthorityKID ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
 nationNumeric Числовой код страны
 nationAlpha Буквенный код страны
 keySerialNumber ЦЕЛОЕ ЧИСЛО(0..255)
 additionalInfo ОКТЕТНАЯ СТРОКА (РАЗМЕР(2))
 caIdentifier ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))
 }

nationNumeric — цифровой код страны сертификационного органа.

nationAlpha — буквенно-цифровой код страны сертификационного органа.

keySerialNumber — серийный номер, позволяющий проводить различие между различными ключами сертификационного органа в случае изменения ключей.

additionalInfo — двухбайтовое поле для дополнительного кодирования (по усмотрению сертификационного органа).

caIdentifier — идентификатор, позволяющий проводить различие между идентификатором ключа сертификационного органа и другими идентификаторами ключа.

Присвоение значения: '01h'.

2.46 CompanyActivityData (данные об операциях с карточкой предприятия)

Информация, записанная на карточке предприятия, которая относится к действиям, проводимым с карточкой (~~приложение~~ **добавление** 1С, требования 373 и 379).

```

CompanyActivityData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
companyPointerNewestRecord ЦЕЛОЕ ЧИСЛО (0..NoOfCompanyActivityRecords-1)
companyActivityRecords УСТАНОВЛЕНИЕ РАЗМЕРА (NoOfLoadTypeEntryRecords)
ПАРАМЕТРА
companyActivityRecord ПОСЛЕДОВАТЕЛЬНОСТЬ {
companyActivityType тип операции, произведенной предприятием
companyActivityTime Реальное время
cardNumberInformation Полный номер карточки
vehicle RegistrationInformation Идентификация регистрации транспортного средства
downloadPeriodBegin Реальное время
downloadPeriodEnd Реальное время
}
}

```

companyPointerNewestRecord — указатель на последнюю обновленную запись о деятельности предприятия.

Присвоение значения: — число, соответствующее числовому показателю записи данных о деятельности предприятия, которое начинается с '0' в случае первой регистрации записей, касающихся деятельности предприятия, в структуре данных.

companyActivityRecords — совокупность всех записей действий, произведенных предприятием.

companyActivityRecord — последовательность информации, относящейся к одному действию, произведенному предприятием.

companyActivityType — тип деятельности предприятия.

companyActivityTime — дата и время данной деятельности предприятия.

cardNumberInformation — номер карточки и название государства-члена, выдавшего Договаривающейся стороне, выдавшей карточку с загруженными с нее данными, если применимо.

vehicleRegistrationInformation — VRN и государство-член Договаривающейся стороны регистрации транспортного средства, данные которого загружены, заблокированы или разблокированы.

downloadPeriodBegin и **downloadPeriodEnd** — период, за который в соответствующих случаях загружены данные с БУ.

2.47 CompanyActivityType (тип операции, произведенной предприятием)

Код, указывающий на действия, произведенные предприятием с использованием карточки предприятия.

```

CompanyActivityType ::= ЦЕЛОЕ ЧИСЛО {
загрузка данных с карточки 1)
загрузка данных с БУ 2)
блокировка БУ 3)
разблокировка БУ 4)
}

```

2.48 CompanyCardApplicationIdentification (идентификация приложения карточки предприятия)

Информация, записанная на карточке предприятия, которая относится к идентификации приложения карточки (~~приложение~~ **добавление 1С**, требования 369 и 375).

```
CompanyCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
  typeOfTachographCardId      Тип оборудования
  cardStructureVersion         Версия структуры карточки
  noOfCompanyActivityRecords   Число записей, касающихся операций предприятия
}
```

typeOfTachographCardId уточняет введенный в действие тип карточки.

cardStctureVersion уточняет версию структуры, реализованной на карточке.

noOfCompanyActivityRecords — число записей о действиях предприятия, которые могут храниться на карточке.

2.48a CompanyCardApplicationIdentificationV2 (идентификация приложения карточки предприятияV2)

Поколение 2, версия 2:

Информация, записанная на карточке предприятия, которая относится к идентификации приложения карточки (**добавление 1С**, требование 375a).

```
CompanyCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
  lengthOfFollowingData        Длина последующих данных
  vuConfigurationLengthRange   Длина данных о конфигурации БУ
}
```

lengthOfFollowingData — число байтов, следующих в данной записи.

vuConfigurationLengthRange — число байтов на карточке тахографа, выделенных на хранение конфигураций БУ.

2.49 CompanyCardHolderIdentification (идентификация держателя карточки предприятия)

Информация, записанная на карточке предприятия, которая относится к идентификации держателя карточки (~~приложение~~ **добавление 1С**, требования 372 и 378).

```
CompanyCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
  companyName                  Название
  companyAddress               Адрес
  cardHolderPreferredLanguage  Предпочитаемый язык держателя карточки
}
```

companyName — название предприятия держателя.

companyAddress — адрес предприятия держателя.

cardHolderPreferredLanguage — предпочитаемый язык держателя карточки.

2.50 ControlCardApplicationIdentification (идентификация приложения карточки контролера)

Информация, записанная на карточке контролера, которая относится к идентификации приложения карточки (~~приложение~~ добавление 1С, требования 357 и 363).

```
ControlCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
  typeOfTachographCardId      Тип оборудования
  cardStructureVersion         Версия структуры карточки
  noOfControlActivityRecords   Число записей, касающихся операций по контролю
}
```

typeOfTachographCardId уточняет введенный в действие тип карточки.

cardStctureVersion уточняет версию структуры, реализованной на карточке.

noOfControlActivityRecords — число записей, касающихся операций по контролю, которое может храниться на карточке

2.50a ControlCardApplicationIdentificationV2 (идентификация приложения карточки контролераV2)

Поколение 2, версия 2:

Информация, записанная на карточке контролера, которая относится к идентификации приложения карточки (добавление 1С, требование 363а).

```
ControlCardApplicationIdentificationV2 ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
  lengthOfFollowingData      длина следующих данных.
  vuConfigurationLengthRange длина данных о конфигурации БУ.
}
```

lengthOfFollowingData — число байтов, следующих в записи.

vuConfigurationLengthRange — число байтов в карточке тахографа, предусмотренных для хранения данных о конфигурации БУ.

2.51 ControlCardControlActivityData (данные о проверочных операциях на карточке контролера)

Информация, записанная на карточке контролера, которая относится к действиям, производимым с карточкой (~~приложение~~ добавление 1С, требования 361 и 367).

```
ControlCardControlActivityData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
  controlPointerNewestRecord ЦЕЛОЕ ЧИСЛО (0.. NoOfControlActivityRecords-1)
  controlActivityRecords     УСТАНОВЛЕНИЕ РАЗМЕРА (NoOfLoadTypeEntryRecords)
  controlActivityRecord      ПОСЛЕДОВАТЕЛЬНОСТИ {
  controlType                Тип контроля
  controlTime                Реальное время
  controlledCardNumber       Полный номер карточки,
  controlledVehicleRegistration Идентификация регистрации транспортного средства
```

```

controlDownloadPeriodBegin    Реальное время
controlDownloadPeriodEnd      Реальное время
                                }
}

```

controlPointerNewestRecord — последняя запись указателя на последнюю обновленную запись по контролю.

Присвоение значения: число, соответствующее числовому показателю записи данных о деятельности по контролю, которое начинается с '0' в случае первой регистрации записи по контролю в структуре данных.

controlActivityRecords — совокупность всех записей деятельности по контролю.

controlActivityRecord — последовательность информации, относящейся к одному действию по контролю.

controlType — тип контроля.

controlTime — дата и время события, связанного с контролем.

controlledCardNumber — номер карточки и название государства-члена, выдавшего Договаривающейся стороне, выдавшей карточку, подверженной контролю.

controlledVehicleRegistration — VRN и государство-член Договаривающаяся сторона регистрации транспортного средства, в котором был произведен контроль.

controlDownloadPeriodBegin и **controlDownloadPeriodEnd** — период, за который в случае необходимости загружаются данные.

2.52 ControlCardHolderIdentification (идентификация держателя карточки контролера)

Информация, записанная на карточке контролера, которая относится к идентификации держателя карточки (~~приложение~~ **добавление 1С**, требования 360 и 366).

```

ControlCardHolderIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
controlBodyName                Название
controlBodyAddress              Адрес
cardHolderName                  Фамилия держателя
cardHolderPreferredLanguage     Язык
}

```

controlBodyName — название контрольного органа держателя карточки.

controlBodyAddress — адрес контрольного органа держателя карточки.

cardHolderName — фамилия и имя (имена) держателя карточки.

cardHolderPreferredLanguage — предпочитаемый язык держателя карточки.

2.53 ControlType (тип контроля)

Код, указывающий на действия, проведенные в ходе контроля. Этот тип данных связан с требованиями 126, 274, 299, 327 и 350 в ~~приложении~~ **добавлении 1С**.

```
ControlType ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))
```

Поколение 1:

Присвоение значения — выравнивание по октетам: 'c'V (8 битов)

- 'c'V загрузка карточки:
- '0'V: во время данной контрольной операции загрузка данных с карточки не производилась,
 - '1'V: во время данной контрольной операции загрузка данных с карточки производилась,
- 'v'V Загрузка данных с БУ
- '0'V: во время данной контрольной операции загрузка данных с БУ не производилась,
 - '1'V: во время данной контрольной операции загрузка данных с карточки производилась,
- 'p'V вывод на печать:
- '0'V: во время данной контрольной операции данные с карточки на печать не выводились,
 - '1'V: во время данной контрольной операции данные с карточки на печать выводились,
- 'd'V вывод на дисплей:
- '0'V: во время данной контрольной операции вывод данных на дисплей не производился,
 - '1'V: во время данной контрольной операции вывод данных на дисплей производился,
- 'xxxx'V Не используется.

Поколение 2:

Присвоение значения — выравнивание по октетам: 'c'p'dexxx'V (8 бит)

- 'c'V загрузка данных с карточки:
- '0'V: во время данной контрольной операции загрузка данных с карточки не производилась,
 - '1'V: во время данной контрольной операции загрузка данных с карточки производилась,
- 'v'V Загрузка данных с БУ:
- '0'V: во время данной контрольной операции загрузка данных с БУ не производилась,
 - '1'V: во время данной контрольной операции загрузка данных с БУ производилась,
- 'p'V вывод на печать:
- '0'V: во время данной контрольной операции вывод данных на печать не производился,
 - '1'V: во время данной контрольной операции вывод данных на печать производился,
- 'd'V вывод на дисплей:
- '0'V: во время данной контрольной операции вывод данных на дисплей не производился,
 - '1'V: во время данной контрольной операции вывод данных производился,

- ‘e’В Проверка калибровки на дорогах:
- ‘0’В: во время данной контрольной операции параметры калибровки не проверялись,
 - ‘1’В: во время данной контрольной операции параметры калибровки проверялись,
- ‘xxx’В ~~RFU~~ **Зарезервировано для использования в будущем.**

2.54 CurrentDateTime (текущая дата/время)

Текущие показатели даты и времени ~~записывающего оборудования~~ **контрольного устройства.**

CurrentDateTime ::= Реальное время

Присвоение значения: дополнительно не указывается.

2.55 CurrentDateTimeRecordArray (данные о текущей дате/времени и метаданные)

Поколение 2:

Текущие показатели даты и времени и метаданные, используемые в протоколе загрузки.

CurrentDateTimeRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType	Тип записи
recordSize	ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords	ЦЕЛОЕ ЧИСЛО(0..65535)
records	УСТАНОВЛЕННЫЙ РАЗМЕР(noOfRecords) ПАРАМЕТРА текущих показаний даты и времени

}

recordType указывает на тип записи (CurrentDateTime).

Присвоение значения: см. RecordType.

recordSize — размер CurrentDateTime в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей текущих показателей даты и времени.

2.56 DailyPresenceCounter (счетчик ежедневного присутствия)

Показания счетчика, записанные на карточке водителя или предприятия, которые увеличиваются на единицу за каждый календарный день, в течение которого в БУ вводилась данная карточка. Этот тип данных связан с требованиями 266, 299, 320 и 343 в ~~приложении~~ **добавлении 1С.**

DailyPresenceCounter ::= СтрокаBCD(РАЗМЕР(2))

Присвоение значения: порядковый номер с максимальным значением = 9999, который снова начинается с 0. В момент первой выдачи номера карточки это число устанавливается на 0.

2.57 Datef (формат даты)

Дата, выраженная в числовом формате, которая может сразу выводиться на печать.

```
Datef ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
год                СтрокаBCD(РАЗМЕР(2))
месяц             СтрокаBCD(РАЗМЕР(1))
день              СтрокаBCD(РАЗМЕР(1))
}
```

Присвоение значения:

уууу	год
мм	месяц
дд	день

‘00000000’Н явно выражает отсутствие даты.

2.58 DateOfDayDownloaded (дата и время загрузки)

Поколение 2:

Дата и время загрузки.

DateOfDayDownloaded ::= Реальное время

Присвоение значения: дополнительно не указывается.

2.59 DateOfDayDownloadedRecordArray (данные о дне и времени загрузки и метаданные)

Поколение 2:

Текущие показатели даты и времени и метаданные, используемые в протоколе загрузки.

```
DateOfDayDownloadedRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType        Тип записи
recordSize        ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords       ЦЕЛОЕ ЧИСЛО(0..65535)
records           УСТАНОВЛЕНИЕ РАЗМЕРА (noOfRecords)
                  ПАРАМЕТРА даты и времени загрузки
}
```

recordType указывает на тип записи (CurrentDateTime).

Присвоение значения: см. RecordType.

recordSize — размер CurrentDateTime в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей даты и времени загрузки.

2.60 Distance (расстояние)

Пройденное расстояние (результат расчета разницы между двумя показаниями счетчика пробега транспортного средства в километрах).

Расстояние ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: Двоичное значение без знака. Значение в км в рабочем диапазоне от 0 до 9 999 км.

2.60a DownloadInterfaceVersion (версия загрузочного интерфейса)

Поколение 2, версия 2:

Код, указывающий на версию интерфейса загрузки бортового устройства.

DownloadInterfaceVersion ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(2))

Присвоение значения: 'aabb'Н:

'aa'Н '00'Н: не используется,

'01'Н: Бортовое устройство поколения 2,

'bb'Н '00'Н: не используется,

'01'Н: Бортовое устройство версии 2 поколения 2.

2.61 DriverCardApplicationIdentification (идентификация приложения карточки водителя)

Информация, записанная на карточке водителя, которая относится к идентификации приложения карточки (~~приложение~~ добавление 1С, требования 253 и 278).

Поколение 1:

DriverCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

typeOfTachographCardId	Тип оборудования
cardStructureVersion	Версия структуры карточки
noOfEventsPerType	Число событий по типу
noOfFaultsPerType	Число неисправностей по типу
activityStctureLength	Длина записи о деятельности на карточке
noOfCardVehicleRecords	Число записей на карточке, касающихся транспортных средств
noOfCardPlaceRecords,	Число записей на карточке, касающихся мест)
}	

typeOfTachographCardId уточняет введенный в действие тип карточки.

cardStctureVersion уточняет версию структуры, реализованную на карточке.

noOfEventsPerType — число событий по типу события, которое может быть записано на карточку.

noOfFaultsPerType — число неисправностей каждого типа, которое может быть записано на карточку.

activityStctureLength — число байтов, которые могут быть использованы для хранения записей, относящихся к виду деятельности.

noOfCardVehicleRecords — число записей, касающихся транспортных средств, на карточке.

noOfCardPlaceRecords — число записей на карточке, касающихся мест.

Поколение 2:

DriverCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

typeOfTachographCardId	Тип оборудования
cardStructureVersion	Версия структуры карточки
noOfEventsPerType	Число событий по типу
noOfFaultsPerType	Число неисправностей по типу
activityStctureLength	Длина записи о деятельности на карточке
noOfCardVehicleRecords	Число записей, касающихся транспортных средств, на карточке
noOfCardPlaceRecords,	Число записей на карточке, касающихся мест
noOfGNSSCDRecords	Число записей ГНСС, касающихся НепБУ
noOfGNSSADRecords	Число записей ГНСС, касающихся НакБУ
noOfSpecificConditionRecords	Число записей, касающихся особых условий
noOfCardVehicleUnitRecords	Число записей, касающихся единиц транспортных средств на карточке

}

В дополнение к первому поколению используется следующий элемент данных:

~~noOfGNSSCDRecords~~ noOfGNSSCDRecords — число записей о ~~непрерывном~~ **накопленном** времени управления по ГНСС, которые могут храниться на карточке.

noOfSpecificConditionRecords — число записей об особых условиях, которое может храниться на карточке

noOfCardVehicleUnitRecords — **число записей, касающихся единиц транспортных средств, которые могут храниться на карточке.**

2.61a DriverCardApplicationIdentificationV2 (идентификация приложения карточки водителяV2)

Поколение 2, версия 2:

Информация, записанная на карточке водителя, которая относится к идентификации приложения карточки (добавление 1С, требование 278a).

DriverCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

lengthOfFollowingData	Длина следующих данных
noOfBorderCrossingRecords	Число записей о пересечении границы
noOfLoadUnloadRecords	Число записей о загрузке/разгрузке
noOfLoadTypeEntryRecords	Число записей о типе поступившего груза
	vuConfigurationLengthRange Длина данных о конфигурации БУ

}

lengthOfFollowingData — число следующих байтов в записи.

noOfBorderCrossingRecords — число записей о пересечении границы, которые могут храниться на карточке водителя.

noOfLoadUnloadRecords — число записей о загрузке/разгрузке, которые могут храниться на карточке водителя.

noOfLoadTypeEntryRecords — число записей о типе поступившего груза, которые могут храниться на карточке водителя.

vuConfigurationLengthRange — число байтов на карточке тахографа, доступных для хранения конфигураций БУ.

2.62 DriverCardHolderIdentification (идентификация держателя карточки водителя)

Информация, записанная на карточке водителя, которая относится к идентификации держателя карточки (~~приложение добавление 1С~~, требования 256 и 281).

DriverCardHolderIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

cardHolderName — Фамилия держателя карточки

cardHolderBirthDate — Формат даты

cardHolderPreferredLanguage — Язык

}

cardHolderName — фамилия и имя (имена) держателя карточки водителя.

cardHolderBirthDate — дата рождения держателя карточки водителя.

cardHolderPreferredLanguage — предпочитаемый язык владельца карточки.

2.63 DSRCSecurityData (система защиты данных DSRCs)

Поколение 2:

Определение этого типа данных см. подраздел добавления 11.

o — DSRCSecurityData

Поколение 2:

Простая текстовая информация и MAC, передаваемые через DSRC из тахографа в устройство дистанционного опроса (RI); более подробно см. приложение 11, часть B, глава 13 63. ~~Зарезервировано для использования в будущем~~

DSRCSecurityData ::= SEQUENCE {

tagLengthPlainText — ОКТЕТНАЯ СТРОКА (РАЗМЕР(2))

currentDateTime — CurrentDateTime

counter — ЦЕЛОЕ ЧИСЛО(0-224..1)

vuSerialNumber — vuSerialNumber

dSRCKMVersionNumber — INTEGER(SIZE(1))

tagLengthMac — ОКТЕТНАЯ СТРОКА (РАЗМЕР(2))

MAC — МАК

}

tagLength — часть кодирования DER-TLV, которая устанавливается как '81-10' (см. приложение 11, часть B, глава 13).

currentDateTime — текущие дата и время бортового устройства.

counter перечисляет сообщения RTM.

vuSerialNumber — серийный номер бортового устройства.

dSRCKMVersionNumber — номер версии главного ключа DSRC, из которого получены ключи DSRC, конкретно связанные с БУ.

~~tagLengthMac~~ — маркировка и длина объекта данных MAC как части кодирования DER TLV. Маркировка устанавливается как '8E', длина кодирует октетную длину MAC (см. приложение 11, часть В, глава 13).

~~mac~~ — это значение MAC, вычисленное при помощи сообщения RTM (см. приложение 11, часть В, глава 13).

2.64 EGFCertificate (сертификат EGF)

Поколение 2:

Сертификат открытого ключа внешнего устройства ГНСС для взаимной проверки аутентификации с БУ. Структура данного сертификата представлена в ~~приложении~~ **подразделе 11**.

EGFCertificate ::= Сертификат

2.65 EmbedderIcAssemblerId (идентификатор монтажного/сборочного предприятия)

Содержит информацию о монтажном предприятии ИС.

EmbedderIcAssemblerId ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

countryCode	Строка IA5(РАЗМЕР(2))
moduleEmbedder	Строка BCD(РАЗМЕР(2))
manufacturerInformation	ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))
}	

countryCode — двухбуквенный код страны монтажного предприятия модуля в соответствии с ISO 3166.

moduleEmbedder — идентификатор монтажного предприятия модуля.

manufacturerInformation — для внутреннего пользования изготовителя.

2.66 EntryTypeDailyWorkPeriod (ввод данных о периоде и типе ежедневной работы)

Код, позволяющий провести различие между началом и концом ввода данных о месте ежедневного периода работы и условиями ввода.

Поколение 1

EntryTypeDailyWorkPeriod ::= ЦЕЛОЕ ЧИСЛО {

Начало, относительное время = время ввода карточки
или время ввода данных (0)

Конец, относительное время = время извлечения карточки
или время ввода данных (1)

Начало, относительное время (начало) (2)

Конец, относительное время ручного ввода данных
(конец рабочего периода) (3)

Начало, относительное время, зафиксированное БУ (4)

Конец, относительное время, зафиксированное БУ (5)

}

Присвоение значения: в соответствии с ISO/IEC8824-1.

Поколение 2

EntryTypeDailyWorkPeriod ::= ЦЕЛОЕ ЧИСЛО {

Начало, относительное время = время ввода карточки
или время ввода данных (0)

Конец, относительное время = время извлечения карточки
или время ввода данных (1)

Начало, относительное время ручного ввода данных
(время начала работы) (2)

Конец, относительное время ручного ввода данных
(конец рабочего периода) (3)

~~начало, относительное время, зафиксированное БУ (4)~~

~~конец, относительное время, зафиксированное БУ (5)~~

~~Начало, относительное время на основе данных ГНСС (6)~~

~~Конец, относительное время на основе данных ГНСС (7)~~

}

Присвоение значения: в соответствии с ISO/IEC8824-1.

2.67 EquipmentType (тип оборудования)

Код, позволяющий провести различие между разными типами оборудования в связи с использованием тахографа.

EquipmentType ::= ЦЕЛОЕ ЧИСЛО (0..255)

Поколение 1:

– Зарезервировано (0)

– карточка водителя (1)

– карточка мастерской (2)

– карточка контролера (3)

– карточка предприятия (4)

– карточка изготовителя (5)

– бортовое устройство (6)

– датчик движения (7)

– RFU (8..255)

Присвоение значения: в соответствии с ISO/IEC8824-1.

Значение 0 зарезервировано для целей указания ~~государства-члена или Европы~~
Договаривающейся стороны или корневого органа в поле данных СНА сертификатов.

Поколение 2:

Используются те же значения, что и в случае поколения 1, со следующими дополнениями:

– Устройство ГНСС (8)

– Модуль удаленной связи (9)

– Модуль интерфейса ИТС (10)

– Табличка	(11) – можно использовать в случае “in SealRecord” (регистрация пломбы)
– Адаптер M1/N1	(12) – можно использоваться в случае “in SealRecord” (регистрация пломбы)
– Европейский Европейский Корневой CA (ERCA)	(13)
– Государство-член Договаривающаяся сторона CA (MSCA)	(14)
– Внешняя связь ГНСС	(15) – можно использовать в случае “inSealRecord” (регистрация пломбы)
– Не используется	(16) – используется в “SealDataVu” (данные касающиеся пломб, в БУ)
– Карточка водителя (sSign)	(17) – используется только в поле СНА для подписания сертификата
– Карточка мастерской (sSign)	(18) – используется только в поле СНА для подписания сертификата
– Бортовое устройство (sSign)	(19) – используется только в поле СНА для подписания сертификата
– RFU	(20..255)

Примечание 1: Значения второго поколения применительно к табличке, адаптеру и внешнему соединению ГНСС, а также значения первого поколения применительно к бортовому устройству и датчику движения могут использоваться в случае SealRecord, т. е. в случае применимости.

Примечание 2: В поле CardHolderAuthorisation (СНА) сертификата поколения 2 значения (1), (2) и (6) следует интерпретировать как указывающие на сертификат взаимной аутентификации соответствующего типа оборудования. Для указания соответствующего сертификата, необходимого для создания цифровой подписи следует использовать параметры (17), (18) или (19).

2.68 EuropeanPublicKey (европейский открытый ключ)

Поколение 1:

~~Европейский~~ Европейский Корневой открытый ключ.

EuropeanPublicKey ::= PublicKey

2.69 EventFaultRecordPurpose (цель регистрации события или неисправности)

Код, указывающий на причину регистрации события или неисправности.

EventFaultType ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))

Присвоение значения:

‘00’H	одно из 10 самых недавних (или последних) событий или неисправностей
‘01’H	самое продолжительное событие за один из последних 10 дней наличия данного случая
‘02’H	одно из 5 самых продолжительных событий за последние 365 дней
‘03’H	последнее событие за один из последних 10 дней наличия данного случая

'04'H	самое серьезное событие за один из последних 10 дней наличия данного случая
'05'H	одно из 5 самых продолжительных событий за последние 365 дней
'06'H	Первое событие или первая неисправность, наступившее или проявившееся после последней калибровки
'07'H	текущее/продолжающееся событие или текущая/продолжающаяся неисправность
'08'H — '7F'H	RFU
'80'H — 'FF'H	относится конкретно к изготовителю

2.70 EventFaultType (событие: тип неисправности)

Код, отображающий событие или неисправность.

EventFaultType ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))

Присвоение значения:

Поколение 1:

'0x'H	обычные события
'00'H	дополнительно не уточняется
'01'H	ввод недействительной карточки
'02'H	несовместимость карточек
'03'H	нестыковка во времени
'04'H	управление без соответствующей карточки
'05'H	ввод карточки во время управления
'06'H	неправильное завершение последнего сеанса использования карточки
'07'H	превышение скорости
'08'H	прекращение электропитания
'09'H	ошибка данных о движении
'0A'H	противоречивые данные о движении транспортного средства
'0B' — '0F'H	RFU
'1x'H	события, связанные с попыткой нарушения защиты бортового устройства
'10'H	дополнительно не уточняется
'11'H	сбой в аутентификации датчика движения
'12'H	сбой в аутентификации карточки тахографа
'13'H	несанкционированная модификация датчика движения
'14'H	ошибка при проверке целостности введенных данных карточки
'15'H	ошибка при проверке целостности сохраненных пользовательских данных
'16'H	ошибка при внутренней передаче данных
'17'H	несанкционированное вскрытие корпуса
'18'H	саботаж аппаратного обеспечения

'19'Н — '1F'Н	RFU
'2x'Н	события, связанные с попыткой нарушения защиты бортового устройства
'20'Н	дополнительно не уточняется
'21'Н	сбой в аутентификации
'22'Н	ошибка при проверке целостности сохраненных пользовательских данных
'23'Н	ошибка при внутренней передаче данных
'24'Н	несанкционированное вскрытие корпуса
'25'Н	саботаж аппаратного обеспечения
'26'Н — '2F'Н	RFU
'3x'Н	неисправности записывающего оборудования контрольного устройства
'30'Н	дополнительно не уточняется
'31'Н	внутренние неполадки в БУ
'32'Н	неисправность принтера
'33'Н	неисправность дисплея
'34'Н	неисправность при загрузке
'35'Н	неисправность датчика
'36'Н — '3F'Н	RFU
'4x'Н	неисправности карточки
'40'Н	дополнительно не уточняется
'41'Н — '4F'Н	RFU
'50'Н — '7F'Н	RFU
'80'Н — 'FF'Н	относится конкретно к изготовителю

Поколение 2, версия 1:

~~Используются те же значения, что и в случае поколения 1, со следующими дополнениями:~~

'0x'Н	обычные события
'00'Н	дополнительно не уточняется
'01'Н	ввод недействительной карточки
'02'Н	несовместимость карточек
'03'Н	накладка по времени
'04'Н	управление без соответствующей карточки
'05'Н	ввод карточки во время управления
'06'Н	неправильное завершение последнего сеанса использования карточки
'07'Н	превышение скорости
'08'Н	прекращение электропитания
'09'Н	ошибка данных датчика движения
'0A'Н	противоречивые данные о движении транспортного средства

'0B'H	нестыковка во времени (ГНСС и внутренние часы БУ)
'0C' — '0F'H	ошибка связи со средством удаленной связи
'0D'H	отсутствие информации о местоположении из приемника ГНСС
'0E'H	ошибка связи с внешним устройством ГНСС
'0F'H	RFU
'5x'H-GNSS '1x'H	сопутствующие неисправности сбои в системе защиты бортового устройства
50H'10'H	дополнительно не уточняется
'51'H '11'H	сбой в аутентификации датчика движения
'12'H	сбой в аутентификации карточки тахографа
'13'H	несанкционированное изменение датчика движения
'14'H	ошибка при проверке целостности введенных данных карточки
'15'H	ошибка при проверке целостности сохраненных пользовательских данных
'16'H	внутренний сбой при передаче Передача данных в неисправностях внутреннего GNSS приемника
'52'H	неисправность внешнего приемника ГНСС
'53'H	сбой в работе системы внешней связи ГНСС
'54'H	отсутствие данных ГНСС о местоположении
'55'H '17'H	несанкционированное вскрытие корпуса
'18'H	саботаж аппаратного обеспечения
'19'H	обнаружение взлома ГНСС
'56'H '1A'H	сбой аутентификации внешнего устройства ГНСС
'1B'H	истечение срока действия сертификата внешнего устройства ГНСС
'57'H 1C 'H — '5F' '1F'H	RFU
'6x'H '2x'H	события, связанные с попыткой нарушения защиты бортового устройства
'20'H	дополнительно не уточняется
'21'H	сбой в системе аутентификации
'22'H	ошибка целостности сохраненных данных
'23'H	ошибка в процессе внутренней передачи данных
'24'H	несанкционированное вскрытие корпуса
'25'H	саботаж аппаратного обеспечения
'26'H — '2F'H	RFU
'3x'H	сбой в работе контрольного устройства
'30'H	дополнительно не уточняется
'31'H	внутренние неполадки в БУ
'32'H	внутренние неполадки в принтере

'33'Н	неисправность дисплея
'34'Н	неисправность при загрузке
'35'Н	неисправность датчика
'36'Н	внутренний приемник ГНСС
'37'Н	внешнее устройство ГНСС
'38'Н	устройство удаленной связи, неисправность модуля удаленной связи
'60'Н	дополнительно не уточняется
'61'Н	неисправность модуля удаленной связи
'62'Н	устройство неисправность модуля удаленной связи
'63'Н — '6F'Н	RFU
'7x'Н '39'Н	неисправность интерфейса ИТС
'70'Н 3A'Н — '3F'Н	RFU
'4x'Н	сбои в работе карточки
'40'Н	дополнительно не уточняется
'71'Н '41F'Н — '4F'Н	RFU
'50'Н — '7F'Н	RFU
'80'Н — 'FF'Н	относится конкретно к изготовителю
Поколение 2, версия 2:	
'0x'Н	обычные события
'00'Н	дополнительно не уточняется
'01'Н	ввод недействительной карточки
'02'Н	несовместимость карточек
'03'Н	накладка по времени
'04'Н	управление без соответствующей карточки
'05'Н	ввод карточки во время управления
'06'Н	неправильное завершение последнего сеанса использования карточки
'07'Н	превышение скорости
'08'Н	прекращение электропитания
'09'Н	ошибка в данных датчика движения
'0A'Н	противоречивые данные о движении транспортного средства
'0B'	нестыковка во времени (ГНСС и внутренние часы БУ)
'0C'Н	ошибка связи со средством удаленной связи
'0D'Н	отсутствие информации о местоположении из приемника ГНСС
'0E'Н	сбой связи с внешним устройством ГНСС
'0F'Н	аномалия ГНСС

'1x'Н	события, связанные с попыткой нарушения защиты бортового устройства
'10'Н	дополнительно не уточняется
'11'Н	сбой в аутентификации датчика движения
'12'Н	сбой в аутентификации карточки тахографа
'13'Н	несанкционированное изменение датчика движения
'14'Н	ошибка при проверке целостности введенных данных карточки
'15'Н	ошибка при проверке целостности сохраненных пользовательских данных
'16'Н	ошибка при внутренней передаче данных
'17'Н	несанкционированное вскрытие корпуса
'18'Н	саботаж аппаратного обеспечения
'19'Н	обнаружение взлома ГНСС
'1A'Н	сбой в аутентификации внешнего устройства ГНСС
'1B'Н	истечение срока действия сертификата внешнего устройства ГНСС
'1C'Н	несоответствие между данными о движении и сохраненными данными о деятельности водителя
'1D'Н — '1F'Н	RFU
'2x'Н	события, связанные с попытками нарушения системы защиты датчиков безопасности
'20'Н	дополнительно не уточняется
'21'Н	сбой в аутентификации
'22'Н	ошибка целостности сохраненных данных
'23'Н	ошибка при внутренней передаче данных
'24'Н	несанкционированное вскрытие корпуса
'25'Н	саботаж аппаратного обеспечения
'26'Н — '2F'Н	RFU
'3x'Н	неисправность контрольного устройства
'30'Н	дополнительно не уточняется
'31'Н	внутренние неполадки в БУ
'32'Н	неполадки в принтере
'33'Н	неисправность дисплея
'34'Н	неисправность при загрузке
'35'Н	неисправность датчика
'36'Н	внутренний приемник ГНСС
'37'Н	внешнее устройство ГНСС
'38'Н	устройство удаленной связи
'39'Н	интерфейс ИТС

'3A'H	неисправность внутреннего датчика
'3B'H — '3F'H	RFU
'4x'H	сбои в работе карточки
'40'H	дополнительно не уточняется
'41'H — '4F'H	RFU
'50'H — '7F'H	RFU
'80'H — 'FF'H	относится конкретно к изготовителю

2.71 ExtendedSealIdentifier (расширенный идентификатор пломбы)

Поколение 2:

Расширенный идентификатор пломбы, однозначно идентифицирующий пломбу (приложение добавление 1С, требование 401).

```
ExtendedSerialNumber ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
manufacturerCode      Октетная строка IA5ОКТЕТНАЯ СТРОКА (РАЗМЕР(2))
sealIdentifier         Октетная строка IA5ОКТЕТНАЯ СТРОКА (РАЗМЕР(68))
}
```

manufacturerCode — код изготовителя пломбы.

Присвоение значения: см. регистрацию базы данных, которая управляется лабораторией, уполномоченной проводить испытания на эксплуатационную совместимость (см. <https://dtc.jrc.ec.europa.eu>).

sealIdentifier — идентификатор пломбы, уникальный для изготовителя.

Присвоение значения: буквенно-цифровой номер, уникальный в домене изготовителя в соответствии с [ISO8859-1].

2.72 ExtendedSerialNumber (расширенный серийный номер)

Уникальная идентификация оборудования. Она может использоваться в качестве идентификатора открытого ключа оборудования.

Поколение 1:

```
ExtendedSerialNumber ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
serialNumber          ЦЕЛОЕ ЧИСЛО(0..232-1)
monthYear             СтрокаBCD(РАЗМЕР(2))
тип                  ОКТЕТНАЯ СТРОКА(РАЗМЕР(1))
manufacturerCode     Код изготовителя
}
```

serialNumber — серийный номер оборудования, уникальный для данного изготовителя, типа оборудования и месяца и года, указанных ниже.

monthYear — идентификация месяца и года изготовления (или присвоение серийного номера).

Присвоение значения: код BCD месяца (две цифры) и года (две последние цифры).

type — идентификатор типа оборудования.

Присвоение значения: относится конкретно к изготовителю, с зарезервированным значением 'FFh'.

manufacturerCode — цифровой код идентификации изготовителя оборудования утвержденного типа.

Поколение 2:

```
ExtendedSerialNumber ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
serialNumber          ЦЕЛОЕ ЧИСЛО(0..232-1)
monthYear             Строка VCD(РАЗМЕР(2))
type                  Тип оборудования
manufacturerCode      Код изготовителя
}
```

serialNumber — см. Поколение 1

monthYear — см. Поколение 1

type — идентификатор типа оборудования.

manufacturerCode — см. Поколение 1.

2.73 FullCardNumber (полный номер карточки)

Код, полностью идентифицирующий карточку тахографа.

```
FullCardNumber ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
cardType              Тип оборудования
cardIssuingMemberState Цифровой код страны,
cardNumber            Номер карточки
}
```

cardType — тип карточки тахографа.

cardIssuingMemberState — код государства-члена, ~~выдавшего~~ Договаривающейся стороны, ~~выдавшей~~ карточку.

cardNumber — номер карточки.

2.74 FullCardNumberAndGeneration (полный номер и поколение карточки)

Поколение 2:

Код, полностью идентифицирующий карточку тахографа и ее поколение.

```
FullCardNumber ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
FullCardNumber        Полный номер карточки
поколение             Поколение
}
```

fullcardNumber идентифицирует карточку тахографа.

generation указывает на поколение используемой карточки тахографа.

2.75 Generation (поколение)

Поколение 2:

Указывает на поколение используемого тахографа.

Generation ::= ЦЕЛОЕ ЧИСЛО(0..255)

Присвоение значения:

'00'Н	RFU
'01'Н	Поколение 1
'02'Н	Поколение 2
'03'Н .. 'FF'Н	RFU

2.76 GeoCoordinates (геокоординаты)

Поколение 2:

Геокоординаты кодируются как целые числа. Такие целые числа представляют собой показатель кодирования $\pm DDMM.M$ по широте и $\pm DDDMM.M$ по долготе. В данном случае $\pm DD$ и соответственно $\pm DDD$ обозначают градусы, а $MM.M$ — минуты. **Показатели долготы и широты неизвестного местоположения должны быть представлены в виде шестнадцатеричной записи '7FFFFFFF' (десятичная запись 8388607).**

GeoCoordinates ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

широта ЦЕЛОЕ ЧИСЛО(-90000..90001)

долгота ЦЕЛОЕ ЧИСЛО(-180000..180001)

}

широта кодируется как множитель (коэффициент 10) выражения $\pm DDMM.M$.

долгота кодируется как множитель (коэффициент 10) выражения $\pm DDDMM.M$.

2.77 GNSSAccuracy (точность ГНСС)

Поколение 2:

Точность данных ГНСС о местоположении (определение ее). Эта точность кодируется как целое число и является множителем (коэффициент 10) значения X.Y из строки GSA NMEA.

GNSSAccuracy ::= ЦЕЛОЕ ЧИСЛО(1..100)

2.78 ~~GNSSAccumulatedDriving~~

2.78 GNSSAccumulatedDriving (накопленное время управления по ГНСС)

Поколение 2:

Информация, записанная на карточке водителя или мастерской, которая относится к местоположению транспортного средства по ГНСС, если ~~непрерывное~~ **накопленное** время управления водителем достигает значения, кратного трем часам (**приложение добавление 1С, требования 306 и 354**).

~~GNSSContinuousDriving~~ **GNSSAccumulatedDriving** := ПОСЛЕДОВАТЕЛЬНОСТЬ {

~~gnssCDPointerNewestRecord~~ **gnssADPointerNewestRecord**

ЦЕЛОЕ ЧИСЛО (0..NoOfGNSSADRecords NoOfGNSSADRecords -1)

gnssContinuousDrivingRecords gnssAccumulatedDrivingRecords

УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfGNSSCDRecords NoOfGNSSADRecords)

ПАРАМЕТРА GNSSContinuousDrivingRecord GNSSAccumulatedDrivingRecord

}

gnssCDPointerNewestRecord gnssADPointerNewestRecord — индекс последней обновленной записи ГНСС, касающейся непрерывного накопленного времени управления.

Присвоение значения: число, соответствующее числовому показателю записи данных ГНСС о непрерывном накопленном времени управления, которое начинается с “0” в случае первой регистрации записей ГНСС, касающихся накопленного управления, в структуре данных.

gnssContinuousDrivingRecords gnssAccumulatedDrivingRecords — совокупность записей, содержащих дату и время, когда непрерывное накопленное время управления достигает значения, кратного трем часам, и информацию о местоположении транспортного средства.

2.79 GNSSContinuousDrivingRecord GNSSAccumulatedDrivingRecord (запись накопленного времени управления по ГНСС)

Поколение 2:

Информация, записанная на карточке водителя или мастерской, которая относится к местоположению транспортного средства по ГНСС, если непрерывное накопленное время управления водителем достигает значения, кратного трем часам (приложение добавление 1С, требования 305 и 353).

GNSSContinuousDrivingRecord GNSSAccumulatedDrivingRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

timeStamp Реальное время

gnssPlaceRecord Запись названия места по ГНСС

vehicleOdometerValue Показания счетчика пробега

}

timeStamp — дата и время, когда непрерывное накопленное время управления владельцем карточки достигает значения, кратного трем часам.

gnssPlaceRecord содержит информацию, касающуюся местоположения транспортного средства.

vehicleOdometerValue — показания счетчика пробега, когда накопленное время управления достигает значения, кратного трем часам.

2.79a GNSSAuthAccumulatedDriving (разрешенное накопленное время управления по ГНСС)

Поколение 2, версия 2:

Информация, записанная на карточке водителя или мастерской, которая относится к местоположению транспортного средства по ГНСС, если непрерывное накопленное время управления достигает значения, кратного трем часам (добавление 1С, требования 306d и 356d).

GNSSAuthAccumulatedDriving ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

gnssAuthADPointerNewestRecord ЦЕЛОЕ ЧИСЛО(0..NoOfGNSSCDRecords -1)

gnssAuthStatusADRecords УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfGNSSADRecords)
ПАРАМЕТРА GNSSAuthStatusADRecord

}

gnssAuthADPointerNewestRecord — индекс последней обновленной записи ГНСС, касающейся статуса аутентификации местоположения.

Присвоение значения: число, соответствующее числовому показателю записи данных ГНСС о статусе аутентификации местоположения, начиная с '0' в случае первой регистрации записи ГНСС, касающейся аутентификации местоположения, в структуре данных.

gnssAuthStatusADRecords — совокупность записей, содержащих дату и время, когда накопленное время управления достигает значения, кратного трем часам, и статус аутентификации информации о местоположении по ГНСС.

2.79b GNSSAuthStatusADRecord (запись данных в БУ о НакВУ по ГНСС)

Поколение 2, версия 2:

Информация, записанная на карточке водителя или мастерской, которая относится к статусу аутентификации местоположения транспортного средства по ГНСС, если накопленное время управления достигает значения, кратного трем часам (добавление 1С, требования 306с и 356с). Другая информация, связанная с местоположением самой ГНСС, хранится в другой записи (см. 2.79 GNSSAccumulatedDrivingRecord).

GNSSAuthStatusADRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

timeStamp	Реальное время
authenticationStatus	Статус аутентификации местоположения

}

timeStamp — дата и время, когда накопленное время управления достигает значения, кратного трем часам (это — та же дата и время, что и в соответствующей записи GNSSAccumulatedDrivingRecord).

authenticationStatus — статус аутентификации местоположения по ГНСС, когда накопленное время управления достигает значения, кратного трем часам.

2.79c GNSSPlaceAuthRecord (запись аутентифицированного места по ГНСС)

Поколение 2, версия 2:

Информация, которая имеет отношение к местоположению транспортного средства по ГНСС (приложение 1С, требования 108, 109, 110, 296, 306а, 306с, 306е, 306g, 356а, 356с, 356е и 356g)).

GNSSAuthStatusADRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

timeStamp	Реальное время
gnssAccuracy	Точность GNSS
GeoCoordinates	Геокоординаты
authenticationStatus	Статус аутентификации местоположения

}

timeStamp — дата и время, когда установлено местоположение транспортного средства по ГНСС.

gnssAccuracy — точность данных ГНСС о местоположении.

geoCoordinates — местоположение, зарегистрированное с помощью ГНСС.

authenticationStatus — статус аутентификации позиции ГНСС на момент ее определения.

2.80 GNSSPlaceRecord (запись названия места по ГНСС)

Поколение 2:

Информация, которая имеет отношение к местоположению транспортного средства по ГНСС (приложение добавление 1С, требования 108, 109, 110, 296, 305, 347 и 353).

GNSSAuthStatusADRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

timeStamp Реальное время

gnssAccuracy Точность GNSS

geoCoordinates Геокоординаты

}

timeStamp — дата и время, когда установлено местоположение транспортного средства по ГНСС.

gnssAccuracy — точность данных ГНСС о местоположении.

geoCoordinates — местоположение, зарегистрированное с помощью ГНСС.

2.81 HighResOdometer (счетчик пробега с высоким разрешением)

Показания счетчика пробега транспортного средства: совокупное расстояние, пройденное транспортным средством за период его эксплуатации.

HighResOdometer ::= ЦЕЛОЕ ЧИСЛО(0..2³²-1)

Присвоение значения: Двоичное значение без знака. Значение, равное 1/200 км в рабочем диапазоне от 0 до 21 055 406 км.

2.82 HighResTripDistance (расстояние, пройденное за рейс, с высоким разрешением)

Расстояние, пройденное за весь или часть рейса.

HighResTripDistance ::= ЦЕЛОЕ ЧИСЛО(0..2³²-1)

Присвоение значения: двоичное значение без знака. Значение, равное 1/200 км в рабочем диапазоне от 0 до 21 055 406 км.

2.83 HolderName (фамилия и имя (имена) держателя)

Фамилия и имя (имена) держателя карточки.

HolderName ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

holderSurname Фамилия

holderFirstNames Имя (имена)

}

holderSurname — фамилия держателя. Фамилия не включает в себя форму обращения.

Присвоение значения: если карточка не именная, то позиция **holderSurname** содержит ту же информацию, что и **companyName** или **workshopName**, или **controlBodyName**.

holderFirstNames — имя (имена) и инициалы держателя.

2.84 Зарезервировано для будущего использования **InternalGNSSReceiver**

Поколение 2:

~~Информация о том, является ли приемник ГНСС внешним или внутренним устройством бортового устройства. True — приемник ГНСС встроен в БУ. False — приемник ГНСС является внешним устройством.~~

~~InternalGNSSReceiver ::= BOOLEAN~~

2.85 **K-ConstantOfRecordingEquipment** (постоянная К записывающего оборудования)

Постоянная величина ~~записывающего оборудования~~ **контрольного устройства** (определение m).

Постоянная К записывающего оборудования ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: импульсы на километр в рабочем диапазоне от 0 до 64 255 имп./км.

2.86 **KeyIdentifier** (идентификатор ключа)

Уникальный идентификатор открытого ключа, используемого для назначения и выбора ключа. Он также идентифицирует держателя ключа.

KeyIdentifier ::= ВЫБОР {

extendedSerialNumber	Расширенный серийный номер
certificateRequestID	ИД запроса на сертификат
certificationAuthorityKID	Сертификационный орган ключа

}

Первый вариант подходит для ссылки на открытый ключ бортового устройства, карты тахографа **или внешнего устройства ГНСС**.

Второй вариант выбора подходит для ссылки на открытый ключ бортового устройства (если в ~~момент~~ **случае** создания сертификата серийный номер бортового устройства неизвестен).

Третий вариант выбора подходит для ссылки на открытый ключ ~~государства-члена Договаривающейся стороны~~.

2.87 **KMWCKey** (ключ KMWC)

Поколение 2:

Ключ AES и связанная с ним версия ключа используются для соединения БУ и датчика движения. Подробную информацию см. в ~~приложении~~ **подразделе 11**.

KMWCKey ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

kMWCKey	AESKey
keyVersion	ЦЕЛОЕ ЧИСЛО (РАЗМЕР(1))

}

kMWCKey — длина ключа AES, соединенного с ключом, используемым для соединения БУ и датчика движения.

keyVersion обозначает основную версию ключа AES.

2.88 Language (язык)

Код, идентифицирующий язык.

Language ::= СтрокаIA5(РАЗМЕР(2))

Присвоение значения: код в виде двух строчных букв в соответствии со стандартом ISO 639.

2.89 LastCardDownload (последняя дата загрузки с карточки)

Дата и время, записанные на карточке водителя, последней загрузки данных с карточки (для иных целей, кроме контроля) (~~приложение~~ **добавление 1С**, требования 257 и 282). Эта дата может обновляться БУ или любым считывающим устройством.

LastCardDownload ::= Реальное время

Присвоение значения: дополнительно не указывается.

2.89a LengthOfFollowingData (длина следующих данных)

Поколение 2, версия 2:

Индикатор длины для расширяемых записей.

LengthOfFollowingData ::= ЦЕЛОЕ ЧИСЛО(0... 2¹⁶-1)

Присвоение значения: см. подраздел 2.

2.90 LinkCertificate (связывающий сертификат)

Поколение 2:

Связывающий сертификат для пар ключей Европейского корневого сертификационного органа

LinkCertificate ::= Certificate

2.90a LoadType (тип груза)

Поколение 2, версия 2:

Введенный код, идентифицирующий тип груза.

LoadType ::= ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения:

'00'Н	Неопределенный тип груза
'01'Н	Грузы
'02'Н	Пассажиры
'03'Н .. 'FF'Н	RFU

2.91 L-TyreCircumference (окружность шины L)

Фактическая окружность шин колес (определение u).

Окружность шины L ::= ЦЕЛОЕ ЧИСЛО(0.. 2¹⁶-1)

Присвоение значения: двоичное значение без знака; значение в 1/8 мм в рабочем диапазоне от 0 до 8031 мм.

2.92 MAC (MAC)

Поколение 2:

криптографическая контрольная сумма длиной 8, 12 или 16 байтов, соответствующая наборам шифров, представленным в ~~приложении~~ подразделе 11.

```
MAC ::= ВЫБОР {
mac8      ОКТЕТНАЯ СТРОКА(РАЗМЕР(8))
mac12     ОКТЕТНАЯ СТРОКА(РАЗМЕР(12))
mac16     ОКТЕТНАЯ СТРОКА(РАЗМЕР(16))
}
```

2.93 ManualInputFlag (метка ручного ввода)

Код, позволяющий определить, ввел ли держатель карточки данные о деятельности водителя вручную в момент ввода карточки или нет (~~приложение~~ **добавление 1В**, требование 081 и ~~приложение~~ **добавление 1С**, требование 102).

```
ManualInputFlag ::= ЦЕЛОЕ ЧИСЛО {
noEntry(отсутствие записи)      (0)
manualEntries (ручная запись)  (1)
}
```

Присвоение значения: дополнительно не указывается.

2.94 ManufacturerCode (код изготовителя)

Код идентификации изготовителя оборудования утвержденного типа.

```
ManufacturerCode ::= ЦЕЛОЕ ЧИСЛО(0..255)
```

Лаборатория, уполномоченная проводить испытания на эксплуатационную совместимость, составляет и публикует перечень кодов изготовителей на своем веб-сайте (~~приложение~~ **добавление 1С**, требование 454).

ManufacturerCodes временно присваиваются разработчикам оборудования тахографов при подаче заявки лаборатории, уполномоченной проводить испытания на эксплуатационную совместимость.

2.95 ManufacturerSpecificEventFaultData (данные о неисправности, связанной с конкретным изготовителем)

Поколение 2:

Коды ошибок, связанные с конкретными изготовителями, упрощают анализ ошибок и обслуживание бортовых устройств.

```
ManufacturerSpecificEventFaultData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ
manufacturerCode      Код изготовителя
manufacturerSpecificErrorCode  ОКТЕТНАЯ СТРОКА(РАЗМЕР(3))
}
```

manufacturerCode идентифицирует изготовителя бортового устройства.

ManufacturerSpecificErrorCode — код ошибки, связанный с конкретным изготовителем.

2.96 MemberStateCertificate (сертификат государства-члена)

Сертификат открытого ключа ~~государства-члена~~ Договаривающейся стороны, выданный ~~Европейским~~ **Корневым** сертификационным органом.

MemberStateCertificate ::= Certificate

2.97 MemberStateCertificateRecordArray (записи о сертификате государства-члена и метаданные)

Поколение 2:

Сертификат ~~государства-члена~~ Договаривающейся стороны и метаданные, используемые в протоколе загрузки.

MemberStateCertificateRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType	тип записи
recordSize	ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords	ЦЕЛОЕ ЧИСЛО(0..65535)
records	УСТАНОВЛЕНИЕ РАЗМЕРА (noOfRecords) ПАРАМЕТРА записи сертификата государства-члена

}

recordType указывает на тип записи (MemberStateCertificate).

Присвоение значения: см. RecordType.

recordSize — размер MemberStateCertificate в байтах.

noOfRecords — число записей в совокупности записей. Значение устанавливается на 1, так как сертификаты могут быть разной длины.

records — набор сертификатов ~~государств-членов~~ Договаривающихся сторон.

2.98 MemberStatePublicKey (открытый ключ государства-члена)

Поколение 1:

Открытый ключ ~~государства-члена~~ Договаривающейся стороны.

EuropeanPublicKey ::= PublicKey

2.99 Name (название)

а) название;

Name ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

codePage	ЦЕЛОЕ ЧИСЛО (0..255)
название	ОКТЕТНАЯ СТРОКА(РАЗМЕР35))

}

codePage определяет набор символов, указанный в главе 4,

name — название, закодированное с помощью указанного набора символов.

2.100 NationAlpha (буквенный код страны)

Буквенное обозначение страны соответствует отличительным знакам, используемым на транспортных средствах в международном сообщении (Венская конвенция ООН о дорожном движении 1968 года).

NationAlpha ::= СтрокаIA5(РАЗМЕР3))

NationAlpha и цифровые коды включаются в перечень, составляемый на веб-сайте лаборатории, назначенной для проведения испытаний на эксплуатационную совместимость, как указано в требовании 440 приложения добавления 1С.

2.101 NationNumeric (цифровой код страны)

Цифровое обозначение страны.

NationNumeric ::= ЦЕЛОЕ ЧИСЛО(0 255)

Присвоение значения: см. тип данных 2.100 (буквенное обозначение страны).

Любое изменение или обновление спецификации буквенного или цифрового обозначения страны, описанного в предыдущем пункте, осуществляется только после того, как назначенная лаборатория получит отзывы изготовителей бортовых устройств цифровых и смарт-тахографов утвержденного типа.

2.101a NoOfBorderCrossingRecords (число записей о пересечении границы)

Поколение 2, версия 2:

Число записей о пересечении границы, которое может храниться на карточке водителя или мастерской.

NoOfBorderCrossingRecords ::= ЦЕЛОЕ ЧИСЛО(0.. 2¹⁶-1)

Присвоение значения: см. подраздел 2 добавления.

2.102 NoOfCalibrationRecords (число записей о калибровках)

Число записей о калибровке, которое может храниться на карточке мастерской.

Поколение 1:

NoOfCalibrationRecords ::= ЦЕЛОЕ ЧИСЛО(0..255)

Присвоение значения: см. добавление подраздел 2.

Поколение 2:

NoOfCalibrationRecords ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: см. добавление подраздел 2.

2.103 NoOfCalibrationsSinceDownload (число калибровок после загрузки данных)

Счетчик, указывающий на число калибровок, произведенных с карточкой мастерской после последней загрузки данных с этой карточки (приложение добавление 1С, требования 317 и 340).

NoOfCalibrationRecords ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: дополнительно не указывается.

2.104 NoOfCardPlaceRecords (число записей на карточке, касающихся мест)

Число записей на карточке, касающихся мест. Количество записей мест, которые могут храниться на карточке водителя или мастерской.

Поколение 1:

NoOfCalibrationRecords ::= ЦЕЛОЕ ЧИСЛО(0..255)

Присвоение значения: см. приложение подраздел 2.

Поколение 2:

NoOfCardPlaceRecords ::= ЦЕЛОЕ ЧИСЛО(0..216-1)

Присвоение значения: см. приложение подраздел 2.

2.105 NoOfCardVehicleRecords (число записей на карточке, касающихся транспортных средств)

Количество записей, касающихся использования транспортных средств, которые можно хранить на карточке водителя или мастерской.

NoOfCardVehicleRecords ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: см. приложение подраздел 2.

2.106 NoOfCardVehicleUnitRecords (число записей на карточке, касающихся единиц транспортных средств)

Поколение 2:

Количество записей, касающихся использования бортовых устройств, которые можно хранить на карточке водителя или мастерской.

NoOfCardVehicleRecords ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: см. приложение подраздел 2.

2.107 NoOfCompanyActivityRecords (число записей, касающихся операций предприятия)

Количество записей о деятельности предприятий, которые можно хранить на карточке предприятия.

NoOfCardVehicleRecords ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: см. приложение подраздел 2.

2.108 NoOfControlActivityRecords (число записей, касающихся операций по контролю)

Количество записей о деятельности по контролю, которые можно хранить на контрольной карточке.

NoOfCardVehicleRecords ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: см. приложение подраздел 2.

2.109 NoOfEventsPerType (число событий по типу)

Число событий в разбивке по типу события, которое можно хранить на карточке.

NoOfEventsPerType ::= ЦЕЛОЕ ЧИСЛО(0..255)

Присвоение значения: см. ~~приложение~~ подраздел 2.

2.110 NoOfFaultsPerType (число неисправностей по типу)

Число неисправностей в разбивке по типу неисправностей, которые можно хранить на соответствующей карточке.

NoOfEventsPerType ::= ЦЕЛОЕ ЧИСЛО(0..255)

Присвоение значения: см. ~~приложение~~ подраздел 2.

~~2.111 NoOfGNSSCDRecords~~

2.111 NoOfGNSSADRecords (число записей ГНСС, касающихся НакВУ)

Поколение 2:

Число записей о ~~непрерывном~~ **накопленном** времени управления по ГНСС, которые можно хранить на соответствующей карточке.

~~NoOfGNSSCDRecords~~ NoOfGNSSADRecords ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: см. ~~приложение~~ подраздел 2.

2.111a NoOfLoadUnloadRecords (число записей, касающихся загрузки/разгрузки)

Поколение 2, версия 2:

Число записей по загрузке/разгрузке, которые можно хранить на соответствующей карточке.

NoOfCardPlaceRecords ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: см. подраздел 2.

2.112 NoOfSpecificConditionRecords (число записей, касающихся особых условий)

Поколение 2:

Число записей по загрузке/разгрузке, которые можно хранить на соответствующей карточке.

NoOfCalibrationRecords ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: см. ~~добавление~~ подраздел 2.

2.112a NoOfLoadTypeEntryRecords (число записей о типе поступившего груза)

Поколение 2, версия 2:

Число записей о типе груза, которое можно хранить на карточке водителя или мастерской.

NoOfCardPlaceRecords ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: см. подраздел 2.

2.113 OdometerShort (показания счетчика пробега)

Показания счетчика пробега транспортного средства в сокращенном варианте.

OdometerShort ::= ЦЕЛОЕ ЧИСЛО(0..224-1)

Присвоение значения: Двоичное значение без знака. Значение в км в рабочем диапазоне от 0 до 9 999 999 км.

2.114 OdometerValueMidnight (показания счетчика пробега в полночь)

Показания счетчика пробега транспортного средства в полночь на данный день (~~приложение добавление 1В~~, требование 090 и ~~приложение добавление 1С~~, требование 113).

OdometerValueMidnight ::= OdometerShort

Присвоение значения: дополнительно не указывается.

2.114a OperationType (тип операции)

Поколение 2, версия 2:

Введенный код, идентифицирующий тип операции.

Поколение ::= ЦЕЛОЕ ЧИСЛО(0..255)

Присвоение значения:

'00'Н	RFU
'01'Н	Операция по загрузке
'02'Н	Операция по разгрузке
'03'Н	Операция по одновременной загрузке и разгрузке
'04'Н .. 'FF'Н	RFU

2.115 OdometerValueMidnightRecordArray (показания счетчика пробега в полночь и метаданные)

Поколение 2:

OdometerValueMidnight плюс метаданные, используемые в протоколе загрузки.

OdometerValueMidnightRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType	тип записи
recordSize	ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords	ЦЕЛОЕ ЧИСЛО(0..65535)
records	УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords) ПАРАМЕТРА OdometerValueMidnight
}	

recordType обозначает тип записи (OdometerValueMidnight).

Присвоение значения: см. RecordType.

recordSize — размер записи OdometerValueMidnight в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей **OdometerValueMidnight**.

2.116 **OverspeedNumber** (число превышений скорости)

Число случаев превышения скорости после последнего контроля за превышением скорости.

OverspeedNumber ::= ЦЕЛОЕ ЧИСЛО(0..255)

Присвоение значения: 0 означает, что после последнего контроля за превышением скорости случаев превышения скорости не было, 1 означает, что после последнего контроля за превышением скорости был один случай превышения скорости... 255 означает, что после последнего контроля за превышением скорости было 255 или больше случаев превышения скорости.

2.116a **PlaceAuthRecord** (запись аутентификации места)

Информация, касающаяся места, в котором начинается или заканчивается ежедневный период работы (добавление 1С, требования 108, 271, 296, 324 и 347).

Поколение 2, версия 2:

PlaceAuthRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

entryTime	Реальное время
entryTypeDailyWorkPeriod	Ввод данных о периоде и типе ежедневной работы
dailyWorkPeriodCountry	Цифровой код страны
dailyWorkPeriodRegion	Цифровой код региона
vehicleOdometerValue	Показания счетчика пробега
entryGNSSPlaceAuthRecord	Запись аутентификации места въезда по ГНСС

entryTime — дата и время ввода данных.

entryTypeDailyWorkPeriod — тип ввода данных о ежедневных периодах работы.

dailyWorkPeriodCountry — страна въезда.

dailyWorkPeriodRegion — страна въезда.

vehicleOdometerValue — показания счетчика пробега в момент ввода данных о месте.

entryGNSSPlaceAuthRecord — запись зарегистрированного места въезда, запись и время аутентификации места по ГНСС

2.116b **PlaceAuthStatusRecord** (запись статуса аутентификации места)

Поколение 2, версия 2:

Информация, хранящаяся на карточке водителя или мастерской, указывающей статус аутентификации места, в котором начинается или заканчивается ежедневный период работы (добавление 1С, требования 306а и 356а). Другая информация, связанная с самим местом, хранится в другой записи (см. 2.117 **PlaceRecord**).

PlaceAuthStatusRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
entryTime **Реальное время**
authenticationStatus **Статус аутентификации местоположения**
}

entryTime — дата и время, связанные с записью (это — та же дата и то же время, что и в соответствующей записи **PlaceRecord**).

authenticationStatus — статус аутентификации зарегистрированного местоположения по ГНСС.

2.117 **PlaceRecord (место, в котором начинается или заканчивается ежедневный период работы)**

Информация, касающаяся места, в котором начинается или заканчивается ежедневный период работы (~~приложение~~ **добавление 1С**, требования 108, 271, 296, 324 и 347).

Поколение 1:

PlaceRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
время ввода данных **Реальное время**
entryTypeDailyWorkPeriod **Ввод данных о периоде и типе ежедневной работы**
dailyWorkPeriodCountry **Цифровой код страны**
dailyWorkPeriodRegion **Цифровой код региона**
vehicleOdometerValue **Показания счетчика пробега транспортного средства**
}

entryTime — дата и время въезда.

entryTypeDailyWorkPeriod — тип ввода данных о ежедневных периодах работы.

dailyWorkPeriodCountry — введенная страна въезда.

dailyWorkPeriodRegion — введенный регион.

vehicleOdometerValue — показания счетчика пробега в момент ввода данных о месте въезда.

Поколение 2:

PlaceRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
entryTime **Реальное время**
EntryTypeDailyWorkPeriod **Тип ввода данных о ежедневных периодах работы**
dailyWorkPeriodCountry **Цифровой код страны**
dailyWorkPeriodRegion **Цифровой код региона**
vehicleOdometerValue **Показания счетчика пробега**
entryGNSSPlaceRecord **Запись о месте по ГНСС**
}

В дополнение к поколению 1 используется следующий компонент:

entryGNSSPlaceRecord — зарегистрированное место и время.

2.117a PositionAuthenticationStatus (статус аутентификации местоположения)

Поколение 2, версия 2:

PositionAuthenticationStatus ::= ЦЕЛОЕ ЧИСЛО(0..255)

Присвоение значения: см. подраздел 12.

'00'H	Не аутентифицирован (см. подраздел 12, требование GNS_39)
'01'H	Аутентифицирован (см. добавление 12, требование GNS_39)
'02'H .. 'FF'H	RFU

2.118 PreviousVehicleInfo (информация о предыдущем транспортном средстве)

Информация, касающаяся транспортного средства, использованного водителем ранее, в момент ввода его карточки в бортовое устройство (приложение добавление 1B, требование 081 и приложение добавление 1C, требование 102).

Поколение 1:

PreviousVehicleInfo ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

vehicleRegistrationIdentification Идентификация регистрации транспортного средства

cardWithdrawalTime Реальное время

}

vehicleRegistrationIdentification — VRN и государство-член Договаривающаяся страна регистрации транспортного средства.

cardWithdrawalTime — дата и время извлечения карточки.

Поколение 2:

PreviousVehicleInfo ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

vehicleRegistrationIdentification Идентификация регистрации транспортного средства

cardWithdrawalTime Реальное время

vuGeneration Поколение

}

В дополнение к поколению 1, используется следующий элемент:

vuGeneration идентифицирует поколение бортового устройства.

2.119 PublicKey (открытый ключ)

Поколение 1:

Открытый ключ RSA.

PublicKey ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

rsaKeyModulus Модуль ключа RSA

rsaKeyPublicExponent Открытая экспонента ключа RSA

}

rsaKeyModulus — Модуль пары ключей

rsaKeyPublicExponent — Открытая экспонента пары ключей

2.120 RecordType (тип записи)

Поколение 2:

Указание на тип записи. Этот тип данных используется в записи RecordArrays.

RecordType ::= ОКТЕТНАЯ СТРОКА(РАЗМЕР(1))

Присвоение значения:

'01'H	Данные об изменении вида деятельности
'02'H	Статус считывающего устройства карточки
'03'H	Текущая дата/время
'04'H	Сертификат государства-члена
'05'H	Показания счетчика пробега в полночь
'06'H	Дата и время загрузки
'07'H	Подсоединенный датчик
'08'H	Подпись
'09'H	Запись, касающаяся особых условий
'0A'H	Идентификационный номер транспортного средства
'0B'H	Регистрационный номер транспортного средства
'0C'H	Данные в БУ о калибровке
'0D'H	Запись данных в БУ о циклах ввода и извлечения карточек
'0E'H	Запись данных в БУ об используемой карточке
'0F'H	Сертификат БУ
'10'H	Запись данных в БУ о блокировке предприятием и метаданные
'11'H	Запись данных в БУ о контроле за деятельностью
'12'H	Данные в БУ о скорости транспортного средства
'13'H	Сроки хранения данных
'14'H	Данные в БУ о последней загрузке
'15'H	Запись данных в БУ о событиях
'16'H	УчГНССДRecord запись данных в БУ о НепВУ по ГНСС
'17'H	Запись в БУ о согласии водителя использовать ИТС
'18'H	Запись данных в БУ о неисправностях
'19'H	Идентификация бортового устройства
'1A'H	Данные в БУ о превышении скорости
'1B'H	Запись данных в БУ о событиях превышения скорости
'1C'H	Запись данных в БУ о месте, где начинается и заканчивается ежедневный период работ
'1D'H	Данные в БУ о корректировке времени по ГНСС
'1E'H	Запись данных в БУ о корректировке времени
'1F'H	Запись данных в БУ о прекращении электропитания
'20'H	Запись данных о подсоединении датчика
'21'H	Запись о подсоединении внешнего датчика ГНСС

'22'Н — '7F'Н	Запись данных в БУ о пересечении границы RFU
'2380'Н — 'FF'Н	Запись данных в БУ о загрузке/разгрузке, но — уместно изготовителя
'24'Н	Идентификация регистрации транспортного средства
'25'Н — '7F'Н	RFU
'80'Н — 'FF'Н	относится к конкретному изготовителю

2.121 RegionAlpha (буквенный код региона)

Буквенное обозначение региона в конкретной стране.

RegionAlpha ::= IA5STRING(SIZE3))

Поколение 1:

Присвоение значения:

' ' Нет информации

Испания:

'AN'	Андалусия
'AR'	Арагон
'AST'	Астурия
'C'	Кантабрия
'CAT'	Каталония
'CL'	Кастилья-Леон
'CM'	Кастилья-Ла-Манча
'CV'	Валенсия
'EXT'	Эстремадура
'G'	Галисия
'IB'	Балеарские острова
'IC'	Канарские острова
'LR'	Ла-Риоха
'M'	Мадрид
'MU'	Мурсия
'NA'	Наварра
'PV'	Страна Басков

Поколение 2:

Буквенные коды регионов включаются в перечень, составляемый на веб-сайте лаборатории, назначенной для проведения испытаний на эксплуатационную совместимость.

2.122 RegionNumeric (цифровой код региона)

Цифровое обозначение региона в конкретной стране.

RegionNumeric ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))

Поколение 1:

Присвоение значения:

'00'N Нет информации,

Испания:

'01'N	Андалусия
'02'N	Арагон
'03'N	Астурия
'04'N	Кантабрия
'05'N	Каталония
'06'N	Кастилья-Леон
'07'N	Кастилья-Ла-Манча
'08'N	Валенсия
'09'N	Эстремадура
'0A'N	Галисия
'0B'N	Балеарские острова
'0C'N	Канарские острова
'0D'N	Ла-Риоха
'0E'N	Мадрид
'0F'N	Мурсия
'10'N	Наварра
'11'N	Страна Басков

Поколение 2:

Буквенные коды регионов включаются в перечень, составляемый на веб-сайте лаборатории, назначенной для проведения испытаний на эксплуатационную совместимость.

2.123 RemoteCommunicationModuleSerialNumber (серийный номер модуля удаленной связи)

Поколение 2:

Серийный номер модуля удаленной связи.

RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber

2.124 RSAKeyModulus (модуль ключа RSA)

Поколение 1:

Модуль пары ключей RSA.

RSAKeyModulus ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(128))

Присвоение значения: не указано.

2.125 RSAKeyPrivateExponent (закрытая экспонента ключа RSA)

Поколение 1:

Закрытая экспонента пары ключей RSA.

RSAKeyModulus ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (128))

Присвоение значения: не указано.

2.126 RSAKeyPublicExponent (открытая экспонента ключа RSA)

Поколение 1:

Открытая экспонента пары ключей RSA.

RSAKeyModulus ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(128))

Присвоение значения: не указано.

2.127 RtmData (данные удаленного мониторинга тахографа)

Поколение 2:

Определение данного типа данных см. в ~~приложении~~ подразделе 14.

2.128 SealDataCard (данные, касающиеся пломб, указанных на карточке)

Поколение 2:

Этот тип данных хранит информацию о пломбах, наложенных на различные компоненты транспортного средства, и предназначен для хранения на соответствующей карточке. Этот тип данных относится к требованию 337 ~~приложения~~ **добавления 1С**.

SealDataCard ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

noOfSealRecords ЦЕЛОЕ ЧИСЛО (1..5)

sealRecords УСТАНОВЛЕННЫЙ РАЗМЕР (noOfSealRecords)
ПАРАМЕТРА SealRecord

}

noOfSealRecords — количество записей в sealRecords.

sealRecords — совокупность записей о пломбах.

2.129 SealDataVu (данные, касающиеся пломб, в БУ)

Поколение 2:

Этот тип данных хранит информацию о пломбах, наложенных на различные компоненты транспортного средства, и предназначен для хранения в бортовом устройстве.

SealDataVu ::= РАЗМЕР ПОСЛЕДОВАТЕЛЬНОСТИ (5) ПАРАМЕТРА {

sealRecords Запись, касающаяся пломб

}

sealRecords — массив записей о пломбах. Если число пломб менее 5, значение EquipmentType во всех неиспользуемых позициях sealRecords устанавливается на 156, т. е. не используется.

2.130 SealRecord (запись, касающаяся пломб)

Поколение 2:

Данный тип данных хранит информацию о пломбе, наложенной на соответствующий компонент. Этот тип данных связан с требованием 337 приложения добавления 1С.

```
SealRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
EquipmentType          Тип оборудования
ExtendedSealIdentifier  Расширенный идентификатор пломбы
}
```

equipmentType идентифицирует тип оборудования, на которое наложена пломба.

extendedSealIdentifier — идентификатор пломбы, наложенной на оборудование.

2.131 SensorApprovalNumber (номер официального утверждения датчика)

Номер официального утверждения типа датчика.

Поколение 1:

```
SensorApprovalNumber ::= СтрокаIA5(РАЗМЕР(8))
```

Присвоение значения: не указано.

Поколение 2:

```
SensorApprovalNumber ::= СтрокаIA5(РАЗМЕР(16))
```

Присвоение значения:

Номер официального утверждения указывается в том виде, в каком он опубликован на соответствующем веб-сайте Европейской комиссии, т. е. на веб-сайте лаборатории, уполномоченной проводить испытания на эксплуатационную совместимость, т. е., например, включая дефисы, если таковые имеются. Номер официального утверждения смещен влево.

2.132 SensorExternalGNSSApprovalNumber (номер официального утверждения внешнего датчика ГНСС)

Поколение 2:

Номер официального утверждения типа внешнего устройства ГНСС.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Присвоение значения:

Номер официального утверждения указывается в том виде, в каком он опубликован на соответствующем веб-сайте Европейской комиссии, т. е. на веб-сайте лаборатории, уполномоченной проводить испытания на эксплуатационную совместимость, т. е., например, включая дефисы, если таковые имеются. Номер официального утверждения смещен влево.

2.133 **SensorExternalGNSSCoupledRecord** (запись о соединении внешнего датчика ГНСС)

Поколение 2:

Информация, записанная в бортовом устройстве, которая относится к идентификации внешнего устройства ГНСС, соединенного с бортовым устройством (~~приложение~~ **добавление 1С**, требование 100).

SensorExternalGNSSCoupledRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

sensorSerialNumber	Серийный номер датчика ГНСС
sensorApprovalNumber	Номер официального утверждения датчика ГНСС
sensorCouplingDate	Дата подсоединения к датчику ГНСС

}

sensorSerialNumber — серийный номер датчика ГНСС, соединенного с бортовым устройством.

sensorApprovalNumber — номер официального утверждения датчика ГНСС.

sensorCouplingDate — дата соединения датчика ГНСС с бортовым устройством.

2.134 **SensorExternalGNSSIdentification** (идентификационные данные внешнего датчика ГНСС)

Поколение 2:

Информация, связанная с идентификацией внешнего устройства ГНСС (~~приложение~~ **добавление 1С**, требование 98).

SensorExternalGNSSIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

sensorSerialNumber	Серийный номер датчика ГНСС
sensorApprovalNumber	Номер официального утверждения внешнего датчика GNSS
sensorSCIdentifier	Идентификатор КЗ внешнего датчика ГНСС
sensorOSIdentifier	Идентификатор ОС внешнего датчика ГНСС

}

sensorSerialNumber — расширенный серийный номер внешнего устройства ГНСС.

sensorApprovalNumber — номер официального утверждения внешнего устройства ГНСС.

sensorSCIdentifier — идентификатор компонента защиты внешнего устройства ГНСС.

sensorOSIdentifier — идентификатор операционной системы внешнего устройства ГНСС.

2.135 **SensorExternalGNSSInstallation** (данные, касающиеся установки внешнего датчика ГНСС)

Поколение 2:

Информация, хранящаяся на внешнем устройстве ГНСС, которая относится к установке внешнего датчика ГНСС (~~приложение~~ **добавление 1С**, требование 123).

SensorExternalGNSSInstallation ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

sensorCouplingDateFirst	SensorGNSSCouplingDate
-------------------------	------------------------

<code>firstVuApprovalNumber</code>	Номер официального утверждения первого БУ
<code>firstVuSerialNumber</code>	Серийный номер первого БУ
<code>sensorCouplingDateCurrent</code>	Дата подсоединения с данным датчиком ГНСС
<code>currentVuApprovalNumber</code>	Номер официального утверждения БУ
<code>currentVUSerialNumber</code>	Серийный номер данного БУ
}	

sensorCouplingDateFirst — дата первого соединения внешнего устройства ГНСС с бортовым устройством.

firstVuApprovalNumber — номер официального утверждения первого бортового устройства, соединенного с внешним устройством ГНСС.

firstVuSerialNumber — серийный номер официального утверждения первого бортового устройства, соединенного с внешним устройством ГНСС.

sensorCouplingDateCurrent — дата соединения внешнего устройства ГНСС с бортовым устройством.

currentVuApprovalNumber — номер официального утверждения бортового устройства, соединенного в данный момент с внешним устройством ГНСС.

currentVUSerialNumber — серийный номер бортового устройства транспортного средства, соединенного в данный момент с внешним устройством ГНСС.

2.136 **SensorExternalGNSSOSIdentifier (идентификатор внешнего датчика ОС ГНСС)**

Поколение 2:

Идентификатор операционной системы внешнего устройства ГНСС.

`SensorOSIdentifier ::= СтрокаIA5(РАЗМЕР(2))`

Присвоение значения: по усмотрению изготовителя.

2.137 **SensorExternalGNSSSCIIdentifier (идентификатор внешнего датчика КЗ ГНСС)**

Поколение 2:

Данный тип используется, например, для идентификации криптографического модуля внешнего устройства ГНСС.

Идентификатор компонента безопасности внешнего устройства ГНСС.

`SensorExternalGNSSSCIIdentifier ::= СтрокаIA5(РАЗМЕР(8))`

Присвоение значения: по усмотрению изготовителя компонента.

2.138 **SensorGNSSCouplingDate (дата соединения датчика ГНСС с БУ)**

Поколение 2:

Дата соединения внешнего устройства ГНСС с бортовым устройством.

`SensorGNSSCouplingDate ::= Реальное время`

Присвоение значения: не указано.

2.139 SensorGNSSSerialNumber (серийный номер датчика ГНСС)

Поколение 2:

Данный тип используется для хранения серийного номера приемника ГНСС, как в том случае, когда он встроен в БУ, так и в том случае, когда он установлен вне него.

Серийный номер приемника ГНСС.

SensorGNSSSerialNumber ::= Расширенный серийный номер

2.140 SensorIdentification (идентификация датчика)

Информация, записанная в датчике движения, которая относится к идентификации датчика движения (~~приложение~~ **добавление 1B**, требование 077 и ~~приложение~~ **добавление 1C**, требование 95).

SensorIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

sensorSerialNumber	Серийный номер датчика
sensorApprovalNumber	Номер официального утверждения датчика
sensorSCIdentifier	Идентификатор КЗ датчика
sensorOSIdentifier	Идентификатор ОС датчика

}

sensorSerialNumber — расширенный серийный номер датчика движения (включая номер детали и код изготовителя).

sensorApprovalNumber — номер официального утверждения датчика движения.

sensorSCIdentifier — идентификатор компоненты защиты датчика движения.

sensorOSIdentifier — идентификатор операционной системы датчика движения.

2.141 SensorInstallation (установка датчика)

Информация, записанная в датчике движения, которая относится к установке датчика движения (~~приложение~~ **добавление 1B**, требование 099 и ~~приложение~~ **добавление 1C**, требование 122).

SensorExternalGNSSIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

sensorPairingDateFirst	Дата соединения с датчиком
firstVuApprovalNumber	Номер официального утверждения первого БУ
firstVuSerialNumber	Серийный номер первого БУ
sensorPairingDateCurrent	Дата соединения с датчиком
currentVuApprovalNumber	Номер официального утверждения данного БУ
currentVUSerialNumber	Серийный номер данного БУ

}

sensorPairingDateFirst — дата первого соединения датчика движения с бортовым устройством.

firstVuApprovalNumber — номер официального утверждения первого бортового устройства, соединенного с датчиком движения.

firstVuSerialNumber — серийный номер первого бортового устройства, соединенного с датчиком движения.

sensorPairingDateCurrent — дата текущего соединения датчика движения с бортовым устройством.

currentVuApprovalNumber — номер официального утверждения бортового устройства, соединенного в данный момент с датчиком движения.

currentVUSerialNumber — серийный номер бортового устройства, соединенного в данный момент с датчиком движения.

2.142 **SensorInstallationSecData (данные, касающиеся защиты при установке датчика)**

Информация, записанная на карточке мастерской, которая имеет отношение к данным о защите, необходимым для подсоединения датчиков движения к бортовым устройствам (~~приложение~~ **добавление 1С**, требования 308 и 331).

Поколение 1:

SensorInstallationSecData ::= TDesSessionKey

Присвоение значения: в соответствии с ISO 16844-3.

Поколение 2:

Как описано в ~~приложении~~ **подразделе 11**, на карточке мастерской хранится до трех ключей в целях соединения БУ и датчика движения. Эти ключи относятся к разным версиям.

SensorExternalGNSSIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

kMWCKey1	kMWCKey
kMWCKey2	КМWCKey, ФАКУЛЬТАТИВНО
kMWCKey3	КМWCKey, ФАКУЛЬТАТИВНО

}

2.143 **SensorOSIdentifier (идентификатор ОС датчика)**

SensorOSIdentifier — Идентификатор операционной системы датчика движения.

SensorOSIdentifier ::= СтрокаIA5(РАЗМЕР(2))

Присвоение значения: по усмотрению изготовителя.

2.144 **SensorPaired (подсоединенный датчик)**

Поколение 1:

Информация, записанная в бортовом устройстве, которая относится к идентификации датчика движения, соединенного с бортовым устройством (~~приложение~~ **добавление 1В**, требование 079).

SensorPaired ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

SensorSerialNumber	Серийный номер датчика
sensorApprovalNumber	Номер официального утверждения датчика
sensorPairingDateFirst	Дата первого подсоединения датчика

}

sensorSerialNumber — серийный номер датчика движения, соединенного в данный момент с бортовым устройством.

sensorApprovalNumber — номер официального утверждения датчика движения, соединенного в данный момент с бортовым устройством.

sensorPairingDateFirst — дата первого соединения с бортовым устройством датчика движения, который в данный момент соединен с данным бортовым устройством.

2.145 **SensorPairedRecord (запись данных о подсоединении датчика)**

Поколение 2:

Информация, записанная в бортовом устройстве, которая относится к идентификации датчика движения, соединенного с бортовым устройством (~~приложение~~ **добавление** 1С, требование 97).

SensorPaired ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

sensorSerialNumber Серийный номер датчика

sensorApprovalNumber Номер официального утверждения датчика

SensorPairingDate Дата подсоединения датчика

}

sensorSerialNumber — серийный номер датчика движения, соединенного с бортовым устройством.

sensorApprovalNumber — номер официального утверждения этого датчика движения.

sensorPairingDate — дата первого соединения датчика движения с бортовым устройством.

2.146 **SensorPairingDate (дата подсоединения датчика)**

Дата первого соединения датчика движения с бортовым устройством.

SensorPairingDate ::= Реальное время

Присвоение значения: не указано.

2.147 **SensorSCIdentifier (идентификатор КЗ датчика)**

Идентификатор компонента безопасности датчика движения.

SensorExternalGNSSSCIdentifier ::= СтрокаIA5(РАЗМЕР(8))

Присвоение значения: по усмотрению изготовителя конкретного компонента.

2.148 **SensorSerialNumber (серийный номер датчика)**

Серийный номер датчика движения.

SensorSerialNumber ::= Расширенный серийный номер

2.149 **Signature (подпись)**

Цифровая подпись.

Поколение 1:

Подпись ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(128))

Присвоение значения: в соответствии с ~~приложением~~ **подразделом** 11 добавления «Общие механизмы безопасности».

Поколение 2:

Подпись ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(128))

Присвоение значения: в соответствии с ~~приложением~~ подразделом 11 добавления «Общие механизмы безопасности».

2.150 SignatureRecordArray (набор подписей и метаданные)

Поколение 2:

Набор подписей и метаданные, используемые в протоколе загрузки.

SignatureRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType RecordType,
recordSize ЦЕЛОЕ ЧИСЛО(1..65535),
noOfRecords ЦЕЛОЕ ЧИСЛО(0..65535),
records УСТАНОВЛЕНИЕ РАЗМЕРА (noOfRecords) ПАРАМЕТРА подписи
}

recordType указывает на тип записи (подпись).

Присвоение значения: см. RecordType.

recordSize — размер подписи в байтах.

noOfRecords — число записей в совокупности данных. Значение устанавливается на 1, так как подписи могут быть разной длины.

records — набор подписей.

2.151 SimilarEventsNumber (число похожих событий)

Число похожих событий в течение одного конкретного дня (~~приложение добавление 1B~~, требование 094, и ~~приложение добавление 1C~~, требование 117).

SimilarEventsNumber ::= ЦЕЛОЕ ЧИСЛО(0..255)

Присвоение значения: 0 не используется, 1 означает, что в данный день имело место и было зарегистрировано только одно событие этого типа, 2 означает, что в этот день имели место 2 события (из которых было сохранено только одно), ...255 означает, что в данный день произошло 255 или более событий этого типа.

2.152 SpecificConditionRecord (запись особых условий)

Информация, записанная на карточке водителя или мастерской или в бортовом устройстве, которая имеет отношение к соответствующему особому условию (~~приложение добавление 1C~~, требования 130, 276, 301, 328 и 355).

SpecificConditionRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

entryTime Реальное время
specificConditionType Тип особого условия
}

entryTime — дата и время ввода данных.

specificConditionType — код, позволяющий идентифицировать особое условие.

2.153 SpecificConditions (особые условия)

Информация, записанная на карточке водителя или мастерской или в бортовом устройстве, которая имеет отношение к соответствующему особому условию (~~приложение~~ **добавление 1С**, требования 131, 277, 302, 329 и 356).

Поколение 2:

```
SpecificConditionRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
conditionPointerNewestRecord ЦЕЛОЕ ЧИСЛО (0..NoOfSpecificConditionRecords-1)
specificConditionRecords УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfSpecificConditionRecords)
ПАРАМЕТРА SpecificConditionRecord
}
```

conditionPointerNewestRecord — индекс последней обновленной записи об особых условиях.

Присвоение значения: число, соответствующее числовому показателю записи данных об особых условиях, которое начинается с 0 в случае первой регистрации записей, касающихся особых условий, в структуре данных.

specificConditionRecords — совокупность записей, содержащих информацию об зафиксированных особых условиях.

2.154 SpecificConditionType (тип особых условий)

Код, позволяющий идентифицировать соответствующее особое условие (~~приложение~~ **добавление 1В**, требования 050b, 105a, 212a и 230a, и ~~приложение~~ **добавление 1С**, требования ~~требование~~ **требование 62**).

SpecificConditionType ::= ЦЕЛОЕ ЧИСЛО(0..255)

Поколение 1:

Присвоение значения:

'00'Н	RFU
'01'Н	Неприменимо — начало
'02'Н	Неприменимо — конец
'03'Н	Паром/ж-д переезд
'0'Н .. 'FF'Н	RFU

Поколение 2:

Присвоение значения:

'00'Н	RFU
'01'Н	Неприменимо — начало
'02'Н	Неприменимо — конец
'03'Н	Паром/ж-д переезд — начало
'04'Н	Паром/ж-д переезд — конец
'05'Н 'FF'Н	RFU

2.155 Speed (скорость)

Скорость транспортного средства (км/ч).

Speed ::= ЦЕЛОЕ ЧИСЛО(0..255)

Присвоение значения: километры в час в рабочем диапазоне от 0 до 220 км/ч.

2.156 SpeedAuthorised (разрешенная скорость)

Максимальная разрешенная скорость транспортного средства (определение hh).

SpeedAuthorised ::= Скорость

2.157 SpeedAverage (средняя скорость)

Средняя скорость за предварительно определенный промежуток времени (км/ч).

SpeedAuthorised ::= Скорость

2.158 SpeedMax (максимальная скорость)

Максимальная скорость, измеренная за предварительно определенный промежуток времени.

SpeedMax ::= Скорость

2.158a TachographCardsGen1Suppression (отмена карточек тахографа первого поколения)

Поколение 2, версия 2:

Способность БУ второго поколения использовать карточки водителя, контролера и предприятия первого поколения (см. подраздел 15 добавления, MIG_002).

TachographCardsGen1Suppression ::= ЦЕЛОЕ ЧИСЛО (0..2¹⁶-1)

Присвоение значения:

‘0000’H БУ может использовать карточки тахографа поколения 1 (значение по умолчанию)

‘A5E3’H БУ не может использовать карточки тахографа поколения 1

Все остальные значения Не используются.

2.159 TachographPayload (пакет данных тахографа)

Поколение 2:

Определение данного типа данных см. в ~~приложении~~ подразделе 14.

2.160 Reserved for future use (зарезервировано для использования в будущем)

~~TachographPayloadEncrypted~~

~~Поколение 2~~

~~Зашифрованные данные тахографа DER TLV, т. е. данные, передаваемые в зашифрованном виде сообщением RTM. По вопросу шифрования см. приложение 11, часть Б, глава 13.~~

~~TachographPayloadEncrypted ::= SEQUENCE {~~

~~ОКТЕТНАЯ СТРОКА(РАЗМЕР(1)),~~

~~Длина ОКТЕТНАЯ СТРОКА (РАЗМЕР 1.2.160 Зарезервировано для будущего использования 2)~~

~~paddingContentIndicatorByte~~ — ОКТЕТНАЯ СТРОКА(РАЗМЕР(1));

~~encryptedData~~ — ОКТЕТНАЯ СТРОКА(РАЗМЕР(16,192));

~~tag~~ — часть кодирования DER-TLV, которая устанавливается как '87' (см. приложение 11, часть Б, глава 13).

~~length~~ — часть кодирования DER-TLV, кодирующая длину следующих позиций ~~paddingContentIndicatorByte~~ и ~~encryptedData~~. — байт с указанием содержимого и зашифрованные данные (~~encryptedData~~)

~~paddingContentIndicatorByte~~ устанавливается на '00'.

~~encryptedData~~ — это зашифрованная позиция ~~tachographPayload~~, как указано в приложении 11, часть Б, глава 13. Длина Октетная длина данного элемента данных всегда кратна 16.

2.161 TDesSessionKey (тройной ключ сеанса в системе TDes)

Поколение 1:

Тройной ключ сеанса в системе DES.

```
TDesSessionKey ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
tDesKeyA      ОКТЕТНАЯ СТРОКА (РАЗМЕР(8))
tDesKeyB      ОКТЕТНАЯ СТРОКА (РАЗМЕР(8))
}
```

Присвоение значения: дополнительно не указывается.

2.162 TimeReal (реальное время)

Код для комбинированного поля даты и времени, в котором дата и время выражены в виде секунд, прошедших с 00ч.00м.00с. на 1 января 1970 года по Гринвичу UTC.

```
TimeReal{INTEGER:TimeRealRange} ::= ЦЕЛОЕ ЧИСЛО(0..TimeRealRange)
```

Присвоение значения — **выровненный октет:** количество секунд с полуночи 1 января 1970 года GMT UTC.

Максимально возможное отображение даты/времени — 2106 год.

2.163 TyreSize (размер шин)

Обозначение размера шин.

```
TyreSize ::= IA5String(SIZE(15))
```

Присвоение значения: в соответствии с Директивой 92/23 (ЕЭС) от 31/03/1992, ОЖЛ 129, р. 95 Правилами ЕЭК ООН № 54.

2.164 VehicleIdentificationNumber (идентификационный номер транспортного средства)

Идентификационный номер транспортного средства (VIN), указывающий на транспортное средство в целом; обычно это серийный номер шасси или номер рамы.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Присвоение значения: как описано в ISO 3779.

2.165 VehicleIdentificationNumberRecordArray (идентификационный номер транспортного средства и метаданные)

Поколение 2:

Идентификационный номер транспортного средства и метаданные, используемые в протоколе загрузки.

```
VehicleIdentificationNumberRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType                Тип записи
recordSize                ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords              ЦЕЛОЕ ЧИСЛО(0..65535)
records                  УСТАНОВЛЕННЫЙ РАЗМЕР(noOfRecords)
                        записи VehicleIdentificationNumber
}
```

recordType обозначает тип записи (VehicleIdentificationNumber).

Присвоение значения: см. RecordType.

recordSize — размер записи VehicleIdentificationNumber в байтах.

noOfRecords — количество записей в предусмотренном наборе записей.

records — набор идентификационных номеров транспортных средств.

2.166 VehicleRegistrationIdentification (идентификация регистрации транспортного средства)

Идентификация транспортного средства, уникальная для Европы (VRN и государство-член Договаривающаяся сторона).

```
VehicleRegistrationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
vehicleRegistrationNation Числовой код страны
vehicleRegistrationNumber Регистрационный номер транспортного средства
}
```

vehicleRegistrationNation — страна, в которой зарегистрировано транспортное средство.

vehicleRegistrationNumber — регистрационный номер транспортного средства (VRN).

2.166a VehicleRegistrationIdentificationRecordArray (идентификация регистрации транспортного средства и метаданные)

Поколение 2, версия 2:

Идентификация регистрации транспортного средства плюс метаданные в том виде, в котором они используются в протоколе загрузки).

```
VehicleRegistrationIdentificationRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType                Тип записи
recordSize                ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords              ЦЕЛОЕ ЧИСЛО(0..65535)
records                  УСТАНОВЛЕННЫЙ РАЗМЕР(noOfRecords)
                        ПАРАМЕТРА VehicleRegistrationIdentification
}
```

recordType обозначает тип записи (**VehicleRegistrationIdentification**).

Присвоение значения: см. **RecordType**.

recordSize — размер позиции **VehicleRegistrationIdentification** в байтах.

noOfRecords — число записей в предусмотренном наборе записей.

records — набор знаков идентификации регистрации данного транспортного средства.

2.167 **VehicleRegistrationNumber** (регистрационный номер транспортного средства)

Регистрационный номер транспортного средства (VRN). Номер регистрации присваивается компетентным органом, регистрирующим транспортное средство.

```
VehicleRegistrationIdentificationRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
codePage          ЦЕЛОЕ ЧИСЛО (0..255)
vehicleRegNumber  ОКТЕТНАЯ СТРОКА (РАЗМЕР(13))
}
```

codePage уточняет набор символов, определенный в главе 4.

vehicleRegNumber — VRN, закодированный с помощью указанного набора символов.

Присвоение значения: по усмотрению конкретной страны.

2.168 **VehicleRegistrationNumberRecordArray** (регистрационный номер транспортного средства и метаданные)

Поколение 2, версия 1:

Идентификационный номер транспортного средства плюс метаданные, используемые в протоколе загрузки.

```
VehicleRegistrationNumberRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType        Тип записи
recordSize        ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords       ЦЕЛОЕ ЧИСЛО(0..65535)
records           УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
                  ПАРАМЕТРА VehicleRegistrationNumber
}
```

recordType обозначает тип записи (**VehicleRegistrationNumber**).

Присвоение значения: см. **RecordType**.

recordSize — размер записи **VehicleRegistrationNumber** в байтах.

noOfRecords — число записей в предусмотренном наборе записей.

records — набор регистрационных номеров транспортных средств.

2.169 **VuAbility** (характеристики БУ)

Поколение 2:

Информация, хранящаяся в БУ о способности или неспособности БУ использовать карточки тахографов первого поколения (~~приложение~~ **добавление 1С**, требование 121).

```
VuAbility ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))
```

Присвоение значения — выровненный октет: 'xxxxxxa'В (8 битов)

Применительно к способности поддержки первого поколения:

'a'В	Способность поддерживать карточки тахографов первого поколения:
'0' В	Поколение 1 поддерживается
'1' В	Поколение 1 не поддерживается
'xxxxxx'В	RFU

2.170 VuActivityDailyData (данные в БУ о деятельности за данный день)

Поколение 1:

Информация, записанная в БУ, которая имеет отношение к изменению вида деятельности и/или изменению статуса управления и/или изменению статуса карточки за данный календарный день (~~приложение~~ **добавление 1В**, требование 084, и ~~приложение~~ **добавление 1С**, требования 105, 106 и 107) и к статусу считывающих устройств на 00:00 часов в указанный день.

```
VuActivityDailyData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
noOfActivityChanges          ЦЕЛОЕ ЧИСЛО(0..1440)
activityChangeInfos          УСТАНОВЛЕННЫЙ РАЗМЕР(noOfActivityChanges)
                             ПАРАМЕТРА ActivityChangeInfo
}
```

noOfActivityChanges — число слов параметра ActivityChangeInfo в совокупности данных activityChangeInfos.

activityChangeInfos — совокупность слов параметра ActivityChangeInfo, записанных в БУ за данный день. Она всегда включает в себя два слова ActivityChangeInfo, указывающих на состояние двух считывающих устройств в 00:00 часов в указанный день.

2.171 VuActivityDailyRecordArray (записи в БУ о деятельности или статусе и метаданные)

Поколение 2:

Информация, записанная в БУ, которая имеет отношение к изменению вида деятельности и/или изменению статуса управления и/или изменению статуса карточки за данный календарный день (~~приложение~~ **добавление 1С**, требования 105, 106 и 107) и к статусу считывающих устройств на 00:00 часов в указанный день.

```
VuActivityDailyRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType                   Тип записи
recordSize                   ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords                  ЦЕЛОЕ ЧИСЛО(0..65535)
records                      УСТАНОВЛЕННЫЙ РАЗМЕР (noOfActivityChanges)
                             ПАРАМЕТРА ActivityChangeInfo
}
```

recordType обозначает тип записи (ActivityChangeInfo).

Присвоение значения: см. RecordType.

recordSize — размер параметра ActivityChangeInfo в байтах.

noOfRecords — число записей в совокупности записей.

records — набор слов ActivityChangeInfo, хранящихся в БУ за день. Он всегда включает в себя два слова ActivityChangeInfo, указывающих на статус двух считывающих устройств в 00:00 часов в указанный день.

2.172 VuApprovalNumber (номер официального утверждения БУ)

Номер официального утверждения типа бортового устройства.

Поколение 1:

VuApprovalNumber ::= СтрокаIA5(РАЗМЕР(8))

Присвоение значения: не указано.

Поколение 2:

VuApprovalNumber ::= СтрокаIA5(РАЗМЕР(16))

Присвоение значения:

Номер официального утверждения указывается в том виде, в каком он опубликован на ~~соответствующем веб-сайте Европейской комиссии, т. е. на веб-сайте лаборатории,~~ **уполномоченной проводить испытания на эксплуатационную совместимость, т. е.,** например, включая дефисы, если таковые имеются. Номер официального утверждения смещен влево.

2.173 VuCalibrationData (данные в БУ о калибровке)

Поколение 1:

Информация, записанная в бортовом устройстве, которая относится к калибровке ~~записывающего оборудования~~ **контрольного устройства (приложение добавление 1В,** требование 098).

```
VuCalibrationData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
noOfVuCalibrationRecords    ЦЕЛОЕ ЧИСЛО(0..255)
vuCalibrationRecords        УСТАНОВЛЕННЫЙ РАЗМЕР (noOfVuCalibrationRecords)
                             ПАРАМЕТРА VuCalibrationRecord
}
```

noOfVuCalibrationRecords — число записей, содержащихся в совокупности записей vuCalibrationRecords.

vuCalibrationRecords — совокупность записей калибровки.

2.174 VuCalibrationRecord (запись в БУ о калибровке)

Информация, записанная в бортовом устройстве, которая относится к калибровке ~~записывающего оборудования~~ **контрольного устройства (приложение добавление 1В,** требование 098, и ~~приложение добавление 1С, требования 119 и 120).~~

Поколение 1:

```
VuCalibrationData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
calibrationPurpose          Цель калибровки
workshopName                Название
workshopAddress             Адрес
workshopCardNumber          Полный номер карточки
workshopCardExpiryDate     Реальное время
```


vehicleIdentificationNumber	Номер идентификации транспортного средства
vehicleRegistrationIdentification	Идентификация регистрации транспортного средства
wVehicleCharacteristicConstant	Характеристическая константа W транспортного средства
kConstantOfRecordingEquipment	Константа K контрольного устройства
lTyreCircumference	Окружность шины L
tyreSize	Размер шины
authorisedSpeed	Разрешенная скорость
oldOdometerValue	Прежние показания счетчика пробега
newOdometerValue	Новые показания счетчика пробега
oldTimeValue	Реальное время
newTimeValue	Реальное время
nextCalibrationDate	Реальное время
}	

calibrationPurpose — цель калибровки.

workshopName, workshopAddress — название и адрес мастерской.

workshopCardNumber — идентификатор карточки мастерской, используемой во время калибровки.

workshopCardExpiryDate — дата истечения срока действия карточки.

vehicleIdentificationNumber — идентификационный номер транспортного средства (VIN).

vehicleRegistrationIdentification — VRN и государство-член Договаривающаяся сторона регистрации транспортного средства.

wVehicleCharacteristicConstant — характеристический коэффициент транспортного средства.

kConstantOfRecordingEquipment — постоянная величина k записывающего оборудования контрольного устройства.

lTyreCircumference — фактическая окружность шин колес.

tyreSize — обозначение габаритов шин, установленных на транспортном средстве.

authorisedSpeed — допустимая скорость транспортного средства.

oldOdometerValue, newOdometerValue — старые и новые показания счетчика пробега.

oldTimeValue, newTimeValue — старые и новые значения даты и времени.

nextCalibrationDate — дата следующей калибровки типа, указанного в параметре **CalibrationPurpose**, которую должен провести уполномоченный инспекционный орган.

Поколение 2, версия 1:

VuCalibrationData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

calibrationPurpose	Цель калибровки
workshopName	Название
workshopAddress	Адрес
workshopCardNumber	Полный номер карточки

workshopCardExpiryDate	Реальное время
vehicleIdentificationNumber	Идентификационный номер транспортного средства
vehicleRegistrationIdentification	Идентификация регистрации транспортного средства
wVehicleCharacteristicConstant	Характеристическая константа W транспортного средства
kConstantOfRecordingEquipment	Константа K контрольного устройства
lTyreCircumference	Окружность шины L
TyreSize	Размер шины
authorisedSpeed	Разрешенная скорость
oldOdometerValue	Новые показания счетчика пробега
newOdometerValue	Старые показания счетчика пробега
oldTimeValue	Реальное время
newTimeValue	Реальное время
nextCalibrationDate	Реальное время
sealDataVu	Данные, касающиеся пломб, в БУ
}	

В дополнение к поколению 1, используется следующий элемент данных:

SealDataVu содержит информацию о пломбах, наложенных на различные компоненты транспортного средства.

Поколение 2, версия 2:

VuCalibrationData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

calibrationPurpose	Цель калибровки
workshopName	Название
workshopAddress	Адрес
workshopCardNumber	Полный номер карточки мастерской
workshopCardExpiryDate	Реальное время
vehicleIdentificationNumber	Номер идентификации транспортного средства
vehicleRegistrationIdentification	Идентификация регистрации транспортного средства
wVehicleCharacteristicConstant,	Характеристическая константа W транспортного средства
kConstantOfRecordingEquipment	Константа K контрольного устройства
lTyreCircumference	Окружность шины L
tyreSize	Размер шины
authorisedSpeed	Разрешенная скорость
oldOdometerValue	Показания счетчика пробега
newOdometerValue	Показания счетчика пробега
oldTimeValue	Реальное время
newTimeValue	Реальное время

nextCalibrationDate	Реальное время
sensorSerialNumber	Серийный номер датчика
sensorGNSSSerialNumber	Серийный номер датчика ГНСС
rsmSerialNumber	Серийный номер удаленного модуля связи
sealDataVu	Данные, касающиеся пломб, в БУ
byDefaultLoadType	Тип загрузки
calibrationCountry	Числовой код страны
calibrationCountryTimestamp	Реальное время
}	

В дополнение к поколению 1 используется следующий элемент данных:

sensorSerialNumber — серийный номер датчика движения, соединенного с бортовым устройством в конце калибровки,

sensorGNSSSerialNumber — серийный номер внешнего устройства ГНСС, соединенного с бортовым устройством (в случае наличия).

rsmGNSSSerialNumber — серийный номер внешнего устройства удаленной связи ГНСС, соединенного с бортовым устройством в конце калибровки (в случае наличия).

sealDataVu содержит информацию о пломбах, наложенных на различные компоненты транспортного средства.

byDefaultLoadType — тип груза по умолчанию для транспортного средства (присутствует только в случае версии 2).

calibrationCountry — страна, в которой была выполнена калибровка.

calibrationCountryTimestamp — дата и время выдачи приемником ГНСС местоположения, использованного для определения страны, в которой была выполнена калибровка.

2.175 VuCalibrationRecordArray (данные в БУ о калибровке и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, которая относится к калибровке записывающего оборудования контрольного устройства (приложение добавление 1С, требования 119 и 120).

VuCalibrationData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType	Тип записи
recordSize	ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords	ЦЕЛОЕ ЧИСЛО(0..65535)
records	УСТАНОВЛЕННЫЙ РАЗМЕР(noOfVuCalibrationRecords) ПАРАМЕТРА VuCalibrationRecord
}	

recordType обозначает тип записи (VuCalibrationRecord).

Присвоение значения: см. RecordType.

recordSize — размер записи VuCalibrationRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей калибровки.

2.176 VuCardIWData (данные в БУ о циклах ввода и извлечения карточек)

Поколение 1:

Информация, записанная в бортовом устройстве, которая относится к циклам ввода карточек водителя или карточек мастерской в бортовое устройство и их извлечения (~~приложение добавление 1В~~, требование 081, и ~~приложение добавление 1С~~, требование 103).

```
VuCalibrationData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
noOfIWRecords          ЦЕЛОЕ ЧИСЛО(0..216-1),
vuCardIWRecords       УСТАНОВЛЕННЫЙ РАЗМЕР(noOfVuCalibrationRecords)
                       ПАРАМЕТРА VuCalibrationRecord
}
```

noOfIWRecords — количество записей в наборе vuCardIWRecords.

vuCardIWRecords — совокупность записей, относящихся к циклам ввода и извлечения карточек.

2.177 VuCardIWRecord (запись данных в БУ о циклах ввода и извлечения карточек)

Информация, записанная в бортовом устройстве, которая имеет отношение к циклу ввода карточки водителя или карточки мастерской в бортовое устройство и их извлечения (~~приложение добавление 1В~~, требование 081, и ~~приложение добавление 1С~~, требование 102).

Поколение 1:

```
VuCalibrationData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
cardHolderName         Название держателя
fullCardNumber         Полный номер карточки
cardExpiryDate         Реальное время
cardInsertionTime      Реальное время
vehicleOdometerValueAtInsertion Показания счетчика пробега
cardSlotNumber         Номер считывающего устройства карточки
cardWithdrawalTime     Реальное время
vehicleOdometerValueAtWithdrawal Показания счетчика пробега
PreviousVehicleInfo    Предыдущая информация о транспортном
                       средстве
manualInputFlag        Метка ручного ввода
}
```

cardHolderName — фамилия и имя (имена) держателя карточки водителя или мастерской, записанные на карточке.

fullCardNumber — тип карточки, ~~выдавшее ее государство-член~~ **выдавшая ее Договаривающаяся сторона** и ее номер, хранящийся на карточке.

cardExpiryDate — дата истечения срока действия карточки, хранящаяся на карточке.

cardInsertionTime — дата и время ввода.

vehicleOdometerValueAtInsertion — показание счетчика пробега транспортного средства в момент ввода карточки.

cardSlotNumber — считывающее устройство, в которое вставляется карточка.

cardWithdrawalTime — дата и время извлечения карточки.

vehicleOdometerValueAtWithdrawal — показание счетчика пробега транспортного средства в момент извлечения карточки.

previousVehicleInfo — информация о предыдущем транспортном средстве, которым пользовался водитель, записанная на карточке.

manualInputFlag — метка, позволяющая определить, ввел ли держатель карточки данные о деятельности водителя вручную в момент ее ввода.

Поколение 2:

VuCardIWRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

cardHolderName	Название держателя
fullCardNumberAndGeneration	Полный номер и поколение карточки
cardExpiryDate	Реальное время
cardInsertionTime	Реальное время
vehicleOdometerValueAtInsertion	Показания счетчика пробега
cardSlotNumber	Номер считывающего устройства карточки
cardWithdrawalTime	Реальное время
vehicleOdometerValueAtWithdrawal	Показания счетчика пробега
previousVehicleInfo	Предыдущая информация о транспортном средстве
manualInputFlag	Метка, указывающая на ручной ввод данных

}

Вместо fullCardNumber в структуре данных второго поколения используется следующий элемент данных.

fullCardNumberAndGeneration — тип карточки, ~~выдавшее ее~~ государство-член выдавшая ее **Договаривающаяся сторона** и ее номер, хранящийся на карточке.

2.178 VuCardIWRecordArray (данные о циклах ввода и извлечения карточек и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, которая относится к циклам ввода карточек водителя или карточек мастерской в бортовое устройство и их извлечения (~~приложение~~ **добавление 1С, требование 103**).

VuCardIWRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType	Тип записи
recordSize	ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords	ЦЕЛОЕ ЧИСЛО(0..65535)
records	УСТАНОВЛЕННЫЙ РАЗМЕР(noOfRecords) ПАРАМЕТРА VuCardIWRecord

}

recordType обозначает тип записи (VuCalibrationRecord).

Присвоение значения: см. RecordType.

recordSize — размер записи VuCalibrationRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей, относящихся к циклам ввода и извлечения карточек.

2.179 VuCardRecord (запись данных в БУ об используемой карточке)

Поколение 2:

Информация, записанная в бортовом устройстве, применительно к используемой карточке тахографа (~~приложение добавление 1С~~, требование 132).

VuCardRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

CardNumberAndGenerationInformation Полный номер карточки и ее поколение

cardExtendedSerialNumber Расширенный серийный номер

~~cardPersonaliserID ОКТЕТНАЯ СТРОКА(РАЗМЕР(1))~~

~~typeOfTachographCardId EquipmentType (тип оборудования)~~

cardStcureVersion Версия структуры карточки

cardNumber Номер карточки

}

cardNumberAndGenerationInformation — полный номер карточки и поколение используемой карточки (тип данных 2.74).

cardExtendedSerialNumber в том виде, как она считывается из файла EF_ICC в MF карточки.

~~**cardPersonaliserID** в том виде, как считывается из файла EF_ICC в MF карточки.~~

~~**typeOfTachographCardId** в том виде, как считывается из файла EF_Application_Identification в DF_Tachograph_G2.~~

cardStructureVersion в том виде, как она считывается из файла EF_Application_Identification в DF_Tachograph_G2.

cardNumber в том виде, как она считывается из файла EF_Identification в DF_Tachograph_G2.

2.180 VuCardRecordArray (данные об используемых карточках и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, применительно к карточкам тахографа, используемым в данном бортовом устройстве. Эта информация предназначена для анализа проблем сопряжения БУ и карточки (~~приложение добавление 1С~~, требование 132).

VuCardIWRRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType Тип записи

recordSize ЦЕЛОЕ ЧИСЛО(1..65535)

noOfRecords ЦЕЛОЕ ЧИСЛО(0..65535)

records УСТАНОВЛЕННЫЙ РАЗМЕР(noOfRecords)
ПАРАМЕТРА VuCardIWRRecord

}

recordType обозначает тип записи (VuCardRecord).

Присвоение значения: см. RecordType.

recordSize — размер записи VuCardRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей, относящихся к карточкам тахографа, используемым в БУ.

2.181 VuCertificate (сертификат БУ)

Сертификат открытого ключа бортового устройства.

VuCertificate ::= Сертификат

2.182 VuCertificateRecordArray (сертификат БУ и метаданные)

Поколение 2:

Сертификат БУ плюс метаданные, используемые в протоколе загрузки.

VuCertificateRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType Тип записи

recordSize ЦЕЛОЕ ЧИСЛО(1..65535)

noOfRecords ЦЕЛОЕ ЧИСЛО(0..65535)

records УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords) ПАРАМЕТРА VuCertificate

}

recordType обозначает тип записи (VuCertificate).

Присвоение значения: см. RecordType.

recordSize — размер VuCertificate в байтах.

noOfRecords — число записей в совокупности записей. Значение устанавливается на 1, так как сертификаты могут быть разной длины.

records — набор сертификатов БУ.

2.183 VuCompanyLocksData (данные в БУ о блокировке предприятием)

Поколение 1:

Информация, записанная в бортовом устройстве, которая относится к блокировке предприятием (~~приложение добавление 1B~~, требование 104).

VuCompanyLocksData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

noOfLocks ЦЕЛОЕ ЧИСЛО(0..255)

vuCompanyLocksRecords УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
ПАРАМЕТРА VuCardIWRRecord

}

noOfLocks — число блокировок, перечисленных в записях vuCompanyLocksRecords

vuCompanyLocksRecords — совокупность записей по блокировке, произведенной предприятием.

2.184 VuCompanyLocksRecord (запись данных в БУ о блокировке предприятием)

Информация, записанная в бортовом устройстве, применительно к блокировке предприятием (~~приложение добавление~~ 1В, требование 104, и ~~приложение добавление~~ 1С, требование 128).

Поколение 1:

```
VuCompanyLocksRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
lockInTime                Реальное время
lockOutTime               Реальное время
companyName               Название
companyAddress            Адрес
companyCardNumber        Полный номер карточки
}
```

lockInTime, lockOutTime — дата и время блокировки и снятия блокировки.

companyName, companyAddress — название и адрес предприятия, которое произвело блокировку.

companyCardNumber — идентификационные данные карточки, используемой для блокировки.

Поколение 2:

```
VuCompanyLocksRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
lockInTime                Реальное время
lockOutTime               Реальное время
companyName               Название
companyAddress            Адрес
companyCardNumberAndGeneration  Полный номер карточки и поколение
}
```

Вместо `companyCardNumber` в структуре данных второго поколения используется следующий элемент данных.

companyCardNumberAndGeneration идентифицирует карточку, используемую при блокировке, и ее поколение.

2.185 VuCompanyLocksRecordArray (запись данных в БУ о блокировке предприятием и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, которая относится к блокировке предприятием (~~приложение добавление~~ 1С, требование 128).

```
VuCompanyLocksRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType                Тип записи
recordSize                ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords              ЦЕЛОЕ ЧИСЛО(0..65535)
records                  УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
                        ПАРАМЕТРА VuCompanyLocksRecord
}
```


recordType обозначает тип записи (VuCompanyLocksRecord).

Присвоение значения: см. RecordType.

recordSize — размер записи VuCardRecord в байтах.

noOfRecords — число записей в совокупности записей. Значение 0..255.

records — набор записей о блокировке предприятием.

2.185a VuConfigurationLengthRange (длина данных о конфигурации БУ)

Поколение 2, версия 2:

Количество байтов в карточке тахографа, доступных для хранения конфигураций БУ.

VuConfigurationLengthRange ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: см. подраздел 2 добавления

2.186 VuControlActivityData (данные в БУ о контроле за деятельностью)

Поколение 1:

Информация, записанная в бортовом устройстве, которая относится к контрольным действиям с использованием этого БУ (~~приложение добавление 1В~~, требование 102).

VuControlActivityData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

noOfControls ЦЕЛОЕ ЧИСЛО(0..20)

vuControlActivityRecords УСТАНОВЛЕННЫЙ РАЗМЕР (noOfControls)
ПАРАМЕТРА VuControl ActivityRecord

}

noOfControls — число контрольных действий, перечисленных в позиции vuControlActivityRecords.

vuControlActivityRecords — совокупность записей контрольных действий.

2.187 VuControlActivityRecord (запись данных в БУ о контроле за деятельностью)

Информация, записанная в бортовом устройстве, которая относится к контрольным действиям с использованием этого БУ (~~приложение добавление 1В~~, требование 102, и ~~приложение добавление 1С~~, требование 126).

Поколение 1:

VuControlActivityRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

controlType Тип контроля

controlTime Реальное время

controlCardNumber Полный номер карточки

downloadPeriodBeginTime Реальное время

downloadPeriodEndTime Реальное время

}

controlType — тип контроля.

controlTime — дата и время ввода данных.

controlCardNumber — идентификатор карточки контролера, использованной в целях контроля.

downloadPeriodBeginTime — время начала периода, за который загружаются данные (в случае загрузки).

downloadPeriodEndTime — время окончания периода, за который загружаются данные (в случае загрузки).

Поколение 2:

VuControlActivityRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

controlType	Тип контроля
controlTime	Реальное время
controlCardNumberAndGeneration	Полный номер и поколение карточки
downloadPeriodBeginTime	Реальное время
downloadPeriodEndTime	Реальное время

}

Вместо controlCardNumber в структуре данных поколения 2 используется следующий элемент данных.

controlCardNumberAndGeneration — идентификатор контрольной карточки, использованной для контроля, в том числе ее поколение.

2.188 VuControlActivityRecordArray (запись данных в БУ о контроле за деятельностью и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, которая относится к блокировке предприятием с использованием этого БУ (~~приложение~~ **добавление 1С**, требование 126).

VuControlActivityRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType	Тип записи
recordSize	ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords	ЦЕЛОЕ ЧИСЛО(0..65535)
records	УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords) ПАРАМЕТРА VuControlActivityRecord

}

recordType обозначает тип записи (VuControlActivityRecord).

Присвоение значения: см. RecordType

recordSize — размер записи VuControlActivityRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей БУ о деятельности по контролю.

2.189 VuDataBlockCounter (счетчик нумерации циклов ввода и извлечения карточек в БУ)

Счетчик, записанный на карточке, который позволяет определять последовательную нумерацию циклов ввода и извлечения карточек в бортовых устройствах.

VuDataBlockCounter ::= СтрокаBCD(РАЗМЕР(2))

Присвоение значения: Порядковый номер с максимальным значением 9999, который снова начинается с 0.

2.190 VuDetailedSpeedBlock (данные в БУ о скорости транспортного средства)

Информация, записанная в бортовом устройстве, которая относится к подробным данным скорости транспортного средства за минуту, в течение которой транспортное средство находится в движении (~~приложение добавление 1В~~, требование 093 и ~~приложение добавление 1С~~, требование 116).

```
VuDetailedSpeedBlock ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
speedBlockBeginDate    Реальное время
speedsPerSecond        РАЗМЕР ПОСЛЕДОВАТЕЛЬНОСТИ(60) ПАРАМЕТРА скорости
}
```

speedBlockBeginDate — дата и время первого значения скорости в блоке данных.

speedsPerSecond — хронологическая последовательность измеряемых скоростей за каждую секунду в течение минуты, которая начинает отсчитываться с момента активации функции speedBlockBeginDate (включительно).

2.191 VuDetailedSpeedBlockRecordArray (данные в БУ о скорости транспортного средства и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, которая относится к подробным данным о скорости транспортного средства.

```
VuDetailedSpeedBlockRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType              Тип записи
recordSize              ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords            ЦЕЛОЕ ЧИСЛО(0..65535)
records                УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
                       ПАРАМЕТРА VuDetailedSpeedBlock
}
```

recordType обозначает тип записи (VuDetailedSpeedBlock).

Присвоение значения: см. RecordType.

recordSize — размер записи VuDetailedSpeedBlock в байтах.

noOfRecords — число записей в совокупности записей.

records — набор блоков подробных данных о скорости.

2.192 VuDetailedSpeedData (детальные данные в БУ о скорости транспортного средства)

Поколение 1:

Информация, записанная в бортовом устройстве, которая относится к подробным данным о скорости транспортного средства.

```
VuDetailedSpeedData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
noOfSpeedBlocks        ЦЕЛОЕ ЧИСЛО(0..216-1)
```

vuDetailedSpeedBlocks УСТАНОВЛЕННЫЙ РАЗМЕР (noOfSpeedBlocks)
 ПАРАМЕТРА VuDetailedSpeedBlock

}

noOfSpeedBlocks — число блоков данных о скорости в совокупности данных vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks — совокупность записей, касающихся блоков детальных данных о скорости.

2.192a VuDigitalMapVersion (версия цифровой карты в БУ)

Поколение 2, версия 2:

Версия цифровой карты, хранящейся в бортовом устройстве (добавление 1С, требование 133j).

VuDigitalMapVersion ::= СтрокаIA5(РАЗМЕР(12))

Присвоение значения: как указано на специальном защищенном веб-сайте лаборатории, уполномоченной проводить испытания на эксплуатационную совместимость (Приложение 1С, требование 133k).

2.193 VuDownloadablePeriod (сроки хранения данных в БУ)

Самая старая и самая последняя даты, на которые в бортовом устройстве хранятся данные, связанные с деятельностью водителей (~~приложение~~ **добавление 1В**, требования 081, 084 или 087 и ~~приложение~~ **добавление 1С**, требования 102, 105, 108).

VuDownloadablePeriod ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

minDownloadableTime Реальное время

maxDownloadableTime Реальное время

}

minDownloadableTime — самые старые данные о дате и времени ввода карточки, или смене деятельности или месте въезда, хранящиеся в БУ.

maxDownloadableTime — самые последние данные о дате и времени ввода карточки или смене деятельности или месте въезда, хранящиеся в БУ.

2.194 VuDownloadablePeriodRecordArray (сроки хранения записей данных в БУ и метаданные)

Поколение 2:

VUDownloadablePeriod плюс метаданные, используемые в протоколе загрузки.

VuDownloadablePeriodRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType Тип записи

recordSize ЦЕЛОЕ ЧИСЛО(1..65535)

noOfRecords ЦЕЛОЕ ЧИСЛО(0..65535)

records УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
 ПАРАМЕТРА VuDownloadablePeriod

}

recordType обозначает тип записи (VuDownloadablePeriod).

Присвоение значения: см. RecordType.

recordSize — размер VuDownloadablePeriod в байтах.

noOfRecords — число записей в совокупности данных.

records — совокупность записей VuDownloadablePeriod.

2.195 VuDownloadActivityData (данные в БУ о загрузке)

Информация, хранящаяся в бортовом устройстве в связи с его последней загрузкой (~~приложение добавление 1B~~, требование 105, и ~~приложение добавление 1C~~, требование 129).

Поколение 1:

```
VuDownloadActivityData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
  downloadingTime          Реальное время
  fullCardNumber           Полный номер карточки
  companyOrWorkshopName    Название
}
```

downloadingTime — дата и время загрузки.

fullCardNumber — идентификатор использованной карточки, разрешающей загрузку.

companyOrWorkshopName — название предприятия или мастерской.

Поколение 2:

```
VuDownloadActivityData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
  downloadingTime          Реальное время
  fullCardNumberAndGeneration  Полный номер и поколение карточки
  companyOrWorkshopName    Название
}
```

Вместо полного номера карточки в структуре данных поколения 2 используется следующий элемент данных.

fullCardNumberAndGeneration — идентификатор использованной карточки, разрешающей загрузку, включая ее поколение.

2.196 VuDownloadActivityDataRecordArray (данные в БУ о загрузке и метаданные)

Поколение 2:

Информация, связанная с последней загрузкой данных с БУ (~~приложение добавление 1C~~, требование 129).

```
VuDownloadActivityDataRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
  recordType              Тип записи
  recordSize              ЦЕЛОЕ ЧИСЛО(1..65535)
  noOfRecords             ЦЕЛОЕ ЧИСЛО(0..65535)
  records                 УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
                        ПАРАМЕТРА VuDownloadActivityData
}
```

recordType обозначает тип записи (VuDownloadActivityData).

Присвоение значения: см. RecordType.

recordSize — размер VuDownloadActivityData в байтах.

noOfRecords — число записей в массиве.

records — совокупность записей данных о деятельности по загрузке.

2.197 VuEventData (данные в БУ о событиях)

Поколение 1:

Информация, записанная в бортовом устройстве, применительно к соответствующим событиям (~~приложение~~ **добавление 1B**, требование 094, за исключением события превышения скорости).

```
VuEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
noOfVuEvents                ЦЕЛОЕ ЧИСЛО(0..255)
vuEventRecords              УСТАНОВЛЕННЫЙ РАЗМЕР (noOfVuEvents)
                             ПАРАМЕТРА VuEventRecord
}
```

noOfVuEvents — число событий, перечисленных в совокупности данных vuEventRecords.

vuEventRecords — совокупность записей о событиях.

2.198 VuEventRecord (запись данных в БУ о событиях)

Информация, записанная в бортовом устройстве, применительно к соответствующему событию (~~приложение~~ **добавление 1B**, требование 094, и **добавление 1C**, требование 117, за исключением события превышения скорости).

Поколение 1:

```
VuEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
eventType                   Тип событие «неисправность»
eventRecordPurpose         Цели регистрации события «неисправность»
eventBeginTime             Реальное время
eventEndTime               Реальное время
cardNumberDriverSlotBegin  Полный номер карточки
cardNumberCodriverSlotBegin  Полный номер карточки
cardNumberDriverSlotEnd    Полный номер карточки
cardNumberCodriverSlotEnd  Полный номер карточки
similarEventsNumber        Число похожих событий
}
```

eventType — тип события.

eventRecordPurpose — цель регистрации данного события.

eventBeginTime — дата и время начала события.

eventEndTime — дата и время окончания события.

cardNumberDriverSlotBegin — идентификатор карточки, вставленной в считывающее устройство водителя в начале события.

cardNumberCodriverSlotBegin — идентификатор карточки, вставленной в считывающее устройство второго водителя в начале события.

cardNumberDriverSlotEnd — идентификатор карточки, вставленной в считывающее устройство водителя в конце события.

cardNumberCodriverSlotEnd — идентификатор карточки, вставленной в считывающее устройство второго водителя в конце события.

similarEventsNumber — число похожих событий за указанный день.

Эта последовательность может быть использована для всех событий, помимо случаев превышения скорости.

Поколение 2:

```
VuEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
eventType                Тип событие «неисправность»
eventRecordPurpose       Цели регистрации события «неисправность»
eventBeginTime           Реальное время
eventEndTime             Реальное время
cardNumberAndGenDriverSlotBegin  Полный номер карточки и поколение
cardNumberAndGenCodriverSlotBegin  Полный номер карточки и поколение
cardNumberAndGenDriverSlotEnd     Полный номер карточки и поколение
cardNumberAndGenCodriverSlotEnd   Полный номер карточки и поколение
similarEventsNumber           Число похожих событий
manufacturerSpecificEventFaultData  Данные о неисправности, связанной с конкретным изготовителем
}
```

В дополнение к поколению 1 используются следующие элементы данных:

manufacturerSpecificEventFaultData содержит дополнительную информацию, связанную с конкретным изготовителем, о данном событии.

Вместо **cardNumberDriverSlotBegin**, **cardNumberCodriverSlotBegin**, **cardNumberDriverSlotEnd** и **cardNumberCodriverSlotEnd** в структуре данных поколения 2 используются следующие элементы данных:

cardNumberAndGenDriverSlotBegin — идентификатор карточки, вставленной в считывающее устройство водителя в начале события, и ее поколения.

cardNumberAndGenCodriverSlotBegin — идентификатор карточки, вставленной в считывающее устройство второго водителя в начале события, и ее поколения.

cardNumberAndGenDriverSlotEnd — идентификатор карточки, вставленной в считывающее устройство водителя в конце события, и ее поколения.

cardNumberAndGenCodriverSlotEnd — идентификатор карточки, вставленной в считывающее устройство второго водителя в конце события, и ее поколения.

Если событие представляет собой нестыковку во времени, то **eventBeginTime** и **eventEndTime** следует толковать следующим образом:

eventBeginTime — дата и время в записывающем оборудовании контрольном устройстве.

eventEndTime — дата и время по ГНСС.

2.199 VuEventRecordArray (запись данных в БУ о событиях и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, применительно к событиям (~~приложение добавление 1С~~, требование 117, за исключением события превышения скорости).

VuEventRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ

recordType	Тип записи
recordSize	ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords	ЦЕЛОЕ ЧИСЛО(0..65535)
records	УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords) ПАРАМЕТРА VuEventRecord

}

recordType обозначает тип записи (VuEventRecord).

Присвоение значения: см. тип записи.

recordSize — размер записи VuEventRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей о событиях.

2.200 VuFaultData (данные в БУ о неисправностях)

Поколение 1:

Информация, записанная в бортовом устройстве, применительно к блокировке предприятием (~~приложение добавление 1В~~, требование 096).

VuFaultData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

noOfVuFaults	ЦЕЛОЕ ЧИСЛО(0..255),
vuFaultRecords	УСТАНОВЛЕННЫЙ РАЗМЕР (noOfVuFaults) ПАРАМЕТРА VuFaultRecord

}

noOfVuFaults — количество неисправностей, перечисленных в совокупности записей vuFaultRecords.

vuFaultRecords — совокупность записей о неисправностях.

2.201 VuFaultRecord (запись данных в БУ о неисправностях)

Информация, записанная в бортовом устройстве, применительно к неисправности (~~приложение добавление 1В~~, требование 096, и ~~приложение добавление 1С~~, требование 118).

Поколение 1:

VuFaultRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

faultType	Тип события «неисправность»
faultRecordPurpose	Цель регистрации события «неисправность»
faultBeginTime	Реальное время
faultEndTime	Реальное время

cardNumberDriverSlotBegin	Полный номер карточки
cardNumberCodriverSlotBegin	Полный номер карточки
cardNumberDriverSlotEnd	Полный номер карточки
cardNumberCodriverSlotEnd	Полный номер карточки

faultType — тип неисправности ~~записывающего оборудования~~ **контрольного устройства.**

faultRecordPurpose — цель регистрации данного события.

faultBeginTime — дата и время начала неисправности.

faultEndTime — дата и время окончания неисправности.

cardNumberDriverSlotBegin — идентификатор карточки, введенной в считывающее устройство водителя в начале неисправности.

cardNumberCodriverSlotBegin — идентификатор карточки, введенной в считывающее устройство второго водителя в начале неисправности.

cardNumberDriverSlotEnd — идентификатор карточки, введенной в считывающее устройство водителя в конце неисправности.

cardNumberCodriverSlotEnd — идентификатор карточки, введенной в считывающее устройство второго водителя в конце неисправности.

Поколение 2:

VuFaultRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

faultType	Тип события «неисправность»
faultRecordPurpose	Цель регистрации события «неисправность»
faultBeginTime	Реальное время
faultEndTime	Реальное время
cardNumberAndGenDriverSlotBegin	Полный номер и поколение карточки
cardNumberAndGenCodriverSlotBegin	Полный номер и поколение карточки
cardNumberAndGenDriverSlotEnd	Полный номер и поколение карточки
cardNumberAndGenCodriverSlotEnd	Полный номер и поколение карточки
manufacturerSpecificEventFaultData	Данные о неисправности, связанной с конкретным изготовителем

}

В дополнение к поколению 1, используется следующий элемент данных:

manufacturerSpecificEventFaultData содержит дополнительную информацию, связанную с конкретным изготовителем, о данной неисправности.

Вместо cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd и cardNumberCodriverSlotEnd в структуре данных поколения 2 используются следующие элементы данных:

cardNumberAndGenDriverSlotBegin — идентификатор карточки, вставленной в считывающее устройство водителя в начале неисправности, и ее поколения.

cardNumberAndGenCodriverSlotBegin — идентификатор карточки, вставленной в считывающее устройство второго водителя в начале неисправности, и ее поколения.

cardNumberAndGenDriverSlotEnd — идентификатор карточки, вставленной в считывающее устройство водителя в конце неисправности, и ее поколения.

cardNumberAndGenCodriverSlotEnd — идентификатор карточки, вставленной в считывающее устройство второго водителя в конце неисправности, и ее поколения.

2.202 VuFaultRecordArray (запись данных в БУ о неисправностях и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, применительно к неисправностям (~~приложение~~ **добавление** 1С, требование 118).

```
VuFaultRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType                Тип записи
recordSize                 ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords               ЦЕЛОЕ ЧИСЛО(0..65535)
records                   УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
                           ПАРАМЕТРА VuFaultRecord
}
```

recordType обозначает тип записи (VuFaultRecord).

Присвоение значения: см. RecordType.

recordSize — размер записи VuFaultRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей о неисправностях.

2.203 VuGNSSADRecord (запись данных в БУ о НакВУ по ГНСС)

Поколение 2, версия 1:

~~2.203~~ VuGNSSADRecord

Информация, записанная в бортовом устройстве, которая относится к местоположению транспортного средства по ГНСС, если ~~непрерывное~~ **накопленное** время управления ~~водителем~~ достигает значения, кратного трем часам (~~приложение~~ **добавление** 1С, требования 108 и 110).

```
VuGNSSADRecord VuGNSSADRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
timeStamp                 Реальное время
cardNumberAndGenDriverSlot Полный номер и поколение карточки
cardNumberAndGenCodriverSlot Полный номер и поколение карточки
gnssPlaceRecord           Запись о месте по ГНСС
vehicleOdometerValue      Показания счетчика пробега
}
```

timeStamp — дата и время, когда ~~непрерывное~~ **накопленное** время управления ~~водителем~~ **владельцем карточки** достигает значения, кратного трем часам.

cardNumberAndGenDriverSlotEnd — идентификатор и поколение карточки, вставленной в считывающее устройство водителя.

cardNumberAndGenCodriverSlotEnd — идентификатор и поколение карточки, вставленной в считывающее устройство второго водителя.

gnssPlaceRecord содержит информацию, касающуюся местоположения транспортного средства.

vehicleOdometerValue — показания счетчика пробега, когда накопленное время управления достигает значения, кратного трем часам.

Поколение 2, версия 2:

Информация, записанная в бортовом устройстве, которая относится к местоположению транспортного средства по ГНСС, если накопленное время управления достигает значения, кратного трем часам (приложение добавление 1С, требования 108 и 110).

VuGNSSADRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

timeStamp	Реальное время
cardNumberAndGenDriverSlot	Полный номер и поколение карточки
cardNumberAndGenCodriverSlot	Полный номер и поколение карточки
gnssPlaceAuthRecord	Запись аутентифицированного места по ГНСС
vehicleOdometerValue	Показания счетчика пробега

}

В версии 2 поколения 2 вместо **gnssPlaceRecord** используется позиция **gnssPlaceAuthRecord**, которая дополнительно содержит статус аутентификации GNSS.

2.203a **VuBorderCrossingRecord** (запись данных в БУ о пересечении границы)

Поколение 2, версия 2:

Информация, хранящаяся в бортовом устройстве, применительно к пересечению границы данным транспортным средством, когда оно пересекло границу соответствующей страны (добавление 1С, требования 133a и 133b).

VuBorderCrossingRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

cardNumberAndGenDriverSlot	Полный номер и поколение карточки
cardNumberAndGenCodriverSlot	Полный номер и поколение карточки
countryLeft	Числовой код страны
countryEntered	Числовой код страны
gnssPlaceAuthRecord	Запись аутентифицированного места по ГНСС
vehicleOdometerValue	Показания счетчика пробега

}

CardNumberAndGenDriverSlotEnd — идентификатор и поколение карточки, вставленной в считывающее устройство водителя.

cardNumberAndGenCoDriverSlot — идентификатор и поколение карточки, вставленной в считывающее устройство второго водителя.

countryLeft — страна, которую покинуло транспортное средство, на основе последнего доступного местоположения перед обнаружением пересечения границы. «Остальной мир» (числовой код страны 'FF'Н) используется в том случае, когда бортовое устройство не может определить страну, в которой находится транспортное средство в данный момент (например, текущая страна в сохраненных цифровых картах не отражена).

countryEntered — страна, в которую прибыло транспортное средство. «Остальной мир» (числовой код страны 'FF'Н) используется в том случае, когда бортовое устройство не может определить страну, в которой находится транспортное средство в данный момент (например, текущая страна в сохраненных цифровых картах не отражена).

gnssPlaceAuthRecord содержит информацию, относящуюся к местоположению транспортного средства в момент обнаружения пересечения границы, и его статус аутентификации.

vehicleOdometerValue — показания счетчика пробега в тот момент, когда бортовое устройство обнаружило, что транспортное средство пересекло границу соответствующей страны.

2.203b VuBorderCrossingRecordArray (запись данных в БУ о пересечении границы и метаданные)

Поколение 2, версия 2:

Информация, записанная в бортовом устройстве, которая относится к пересечению границы данным транспортным средством (добавление 1С, требование 133с).

```
VuBorderCrossingRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType                Тип записи
recordSize                ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords              ЦЕЛОЕ ЧИСЛО(0..65535)
records                  УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
                        ПАРАМЕТРА VuBorderCrossingRecord
}
```

recordType обозначает тип записи (VuBorderCrossingRecord).

Присвоение значения: см. RecordType.

recordSize — размер записи VuBorderCrossingRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей о пересечении границы.

2.204 VuGNSSADRecordArray (запись данных в БУ о НакВУ по ГНСС и метаданные)

~~2.204 VuGNSSCDRecordArray~~

Поколение 2:

Информация, записанная в бортовом устройстве, которая относится к местоположению транспортного средства по ГНСС, если ~~непрерывное~~ **накопленное** время управления водителем достигает значения, кратного трем часам (~~приложение~~ **добавление 1С**, требования 108 и 110).

```
VuGNSSADRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType                Тип записи
recordSize                ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords              ЦЕЛОЕ ЧИСЛО(0..65535)
```


Поколение 2:

VuIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

vuManufacturerName	Название изготовителя бортового устройства
vuManufacturerAddress	Адрес изготовителя бортового устройства
vuPartNumber	Номер детали БУ
vuSerialNumber	Серийный номер БУ
vuSoftwareIdentification	Идентификация программного обеспечения БУ
vuManufacturingDate	Дата изготовления БУ,
vuApprovalNumber	Номер официального утверждения БУ
vuGeneration	Поколение
vuAbility	Характеристики БУ
vuDigitalMapVersion	Версия цифровой карты в БУ

}

В дополнение к поколению 1 используются следующие элементы данных:

vuGeneration идентифицирует поколение бортового устройства.

vuAbility дает информацию о том, поддерживает ли БУ карточки тахографов поколения 1 или нет.

vuDigitalMapVersion — версия цифровой карты, хранящейся в бортовом устройстве (присутствует только в версии 2).

2.206 VuIdentificationRecordArray (идентификация БУ и метаданные)

Поколение 2:

Идентификация БУ и метаданные, используемые в протоколе загрузки.

VuIdentificationRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType	Тип записи
recordSize	ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords	ЦЕЛОЕ ЧИСЛО(0..65535)
records	УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords) ПАРАМЕТРА VuIdentification

}

recordType обозначает тип записи (VuIdentification).

Присвоение значения: см. RecordType.

recordSize — размер VuIdentification в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей VuIdentification.

2.207 VuITSConsentRecord (запись в БУ о согласии водителя использовать ИТС)

Поколение 2:

Информация, записанная в бортовом устройстве, которая относится к согласию водителя на пользование интеллектуальными транспортными системами.

```

VuITSConsentRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
cardNumberAndGen      Полный номер и поколение карточки
consent                БУЛЕВО ВЫРАЖЕНИЕ
}

```

cardNumberAndGen идентифицирует карточку, в том числе ее поколение. Это должна быть карточка водителя или карточка мастерской.

consent — метка, указывающая на то, дал ли водитель свое согласие на пользование интеллектуальными транспортными системами в случае данного транспортного средства/бортового устройства.

Присвоение значения:

TRUE (ИСТИНА) означает согласие водителя на пользование интеллектуальными транспортными системами

FALSE (ЛОЖЬ) означает отказ водителя от пользования интеллектуальными транспортными системами

2.208 VuITSConsentRecordArray (запись в БУ о согласии водителя использовать ИТС и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, которая относится к согласию на пользование интеллектуальными транспортными системами (~~приложение~~ **добавление 1С**, требование 200).

```

VuITSConsentRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType            Тип записи
recordSize            ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords          ЦЕЛОЕ ЧИСЛО(0..65535)
records              УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
                    ПАРАМЕТРА VuITSConsentRecord
}

```

recordType обозначает тип записи (VuITSConsentRecord).

Присвоение значения: см. RecordType.

recordSize — размер записи VuITSConsentRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей о согласии на пользование ИТС.

2.208a VuLoadUnloadRecord (запись данных в БУ о загрузке/разгрузке)

Поколение 2, версия 2:

Информация, хранящаяся в бортовом устройстве, связанная с введенной операцией загрузки/разгрузки (**добавление 1С**, требования 133e, 133f и 133g).

```

VuLoadUnloadRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
timeStamp            Реальное время
operationType        Тип операции
cardNumberAndGenDriverSlot  Полный номер и поколение карточки
cardNumberAndGenCodriverSlot  Полный номер и поколение карточки
}

```

gnssPlaceAuthRecord	Запись аутентифицированного места по ГНСС
vehicleOdometerValue	Показания счетчика пробега
}	
timeStamp	— дата и время, когда были введены данные по операции загрузки/разгрузки.
operationType	— тип введенной операции (загрузка, разгрузка или одновременная загрузка/разгрузка).
cardNumberAndGenDriverSlot	— идентификатор карточки, вставленной в считывающее устройство водителя, и ее поколение.
cardNumberAndGenCodriverSlot	— идентификатор карточки, вставленной в считывающее устройство второго водителя, и ее поколение.
gnssPlaceAuthRecord	содержит информацию, относящуюся к местоположению транспортного средства, и его статус аутентификации.
vehicleOdometerValue	— показания счетчика пробега в момент ввода данных об операции загрузки/разгрузки.

2.208b VuLoadUnloadRecordArray (запись данных в БУ о загрузке/разгрузке и метаданные)

Поколение 2, версия 2:

Информация, хранящаяся в бортовом устройстве, связанная с введенной операцией загрузки/разгрузки (добавление 1С, требование 133h).

VuLoadUnloadRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType	Тип записи
recordSize	ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords	ЦЕЛОЕ ЧИСЛО(0..65535)
records	УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords) ПАРАМЕТРА VuLoadUnloadRecord
}	

recordType обозначает тип записи (VuLoadUnloadRecord).

Присвоение значения: см. RecordType.

recordSize — размер VuLoadUnloadRecord in байтах.

VuLoadUnloadRecord VuCardRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей по операциям загрузки/выгрузки.

2.209 VuManufacturerAddress (адрес изготовителя БУ)

Адрес изготовителя бортового устройства.

VuManufacturerAddress ::= Адрес

Присвоение значения: не указано.

2.210 VuManufacturerName (наименование изготовителя БУ)

Наименование изготовителя бортового устройства.

VuManufacturerName ::= Наименование

Присвоение значения: не указано.

2.211 VuManufacturingDate (дата изготовления БУ)

Дата изготовления бортового устройства.

VuManufacturingDate ::= Реальное время

Присвоение значения: не указано.

2.212 VuOverSpeedingControlData (данные в БУ о превышении скорости)

Информация, записанная в бортовом устройстве, которая относится к событиям превышения скорости с момента последнего контроля за превышением скорости (~~приложение добавление 1В~~, требование 095, и ~~приложение добавление 1С~~, требование 117).

```
VuOverSpeedingControlData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
lastOverspeedControlTime    Реальное время
firstOverspeedSince         Реальное время
numberOfOverspeedSince      Число превышений скорости
}
```

lastOverspeedControlTime — дата и время последнего контроля за превышением скорости.

firstOverspeedSince — дата и время первого превышения скорости после данного контроля за превышением скорости.

NumberOfOverspeedSince — количество случаев превышения скорости с момента последнего контроля за превышением скорости.

2.213 VuOverSpeedingControlDataRecordArray (данные в БУ о превышении скорости и метаданные)

Поколение 2:

VuOverSpeedingControlData плюс метаданные, используемые в протоколе загрузки.

```
VuOverSpeedingControlDataRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType                  Тип записи
recordSize                  ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords                 ЦЕЛОЕ ЧИСЛО(0..65535)
records                     УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
                             ПАРАМЕТРА VuOverSpeedingControlData
}
```

recordType обозначает тип записи (VuOverSpeedingControlData).

Присвоение значения: см. RecordType.

recordSize — размер VuOverSpeedingControlData в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей данных контроля за превышением скорости.

2.214 VuOverSpeedingEventData (данные в БУ о событиях превышения скорости)

Поколение 1:

Информация, записанная в бортовом устройстве, которая связана с превышением скорости (~~приложение добавление 1В~~, требование 094).

```
VuOverSpeedingEventData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
noOfVuOverSpeedingEvents      ЦЕЛОЕ ЧИСЛО(0..255)
vuOverSpeedingEventRecords    УСТАНОВЛЕННЫЙ РАЗМЕР (noOfVuOverSpeedingEvents)
                               ПАРАМЕТРА VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents — количество событий, перечисленных в совокупности записей OverSpeedingEventRecords.

vuOverSpeedingEventRecords — совокупность записей о событиях превышения скорости.

2.215 VuOverSpeedingEventRecord (запись данных в БУ о событиях превышения скорости)

Поколение 1:

Информация, записанная в бортовом устройстве, применительно к событиям превышения скорости (~~приложение добавление 1В~~, требование 094, и ~~приложение добавление 1С~~, требование 117).

```
VuOverSpeedingEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
eventType                      Событие «тип неисправности»
eventRecordPurpose             Цель регистрации события «неисправность»
eventBeginTime                 Реальное время
eventEndTime                   Реальное время
maxSpeedValue                  Максимальная скорость
averageSpeedValue              Средняя скорость
cardNumberDriverSlotBegin      Полный номер карточки
similarEventsNumber            Число похожих событий
}
```

eventType — тип события.

eventRecordPurpose — цель регистрации данного события.

eventBeginTime — дата и время начала события.

eventEndTime — дата и время окончания события.

maxSpeedValue — максимальная скорость, измеренная во время события.

averageSpeedValue — среднеарифметическая скорость, измеренная во время события.

cardNumberDriverSlotBegin — идентификатор карточки, вставленной в считывающее устройство водителя в начале события.

similarEventsNumber — число похожих событий за указанный день.

Поколение 2:

Информация, записанная в бортовом устройстве, применительно к событиям превышения скорости (~~приложение добавление 1В~~, требование 094, и ~~приложение добавление 1С~~, требование 117).

VuOverSpeedingEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

eventType	Тип события
eventRecordPurpose	Цель регистрации события «неисправность»
eventBeginTime	Реальное время
eventEndTime	Реальное время
maxSpeedValue	Максимальная скорость
averageSpeedValue	Средняя скорость
cardNumberAndGenDriverSlotBegin	Полный номер и поколение карточки
similarEventsNumber	Число похожих событий

Вместо cardNumberDriverSlotBegin в структуре данных поколения 2 используется следующий элемент данных:

cardNumberAndGenDriverSlotBegin — идентификатор и поколение карточки, вставленной в считывающее устройство водителя в начале события.

2.216 VuOverSpeedingEventRecordArray (запись данных в БУ о событиях превышения скорости и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, которая связана с превышением скорости (~~приложение добавление 1С~~, требование 117).

VuOverSpeedingEventRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType	Тип записи
recordSize	ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords	ЦЕЛОЕ ЧИСЛО(0..65535)
records	УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords) ПАРАМЕТРА VuOverSpeedingEventRecord

recordType обозначает тип записи (VuOverSpeedingEventRecord).

Присвоение значения: см. RecordType.

recordSize — размер VuOverSpeedingEventRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — набор записей событий, связанных с превышением скорости.

2.217 VuPartNumber (номер детали БУ)

Номер детали бортового устройства.

VuPartNumber ::= СтрокаIA5(РАЗМЕР(16))

Присвоение значения: по усмотрению конкретного изготовителя БУ.

2.218 VuPlaceDailyWorkPeriodData (данные в БУ о месте, где начинается и заканчивается ежедневный период работы)

Поколение 1:

Информация, записанная в бортовом устройстве, которая относится к местам, где водители начинают или заканчивают дневной период работы (~~приложение добавление~~ 1B, требование 087 и ~~приложение добавление~~ 1C, требования 108 и 110).

```
VuPlaceDailyWorkPeriodData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
noOfPlaceRecords          ЦЕЛОЕ ЧИСЛО(0..255)
vuPlaceDailyWorkPeriodRecords  УСТАНОВЛЕННЫЙ РАЗМЕР (noOfPlaceRecords)
                               ПАРАМЕТРА VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords — число записей, перечисленных в совокупности записей vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords — совокупность записей, касающихся мест ежедневных периодов работы.

2.219 VuPlaceDailyWorkPeriodRecord (запись данных в БУ о месте, где начинается и заканчивается ежедневный период работы)

Поколение 1:

Информация, записанная в бортовом устройстве, которая относится к местам, где водитель начинает или заканчивает ежедневный период работы (~~приложение добавление~~ 1B, требование 087, и ~~приложение добавление~~ 1C, требования 108 и 110).

```
VuPlaceDailyWorkPeriodData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
fullCardNumber            Полный номер карточки
placeRecord              Запись, касающаяся мест
}
```

fullCardNumber — тип карточки водителя, ~~выдавшее ее государство член Договаривающаяся сторона, выдавшая карточку,~~ и номер карточки.

placeRecord содержит информацию, связанную с местом въезда.

Поколение 2, версия 1:

Информация, записанная в бортовом устройстве, которая относится к местам, где водитель начинает или заканчивает ежедневный период работы (~~приложение добавление~~ 1B, требование 087, и ~~приложение добавление~~ 1C, требования 108 и 110).

```
VuPlaceDailyWorkPeriodRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
fullCardNumberAndGeneration  Полный номер и поколение карточки
PlaceRecord                  Запись, касающаяся мест
}
```

Вместо fullCardNumber в структуре данных поколения 2 используется следующий элемент данных.

fullCardNumberAndGeneration — тип карточки, ~~выдавшее ее государство член Договаривающаяся сторона, выдавшая карточку,~~ а также ее номер и поколение, как они записаны на карточке.

Поколение 2, версия 2:

Информация, записанная в бортовом устройстве, которая относится к месту, где водитель начинает или заканчивает ежедневный период работы (добавление 1В, требование 087, и добавление 1С, требования 108 и 110).

VuPlaceDailyWorkPeriodRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

fullCardNumberAndGeneration	Полный номер и поколение карточки
placeAuthRecord	Запись аутентифицированного места

}

Вместо **placeRecord** в структуре данных поколения 2 версии 2 используется следующий элемент данных.

placeAuthRecord содержит информацию, связанную с введенным местом, зарегистрированным местоположением, статусом аутентификации GNSS и временем определения местоположения.

2.220 VuPlaceDailyWorkPeriodRecordArray (запись данных в БУ о месте, где начинается и заканчивается ежедневный период работы, и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, которая относится к местам, где водители начинают или заканчивают ежедневный период работы (приложение добавление 1С, требования 108 и 110).

VuPlaceDailyWorkPeriodRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType	Тип записи
recordSize	ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords	ЦЕЛОЕ ЧИСЛО(0..65535)
records	УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords) ПАРАМЕТРА VuPlaceDailyWorkPeriodRecord

}

recordType обозначает тип записи (VuPlaceDailyWorkPeriodRecord).

Присвоение значения: см. RecordType.

recordSize — размер записи VuPlaceDailyWorkPeriodRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — набор записей, связанных с местом.

2.221 VuPrivateKey (закрытый ключ БУ)

Поколение 1:

Закрытый ключ бортового устройства.

VuPrivateKey ::= закрытая экспонента ключа RSA

2.222 VuPublicKey (открытый ключ БУ)

Поколение 1:

Открытый ключ бортового устройства.

VuPublicKey ::= открытый ключ

2.222a VuRtcTime (время в БУ по часам реального времени)

Поколение 2, версия 2:

Время на часах RTC БУ, передаваемое БУ на внешнее устройство ГНСС, см. подраздел 12, требование GNS_3f.

VuRtcTime ::= Реальное время

2.223 VuSerialNumber (серийный номер БУ)

Серийный номер бортового устройства (~~приложение добавление 1B~~, требование 075, и ~~приложение добавление 1C~~, требование 93).

VuSerialNumber ::= ExtendedSerialNumber

2.224 VuSoftInstallationDate (дата установки программного обеспечения БУ)

Дата установки программного обеспечения бортового устройства.

VuSoftInstallationDate ::= Реальное время

Присвоение значения: не указано.

2.225 VuSoftwareIdentification (идентификация программного обеспечения БУ)

Информация, записанная в бортовом устройстве, которая относится к установленному программному обеспечению.

VuSoftwareIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

vuSoftwareVersion Версия программного обеспечения БУ

vuSoftInstallationDate Дата установки программного обеспечения БУ

}

vuSoftwareVersion — номер версии программного обеспечения бортового устройства.

vuSoftInstallationDate — дата установки программного обеспечения.

2.226 VuSoftwareVersion (версия программного обеспечения БУ)

Номер версии программного обеспечения бортового устройства.

VuSoftwareVersion ::= СтрокаIA5(РАЗМЕР4))

Присвоение значения: не указано.

2.227 VuSpecificConditionData (данные об особых условиях в БУ)

Поколение 1:

Информация, записанная в бортовом устройстве, которая связана с особыми условиями.

```
SpecificConditionRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
noOfSpecificConditionRecords ЦЕЛОЕ ЧИСЛО(0..216-1)
specificConditionRecords УСТАНОВЛЕННЫЙ РАЗМЕР (noOfSpecificConditionRecords)
ПАРАМЕТРА SpecificConditionRecord
}
```

noOfSpecificConditionRecords — количество записей, перечисленных в совокупности записей specificConditionRecords.

specificConditionRecords — совокупность записей об особых условиях.

2.228 VuSpecificConditionRecordArray (данные об особых условиях в БУ и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, которая связана с особыми условиями (~~приложение добавление 1С~~, требование 130).

```
VuSpecificConditionRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType Тип записи
recordSize ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords ЦЕЛОЕ ЧИСЛО(0..65535)
records УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
ПАРАМЕТРА SpecificConditionRecord
}
```

recordType обозначает тип записи (SpecificConditionRecord).

Присвоение значения: см. RecordType.

recordSize — размер записи SpecificConditionRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей об особых условиях.

2.229 VuTimeAdjustmentData (данные в БУ о корректировке времени)

Поколение 1:

Информация, записанная в бортовом устройстве, которая относится к корректировке времени, не связанной с регулярной калибровкой (~~приложение добавление 1В~~, требование 101).

```
VuTimeAdjustmentData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
noOfVuTimeAdjRecords ЦЕЛОЕ ЧИСЛО(0..6),
vuTimeAdjustmentRecords УСТАНОВЛЕННЫЙ РАЗМЕР (noOfVuTimeAdjRecords)
ПАРАМЕТРА VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords — количество записей в совокупности записей **vuTimeAdjustmentRecords**.

vuTimeAdjustmentRecords — совокупность записей о корректировках времени.

2.230 Reserved for future use (зарезервирован для использования в будущем)

~~2.230 VuTimeAdjustmentGNSSRecord~~

2.231 Reserved for future use (зарезервирован для использования в будущем)

2.232 VuTimeAdjustmentRecord (запись данных в БУ о корректировке времени)

Информация, записанная в бортовом устройстве, которая относится к корректировке времени на основании данных времени по ГНСС (приложение 1С, требования 124 и 125). — IC требование 124 и 125)

VuTimeAdjustmentGNSSRecord ПОСЛЕДОВАТЕЛЬНОСТЬ

oldTimeValue — Реальное время

newTimeValue — Реальное время

oldTimeValue, newTimeValue — старые и новые значения даты и времени.

~~2.231 VuTimeAdjustmentGNSSRecordArray~~

Информация, записанная в бортовом устройстве, которая относится к корректировке времени на основании данных времени по ГНСС (приложение 1С, требования 124 и 125).

VuTimeAdjustmentGNSSRecord ПОСЛЕДОВАТЕЛЬНОСТЬ

recordType — RecordType

recordSize — ЦЕЛОЕ ЧИСЛО(1..65535)

noOfRecords — ЦЕЛОЕ ЧИСЛО(0..65535)

records — SETSIZE(noOfRecords)OFVuTimeAdjustmentGNSSRecord

recordType указывает на тип записи (VuTimeAdjustmentGNSSRecord).

Присвоение значения: см. RecordType.

recordSize — размер записи VuTimeAdjustmentGNSSRecord в байтах.

noOfRecords — число записей в массиве.

records — совокупность записей о корректировке времени по ГНСС.

Информация, записанная в бортовом устройстве, которая относится к корректировке времени, не связанной с регулярной калибровкой (приложение добавление 1В, требование 101, и приложение добавление 1С, требования 124 и 125).

Поколение 1:

```
VuTimeAdjustmentRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
oldTimeValue           Реальное время
newTimeValue           Реальное время
workshopName           Название
workshopAddress        Адрес
workshopCardNumber     Полный номер карточки
}
```

oldTimeValue, newTimeValue — старые и новые значения даты и времени.

workshopName, workshopAddress — название и адрес мастерской.

workshopCardNumber — идентификатор карточки мастерской, используемой для корректировки времени.

Поколение 2:

```
VuTimeAdjustmentRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
oldTimeValue           Реальное время
newTimeValue           Реальное время
workshopName           Название
workshopAddress        Адрес
workshopCardNumberAndGeneration  Полный номер и поколение карточки
                               мастерской
}
```

Вместо **workshopCardNumber** в структуре данных поколения 2 используется следующий элемент данных.

workshopCardNumberAndGeneration идентифицирует карточку мастерской, в том числе ее поколение, использованную для выполнения корректировки времени.

2.233 VuTimeAdjustmentRecordArray (запись данных в БУ о корректировке времени и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, которая относится к корректировке времени, не связанной с регулярной калибровкой (~~приложение~~ **добавление 1С**, требования 124 и 125).

```
VuTimeAdjustmentRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType             Тип записи
recordSize             ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords            ЦЕЛОЕ ЧИСЛО(0..65535)
records                УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
                       ПАРАМЕТРА VuTimeAdjustmentRecord
}
```

recordType обозначает тип записи (VuTimeAdjustmentRecord).

Присвоение значения: см. RecordType.

recordSize — размер записи VuTimeAdjustmentRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей о корректировке времени.

2.234 WorkshopCardApplicationIdentification (идентификация приложения карточки мастерской)

Информация, записанная на карточке мастерской, которая относится к идентификации приложения карточки (~~приложение~~ **добавление 1С**, требования 307 и 330).

Поколение 1:

```
WorkshopCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
typeofTachographCardID          Тип оборудования
cardStructureVersion             Версия структуры карточки
noOfEventsPerType                Число событий по типу
noOfFaultsPerType                Число неисправностей по типу
activityStructureLength          Длина записи о деятельности на карточке
noOfCardVehicleRecords           Число записей на карточке, касающихся
                                транспортных средств
noOfCardPlaceRecords             Число записей на карточке, касающихся мест
noOfCalibrationRecords           Число записей о калибровках
}
```

typeofTachographCardId уточняет реализованный ~~используемый~~ тип карточки.

cardStructureVersion уточняет версию структуры, реализованной на карточке.

noOfEventsPerType — число событий по типу события, которое может быть записано на карточку.

noOfFaultsPerType — число неисправностей по типу неисправности, которое может быть записано на карточку.

activityStructureLength — число байтов, которые могут быть использованы для хранения записей, относящихся к виду деятельности.

NoOfCardVehicleRecords — число записей о транспортных средствах, которые можно хранить на карточке.

noOfCardPlaceRecords — число записей о местах, которые можно хранить на карточке.

noOfCalibrationRecords — число записей о калибровке, которые можно хранить на карточке.

Поколение 2:

```
WorkshopCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
typeofTachographCardId          Тип оборудования
cardStructureVersion             Версия структуры карточки
noOfEventsPerType                Число событий по типу
noOfFaultsPerType                Число неисправностей по типу
activityStructureLength          Длина записи о деятельности на карточке
noOfCardVehicleRecords           Число записей о транспортных средствах на
                                карточке
noOfCardPlaceRecords            Число записей о местах на карточке
```

noOfCalibrationRecords	Число записей о калибровках
noOfGNSSCDRecords	NoOfGNSSCDRecords
noOfGNSSADRecords	Число записей о НакУ по ГНСС
noOfSpecificConditionRecords	Число записей об особых условиях
noOfCardVehicleUnitRecords	Число записей о единицах транспортных средств на карточке
}	

В дополнение к поколению 1 используются следующие элементы данных:

~~noOfGNSSCDRecords~~ noOfGNSSADRecords — число записей о непрерывном накопленном времени управления по ГНСС, которые могут храниться на карточке.

noOfSpecificConditionRecords — число записей о конкретных условиях, которые могут храниться на карточке.

NoOfCardVehicleUnitRecords — записей об используемых единицах транспортных средств, которые могут храниться на карточке.

2.234a WorkshopCardApplicationIdentificationV2 (идентификация приложения карточки мастерской V2)

Поколение 2, версия 2:

Информация, записанная на карточке мастерской, которая относится к идентификации приложения карточки (добавление 1С, требование 330a).

WorkshopCardApplicationIdentificationV2 ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

lengthOfFollowingData	Длина следующих данных
noOfBorderCrossingRecords	Число записей о пересечении границы
noOfLoadUnloadRecords	Число записей, касающихся загрузки/разгрузки
noOfLoadTypeEntryRecords	Число записей о типе поступившего груза
vuConfigurationLengthRange	Длина данных о конфигурации БУ
}	

lengthOfFollowingData — количество последующих байтов в записи.

noOfBorderCrossingRecords — число записей о пересечении границы, которые могут храниться на карточке мастерской.

noOfLoadUnloadRecords — число записей о загрузке/разгрузке, которые могут храниться на карточке мастерской.

noOfLoadTypeEntryRecords — число записей о типе поступившего груза, которые могут храниться на карточке мастерской.

vuConfigurationLengthRange — количество байтов в карточке тахографа, доступных для хранения конфигураций БУ.

2.234b WorkshopCardCalibrationAddData (запись дополнительных данных калибровки карточки мастерской)

Поколение 2, версия 2:

Информация, хранящаяся на карточке мастерской, связанная с дополнительными данными (например, тип загрузки по умолчанию), введенными во время калибровки (добавление 1С, требование 356l).

WorkshopCardCalibrationAddData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

calibrationPointerNewestRecord	ЦЕЛОЕ ЧИСЛО (0..NoOfCalibrationRecords-1)
workshopCardCalibrationAddDataRecords	УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfCalibrationRecords) ПАРАМЕТРА WorkshopCardCalibrationAdd DataRecord
}	

calibrationPointerNewestRecord — индекс последней обновленной записи дополнительных данных калибровки.

Присвоение значения — число, соответствующее числителю записи дополнительных данных калибровки, начиная с '0' для первого отображения записи дополнительных сведений о калибровке в структуре данных.

workshopCardCalibrationAddDataRecords — совокупность записей, содержащих старое значение даты и времени, идентификатор транспортного средства и тип груза транспортного средства по умолчанию.

2.234c **WorkshopCardCalibrationAddDataRecord** (запись дополнительных данных калибровки карточки мастерской)

Поколение 2, версия 2:

Информация, хранящаяся на карточке мастерской, связанная с дополнительными данными (например, тип груза по умолчанию), введенными во время калибровки (добавление 1С, требование 356k).

WorkshopCardCalibrationAddDataRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

oldTimeValue	Реальное время
vehicleIdentificationNumber	Идентификационный номер транспортного средства
byDefaultLoadType	Тип груза
calibrationCountry	Числовой код страны
calibrationCountryTimestamp	Реальное время
}	

oldTimeValue — старое значение даты и времени, содержащееся в соответствующей записи **WorkshopCardCalibrationRecord**,

vehicleIdentificationNumber — идентификационный номер транспортного средства, также содержащийся в соответствующей записи **WorkshopCardCalibrationRecord**,

byDefaultLoadType — тип груза по умолчанию в случае данного транспортного средства (присутствует только в случае версии 2).

calibrationCountry — страна, в которой была выполнена калибровка.

calibrationCountryTimestamp — дата и время выдачи приемником ГНСС местоположения, использованного для определения данной страны.

2.235 **WorkshopCardCalibrationData** (данные калибровки карточки мастерской)

Информация, записанная на карточке мастерской, которая относится к действиям мастерской, произведенным с карточкой (приложение добавление 1С, требования 314, 316, 337 и 339).

```

WorkshopCardCalibrationAddData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
calibrationTotalNumber      ЦЕЛОЕ ЧИСЛО(0..20), 216-1)
calibrationPointerNewestRecord  ЦЕЛОЕ ЧИСЛО(0 .. NoOfCalibrationRecords-1),
calibrationRecords          УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfCalibrationRecords)
                             ПАРАМЕТРА WorkshopCardCalibrationRecord
}

```

calibrationTotalNumber — общее число калибровок, произведенных с карточкой.

calibrationPointerNewestRecord — индекс последней обновленной записи данных калибровки.

Присвоение значения: число, соответствующее числовому показателю записи калибровки, которое начинается с с '0' в случае первой регистрации записей калибровки в структуре данных.

calibrationRecords — совокупность данных с записями, содержащими данные о калибровке и/или корректировке времени.

2.236 WorkshopCardCalibrationRecord (запись данных калибровки карточки мастерской)

Информация, записанная на карточке мастерской в связи с произведенной ею калибровкой с данной карточкой (~~приложение~~ **добавление 1С**, требования 314 и 337).

Поколение 1:

```

WorkshopCardCalibrationRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
calibrationPurpose          Цель калибровки
vehicleIdentificationNumber  Идентификационный номер транспортного
                             средства
vehicleRegistration          Идентификация регистрации транспортного
                             средства
wVehicleCharacteristicConstant  Характеристическая константа W транспортного
                             средства
kConstantOfRecordingEquipment  Константа записывающего оборудования
lTyreCircumference          Окружность шины L
tyreSize                    Размер шины
authorisedSpeed              Разрешенная скорость
oldOdometerValue             Показания счетчика пробега
newOdometerValue             Показания счетчика пробега
oldTimeValue                 Реальное время
newTimeValue                 Реальное время
nextCalibrationDate          Реальное время
vuPartNumber                 Номер детали БУ
vuSerialNumber               Серийный номер БУ
sensorSerialNumber           Серийный номер датчика движения
}

```

calibrationPurpose — цель калибровки.

vehicleIdentificationNumber — VIN.

vehicleRegistration — содержит VRN и данные государства-члена Договаривающейся стороны регистрации.

wVehicleCharacteristicConstant — характеристический коэффициент w транспортного средства.

kConstantOfRecordingEquipment — константа ~~записывающего оборудования~~ **контрольного устройства**.

ITyreCircumference — фактическая окружность шин колес.

tyreSize — обозначение габаритов шин, установленных на транспортном средстве.

authorisedSpeed — максимальная допустимая скорость транспортного средства.

oldOdometerValue, newOdometerValue — старые и новые показания счетчика пробега.

oldTimeValue, newTimeValue — старые и новые значения даты и времени.

nextCalibrationDate — дата следующей калибровки типа, указанного в позиции CalibrationPurpose, которую должен произвести уполномоченный инспекционный орган.

vuPartNumber, vuSerialNumber и **sensorSerialNumber** — элементы данных для идентификации ~~записывающего оборудования~~ **контрольного устройства**.

Поколение 2:

WorkshopCardCalibrationRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

calibrationPurpose	Цель калибровки
vehicleIdentificationNumber	Идентификационный номер транспортного средства
vehicleRegistration	Идентификация регистрации транспортного средства
wVehicleCharacteristicConstant	Характеристическая константа W транспортного средства
kConstantOfRecordingEquipment	Константа K контрольного устройства
ITyreCircumference	Окружность шины L
tyreSize	Размер шины
authorisedSpeed	Разрешенная скорость
oldOdometerValue	Показания счетчика пробега
newOdometerValue	Показания счетчика пробега
oldTimeValue	Реальное время
newTimeValue	Реальное время
nextCalibrationDate	Реальное время
vuPartNumber	Номер детали БУ
vuSerialNumber	Серийный номер БУ
sensorSerialNumber	Серийный номер датчика движения
sensorGNSSSerialNumber	Серийный номер датчика ГНСС
rcmSerialNumber	Серийный номер модуля удаленной связи
sealDataCard	Данные, касающиеся пломб, указанных на карточке
}	

В дополнение к поколению 1 используются следующие элементы данных:

SensorGNSSSerialNumber — он позволяет идентифицировать внешнее устройство ГНСС.

rcmSerialNumber — он позволяет идентифицировать модуль удаленной связи.

sealDataCard содержит информацию о пломбах, которые наложены на различные компоненты транспортного средства.

2.237 **WorkshopCardHolderIdentification (идентификация держателя карточки мастерской)**

Информация, записанная на карточке мастерской, которая относится к идентификации держателя карточки (~~приложение~~ **добавление 1С**, требования 311 и 334).

WorkshopCardHolderIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

workshopName	Название
workshopAddress	Адрес
cardHolderName	Название держателя
cardHolderPreferredLanguage	Язык

}

workshopName — название мастерской держателя карточки.

workshopAddress — адрес мастерской держателя карточки.

cardHolderName — фамилия и имя (имена) держателя (например, фамилия и имя техника).

cardHolderPreferredLanguage — предпочитаемый язык держателя карточки.

2.238 **WorkshopCardPIN (ПИН-код карточки мастерской)**

Персональный идентификационный номер карточки мастерской (~~приложение~~ **добавление 1С**, требования 309 и 332).

WorkshopCardPIN ::= СтрокаIA5(РАЗМЕР(8))

Присвоение значения: известный ПИН-код держателя карточки, за которым следует серия байтов 'FF' (до 8 байтов).

2.239 **W-VehicleCharacteristicConstant (характеристическая постоянная W транспортного средства)**

Характеристический коэффициент транспортного средства (определение k).

W-VehicleCharacteristicConstant ::= ЦЕЛОЕ ЧИСЛО(0..2¹⁶-1)

Присвоение значения: импульсы на километр в рабочем диапазоне от 0 до 64 255 имп./км.

2.240 **VuPowerSupplyInterruptionRecord (запись данных в БУ о прекращении электропитания)**

Поколение 2:

Информация, записанная в бортовом устройстве, связана с событиями прекращения электропитания (~~приложение~~ **добавление 1С**, требование 117).

VuPowerSupplyInterruptionRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

eventType	Событие: тип неисправности
eventRecordPurpose	Событие: цель регистрации неисправности
eventBeginTime	Реальное время
eventEndTime	Реальное время
cardNumberAndGenDriverSlotBegin	Полный номер и поколение карточки
cardNumberAndGenDriverSlotEnd	Полный номер и поколение карточки
cardNumberAndGenCodriverSlotBegin	Полный номер и поколение карточки
cardNumberAndGenCodriverSlotEnd	Полный номер и поколение карточки
similarEventsNumber	Число похожих событий
}	

eventType — тип события.

eventRecordPurpose — цель регистрации данного события.

eventBeginTime — дата и время начала события.

eventEndTime — дата и время завершения события.

cardNumberAndGenDriverSlotBegin — идентификатор карточки, вставленной в считывающее устройство водителя в начале события, и ее поколения.

cardNumberAndGenDriverSlotEnd — идентификатор карточки, вставленной в считывающее устройство водителя в конце события, и ее поколения.

cardNumberAndGenCodriverSlotBegin — идентификатор карточки, вставленной в считывающее устройство второго водителя в начале события, и ее поколения.

cardNumberAndGenCodriverSlotEnd — идентификатор карточки, вставленной в считывающее устройство второго водителя в конце события, и ее поколения.

similarEventsNumber — число похожих событий за указанный день.

2.241 VuPowerSupplyInterruptionRecordArray (запись данных в БУ о прекращении электропитания и метаданные)

Поколение 2:

Информация, записанная в бортовом устройстве, связана с событиями прекращения электропитания (~~приложение~~ **добавление** 1С, требование 117).

VuPowerSupplyInterruptionRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

recordType	Тип записи
recordSize	ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords	ЦЕЛОЕ ЧИСЛО(0..65535)
records	УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords) ПАРАМЕТРА VuPowerSupplyInterruptionRecord
}	

recordType обозначает тип записи (VuPowerSupplyInterruptionRecord).

Присвоение значения: см. RecordType

recordSize — размер записи VuPowerSupplyInterruptionRecord в байтах.

noOfRecords — число записей в совокупности записей.

records — совокупность записей событий, связанных с прекращением электропитания.

2.242 VuSensorExternalGNSSCoupledRecordArray (запись данных в БУ о соединении с внешним датчиком ГНСС и метаданные)

Поколение 2:

Набор записей SensorExternalGNSSCoupledRecord плюс метаданные, используемые в протоколе загрузки.

```
VuSensorExternalGNSSCoupledRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType                Тип записи
recordSize                ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords              ЦЕЛОЕ ЧИСЛО(0..65535)
records                  УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
                        ПАРАМЕТРА SensorExternalGNSSCoupledRecord
}
```

recordType обозначает тип записи (SensorExternalGNSSCoupledRecord).

Присвоение значения: см. RecordType.

recordSize — размер записи SensorExternalGNSSCoupledRecord в байтах.

noOfRecords — число записей в массиве.

records — совокупность записей SensorExternalGNSSCoupledRecords.

2.243 VuSensorPairedRecordArray (запись данных о спаренном датчике БУ и метаданные)

Поколение 2:

Набор записей SensorPairedRecord плюс метаданные, используемые в протоколе загрузки.

```
VuSensorPairedRecordArray ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
recordType                Тип записи
recordSize                ЦЕЛОЕ ЧИСЛО(1..65535)
noOfRecords              ЦЕЛОЕ ЧИСЛО(0..65535)
records                  УСТАНОВЛЕННЫЙ РАЗМЕР (noOfRecords)
                        ПАРАМЕТРА SensorPairedRecord
}
```

recordType обозначает тип записи (SensorPairedRecord).

Присвоение значения: см. RecordType.

recordSize — размер записи SensorPairedRecord в байтах.

noOfRecords — число записей в массиве.

records — совокупность записей по спаренным датчикам.

3. Определения диапазонов значений и размеров

Определение значений переменных, используемых для определений, содержащихся в пункте 2.

TimeRealRange ::= $2^{32}-1$

4. Наборы символов

В строках IA5 используются знаки ASCII, определенные в стандарте ISO/IEC 8824-1. Для удобочитаемости и простоты присвоенные значения приводятся ниже. В случае разночтений вместо этой информационной записки следует использовать стандарт ISO/IEC 8824-1.

! " # \$ % & ' () * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?

@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\] ^ _

` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~

Стандартный набор символов	Кодовая страница (десятичная)
ISO/IEC 8859-1 латинский-1 западноевропейский	1
ISO/IEC 8859-2 латинский-2 центральноевропейский	2
ISO/IEC 8859-3 латинский-3 южноевропейский	3
ISO/IEC 8859-5 латинский/кириллический	5
ISO/IEC 8859-7 латинский/греческий	7
ISO/IEC 8859-9 латинский-5 турецкий	9
ISO/IEC 8859-13 латинский-7 прибалтийский	13
ISO/IEC 8859-15 латинский-9	15
ISO/IEC 8859-16 латинский-10 юго-восточный европейский	16
KOI8-R латинский / кириллический	80
KOI8-R латинский/кириллический	85

5. Кодирование

В случае кодирования по правилам кодирования ASN.1 все определенные типы данных кодируются в соответствии со стандартом ISO/IEC 8825-2 (согласованный вариант).

6. Идентификаторы объектов и идентификаторы приложений

6.1 Идентификаторы объектов

Идентификаторы объектов (OID), указанные в настоящей главе, касаются только поколения 2. Эти идентификаторы объектов представлены в TR-03110-3 и повторяются здесь в интересах полноты. Они представлены в поддреже bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
itu-t(0) identified-organization(4) etsi(0)
reserved(127) etsi-identified-organization(0) 7
}
```

Идентификаторы протокола аутентификации БУ

```
id-TA      OBJECT IDENTIFIER ::= { bsi-de protocols(2) smartcard(2) 2 }
id-TA-ECDSA      OBJECT IDENTIFIER ::= { id-TA 2 }
id-TA-ECDSA-SHA-256      OBJECT IDENTIFIER ::= { id-TA -ECDSA 3 }
id-TA-ECDSA-SHA-384      OBJECT IDENTIFIER ::= { id-TA -ECDSA 4 }
id-TA-ECDSA-SHA-512      OBJECT IDENTIFIER ::= { id-TA -ECDSA 5 }
```

Пример: допустим, аутентификация БУ должна производиться при помощи SHA-384, тогда идентификатор объекта, который следует применить, — (в нотации ASN.1) bsi-de protocols(2) smartcard(2) 2 2 4. Значение данного идентификатора объекта в точечной нотации — 0.4.0.127.0.7.2.2.2.4.

	Точечная нотация	Байтовая нотация
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.3	'04 00 7F 00 07 02 02 02 03'
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.4	'04 00 7F 00 07 02 02 02 04'
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.5	'04 00 7F 00 07 02 02 02 05'

Идентификаторы протокола аутентификации чипов

```
id-CA      OBJECT IDENTIFIER ::= { bsi-de protocols(2) smartcard(2) 3 }
id-CA-ECDH      OBJECT IDENTIFIER ::= { id-CA 2 }
id-CA-ECDH-AES-CBC-CMAC-128      OBJECT IDENTIFIER ::= { id- CA-ECDH 2 }
id-CA-ECDH-AES-CBC-CMAC-192      OBJECT IDENTIFIER ::= { id- CA-ECDH 3 }
id-CA-ECDH-AES-CBC-CMAC-256      OBJECT IDENTIFIER ::= { id-CA-ECDH 4 }
```

Пример: допустим, аутентификация микросхемы производится при помощи алгоритма ECDH, в результате чего длина ключа сеанса AES составит 128 битов. Данный ключ сеанса впоследствии используется в рабочем режиме CBC с целью обеспечить конфиденциальность данных и с алгоритмом CMAC с целью обеспечить подлинность данных. Таким образом, идентификатор объекта, который следует применить в этом случае, будет иметь вид (в нотации ASN.1) bsi-de protocols(2) smartcard(2) 3 2 2. Значение данного идентификатора объекта в точечной нотации — 0.4.0.127.0.7.2.2.3.2.2.

	Точечная нотация	Байтовая нотация
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	'04 00 7F 00 07 02 02 03 02 02'
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	'04 00 7F 00 07 02 02 03 02 03'
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	'04 00 7F 00 07 02 02 03 02 04'

6.2 Идентификаторы приложения

Поколение 2:

Идентификатор приложения (AID) для внешнего устройства ГНСС (поколение 2) определяют по выражению 'FF 44 54 45 47 4D'. В соответствии с ISO/IEC 7816-4 это — патентованный AID.

Примечание: В случае внешнего устройства ГНСС для смарт-тахографов последние 5 байтов кодируют DTEGM.

Идентификатор приложения в случае приложения карточки тахографа второго поколения определяется по выражению 'FF 53 4D 52 44 54'. В соответствии с ISO/IEC 7816-4 это — патентованный AID.

Добавление Подраздел 2**Спецификация на карточки тахографов****Содержание**

	<i>Стр.</i>
1. Введение	247
1.1 Сокращения	247
1.2 Справочные материалы	248
2. Электрические и физические характеристики	248
2.1 Напряжение питания и потребление тока	249
2.2 Напряжение программирования V_{pp}	249
2.3 Формирование и частота тактовых сигналов	249
2.4 Контакт «вход/выход»	249
2.5 Статус карточки	249
3. Аппаратное обеспечение и передача данных	250
3.1 Введение	250
3.2 Протокол передачи данных	250
3.2.1 Протоколы	250
3.2.2 ATR	251
3.2.3 PTS	251
3.3 Правила доступа	252
3.4 Обзор команд и кодов ошибок	255
3.5 Описания команд	257
3.5.1 Select (выбор)	244
3.5.2 Read Binary (считывание данных)	259
3.5.3 Update Binary (обновление данных)	267
3.5.4 Get Challenge (получение запроса)	272
3.5.5 Verify (проверка)	273
3.5.6 Get Response (получение ответа)	275
3.5.7 PSO: Verify Certificate (проверка сертификата)	275
3.5.8 Internal Authenticate (внутренняя аутентификация)	278
3.5.9 External Authenticate (внешняя аутентификация)	279
3.5.10 General Authenticate (общая аутентификация)	280
3.5.11 Manage Security Environment (управление средой защиты)	281
3.5.12 PSO: Hash (хеширование)	285
3.5.13 Perform Hash of File (хеширование файла)	286
3.5.14 PSO: Compute Digital Signature (расчет цифровой подписи)	288
3.5.15 PSO: Verify Digital Signature (проверка цифровой подписи)	289
3.5.16 Обработка сообщения DSRC	290

4.	Структура карточек тахографов	292
4.1	Главный файл MF	292
4.2	Приложения карточки водителя	294
4.2.1	Приложение карточки водителя поколения 1	294
4.2.2	Приложение карточки водителя поколения 2	297
4.3	Приложения карточки мастерской	302
4.3.1	Приложение карточки мастерской поколения 1	302
4.3.2	Приложение карточки мастерской поколения 2	305
4.4.	Приложения контрольной карточки	315
4.4.1	Приложение контрольной карточки поколения 1	315
4.4.2	Приложение контрольной карточки поколения 2	316
4.5	Приложения карточки предприятия	304
4.5.1	Приложение карточки предприятия поколения 1	319
4.5.2	Приложение карточки предприятия поколения 2	320

1. Введение

1.1 Сокращения

В настоящем подразделе используются следующие сокращения:

AC	Условия доступа
AES	Расширенный стандарт шифрования
AID	Идентификатор приложения
ALW	Всегда
APDU	Блок данных прикладного протокола (структура команды)
ATR	Ответ на сигнал сброса
AUT	Аутентифицировано
C6, C7	Контакты № 6 и 7 карточки в соответствии с описанием в стандарте ISO/IEC 7816-2
cc	тактыые циклы
CHA	Полномочия держателя сертификата
CHV	Информация для проверки данных держателя карточки
CLA	Байт класса команды APDU
DSRC	Выделенная связь ближнего действия
DF	Выделенный файл. DF может содержать другие файлы (EF или DF)
DO	Объект данных
ECC	Эллиптическая криптография
EF	Элементарный файл
etu	эв (элементарная единица времени)
G1	Поколение 1
G2	Поколение 2
IC	Интегральная схема
ICC	Карточка на интегральной микросхеме
ID	Идентификатор
IFD	Интерфейс (устройство сопряжения)
IFS	Размер информационного поля
IFSC	Размер информационного поля для карточки
IFSD	Устройство регулирования размера информационного поля (для терминала)
INS	Байт класса команды APDU
Lc	Длина входных данных для команды APDU
Le	Длина ожидаемых данных (выходные данные команды)
MF	Главный файл (корневой DF)
NAD	Адрес узла, используемого в протоколе T=1
NEV	Никогда
P1-P2	Байты параметров

PIN	Персональный идентификационный номер
PRO SM	Криптозащищенное сообщение
PTS	Выбор протокола передачи
RFU	Зарезервировано для будущего использования
RST	Перезагрузка (карточки)
SFID	Короткий идентификатор EF
SM	Защищенный обмен сообщениями
SW1-SW2	Байты состояния
TS	Исходный символ ATR
VPP	Напряжение программирования
VU	БУ (бортовое устройство)
XXh	Значение XX в шестнадцатеричном счислении
'XXh'	Значение XX в шестнадцатеричном счислении
 	Символ конкатенации 03 04=0304

1.2 Справочные материалы

В настоящем **подразделе** ~~добавлении~~ используются следующие справочные материалы:

ISO/IEC 7816-2	Идентификационные карточки — карточки на интегральной микросхеме. Часть 2: размеры и расположение контактов. ISO/IEC 7816-2:2007.
ISO/IEC 7816-3	Идентификационные карточки — карточки на интегральной микросхеме. Часть 3: электрический интерфейс и протоколы передачи. ISO/IEC 7816-3:2006.
ISO/IEC 7816-4	Идентификационные карточки — карточки на интегральной микросхеме. Часть 4: организация, безопасность и команды обмена. ISO/IEC 7816-4:2013 + Cor 1: 2014.
ISO/IEC 7816-6	Идентификационные карточки — карточки на интегральной микросхеме. Часть 6: межсекторные элементы данных для обмена. ISO/IEC 7816-6:2004 + Cor 1: 2006.
ISO/IEC 7816-8	Идентификационные карточки — карточки на интегральной микросхеме. Часть 8: команды операций по обеспечению безопасности. ISO/IEC 7816-8:2004.
ISO/IEC 9797-2	Информационная технология — методы обеспечения безопасности. Коды аутентификации сообщений (MAC). Часть 2: механизмы с использованием функции хеширования. ISO/IEC 9797-2:2011

2. Электрические и физические характеристики

TCS_01	Все электронные сигналы соответствуют стандарту ISO/IEC 7816-3, если не указано иное.
TCS_02	Расположение и размеры контактов карточки соответствуют стандарту ISO/IEC 7816-2.

2.1 Напряжение питания и потребление тока

TCS_03 Карточка работает в соответствии со спецификациями в диапазоне предельных значений потребления, указанных в стандарте ISO/IEC 7816-3.

TCS_04 Карточка работает при $V_{cc} = 3 \text{ V} (\pm 0,3\text{V})$ или $V_{cc} = 5 \text{ V} (\pm 0,5 \text{ V})$.
Выбор напряжения производится в соответствии со стандартом ISO/IEC 7816-3.

2.2 Напряжение программирования V_{pp}

TCS_05 Карточка не требует напряжения программирования на выводе С6. Предполагается, что вывод С6 к IFD не подсоединяется. Контакт С6 может быть соединен с V_{cc} карточки, но не заземлен. В любом случае это напряжение интерпретации не подлежит.

2.3 Формирование и частота тактовых сигналов

TCS_06 Карточка работает в диапазоне частот 1–5 МГц и может поддерживать более высокие частоты. В пределах одного сеанса использования карточки тактовая частота может варьироваться в пределах $\pm 2 \%$. Тактовая частота генерируется бортовым устройством, а не самой карточкой. Рабочий цикл может варьироваться в пределах 40–60 %.

TCS_07 В соответствии с параметрами, заложенными в файле карточки EF ICC, внешние часы можно остановить. Первый байт основного файла EF ICC кодирует условия режима остановки часов:

<i>Низкий</i>		<i>Высокий</i>		
Бит 3	Бит 2	Бит 1		
0	0	1	Остановка часов допускается; предпочтительный уровень не предусмотрен	
0	1	1	Остановка часов допускается; предпочтителен высокий уровень	
1	0	1	Остановка часов допускается; предпочтителен низкий уровень	
0	0	0	Остановка часов не допускается	
0	1	0	Остановка часов допускается только на высоком уровне	
1	0	0	Остановка часов допускается только на низком уровне	

Биты 4–8 не используются.

2.4 Контакт «вход/выход»

TCS_08 Контакт «вход/выход» С7 используется для получения данных из IFD и передачи данных в IFD. Во время работы в режиме передачи может находиться только карточка или только IFD. В том случае, если оба устройства работают в режиме передачи, карточка повреждена не будет. Если передача данных с карточки не производится, она переключается в режим приема.

2.5 Состояние карточки

TCS_09 В случае подачи на карточку напряжения она может находиться в двух состояниях:

в рабочем состоянии при выполнении команд или обмене данными с ~~цифровым блоком~~ **бортовым устройством;**

в остальное время — в состоянии простоя; в этом состоянии все данные остаются на карточке.

3. Аппаратное обеспечение и передача данных

3.1 Введение

В настоящем пункте излагаются минимальные требования к функциям карточек тахографа и БУ в целях обеспечения правильной работы и эксплуатационной совместимости.

Карточки тахографа в максимальной степени соответствуют применимым нормам стандарта ISO/IEC (прежде всего ISO/IEC 7816). Однако в целях уточнения некоторых ограниченных видов использования или различий, в случае их наличия, характеристики всех команд и протоколов указываются полностью. Указанные команды полностью соответствуют упомянутым выше стандартам, если не оговорено иное.

3.2 Протокол передачи данных

TCS_10 Протокол передачи данных соответствует ISO/IEC 7816-3 при $T = 0$ и $T = 1$. В частности, БУ должно распознавать сигналы продления времени ожидания, передаваемые карточкой.

3.2.1 Протоколы

TCS_11 Карточка поддерживает как протокол $T = 0$, так и протокол $T = 1$. Кроме того, карточка может поддерживать дополнительные протоколы, ориентированные на контакты.

TCS_12 $T = 0$ — протокол по умолчанию, поэтому для изменения протокола на $T = 1$ нужна команда **PTS**.

TCS_13 Устройства поддерживают прямую связь в обоих протоколах: таким образом, прямая связь для карточки обязательна.

TCS_14 Байт **карточки регулирования размера информационного поля** в ATR представлен символами TA3. Это значение составляет не менее 'F0h' (=240 байтов).

К протоколам применяются следующие ограничения.

TCS_15 $T = 0$

- Интерфейс принимает ответ на входе и выходе после нарастания сигнала на RST начиная с 400 ээв.
- Интерфейс способен считывать символы, отделенные во времени на 12 ээв.
- Интерфейс распознает ошибочные символы и их повторение, если они разделены во времени на 13 ээв. В случае обнаружения ошибочного символа контакт ввода/вывода может отражать сигнал ошибки в интервале 1–2 ээв. Это устройство реагирует на задержку продолжительностью 1 ээв.
- Интерфейс принимает ATR размером 33 байта (TS+32).
- Если в ATR есть TC1, то для символов, передаваемых интерфейсом, должно быть предусмотрено дополнительное время хранения, хотя временной интервал между символами, посылаемыми карточкой, может и в этом случае составлять 12 ээв. Это также применимо к символу AСК, посылаемому карточкой после передачи символа P3 интерфейсом.
- Интерфейс принимает символ NUL, передаваемый карточкой.
- Интерфейс поддерживает дополнительный режим для AСК.
- Команда на получение ответа не может использоваться в режиме прямого вывода для получения данных, длина которых может превышать 255 байтов.

TCS_16 **T=1**

- Байт NAD: не используется (NAD устанавливается на '00').
- S-блок ABORT: не используется.
- S-блок VPP индикации ошибки: не используется.
- ~~Общая длина цепочки вывода данных для поля данных не превышает 255 байтов (обеспечивается IFD).~~
- Размер информационного поля для интерфейса (IFSD) указывается IFD сразу же после ATR: IFD передает запрос на S-блок IFS после ATR, после чего карточка передает обратно данные S-блока IFS. Рекомендуемое значение для IFSD: 254 байта.
- Карточка не требует корректировки IFS.

3.2.2 **ATR**

TCS_17 Устройство проверяет байты ATR в соответствии со стандартом ISO/IEC 7816-3. Проверка архивных символов ATR не производится.

Архивные символы

Пример базового двойного протокола ATR согласно ISO/IEC 7816-3

<i>Буква</i>	<i>Значение</i>	<i>Примечания</i>
TS	'3Bh'	Указывает на прямое соглашение
T0	'85h'	TD1 присутствует; 5 архивных байтов присутствуют
TD1	'80h'	TD2 присутствует; T=0 подлежит использованию
TD2	'11h'	TA3 присутствует; T=1 подлежит использованию
TA3	'XXh' (не менее 'F0h')	Размер информационного поля карточки (IFSC)
TH1–TH5	'XXh'	Архивные символы
TCK	'XXh'	Проверочный знак (исключительно OR)

TCS_18 После ответа на сигнал перезагрузки (ATR) выбирается по косвенным признакам главный файл (MF), который становится текущей директорией.

3.2.3 **PTS**

TCS_19 Протоколом по умолчанию является T=0. Для перехода на протокол T=1 на карточку необходимо передать сигнал PTS (также обозначаемый в виде PPS).

TCS_20 Поскольку для карточки оба протокола T=0 и T=1 обязательны, базовый сигнал PTS для перехода с одного протокола на другой обязателен и для карточки.

PTS может использоваться, как указано в стандарте ISO/IEC 7816-3, для перехода на более высокие скорости передачи данных в бодах, чем скорость по умолчанию, предлагаемая в соответствующих случаях карточкой в ATR (байт (TA(1))).

Более высокие скорости передачи в бодах для карточки факультативны.

TCS_21 Если другая скорость передачи в бодах, помимо скорости по умолчанию, не поддерживается (или если не поддерживается выбранная скорость передачи в бодах), карточка передает правильную команду PTS в соответствии со стандартом ISO/IEC 7816-3, опустив байт PPS1.

Примеры базовой команды PTS для выбора протокола указаны ниже:

Символ	Значение	Примечания
PPSS	'FFh'	Начальный знак
PPS0	'00h' или '01h'	PPS1–PPS3 не присутствуют; '00h' для выбора T0, '01h' для выбора T1
PK	'XXh'	Проверка знака: 'XXh' = 'FFh', если PPS0 = '00h', 'XXh' = 'FEh', если PPS0 = '01h'

3.3 Правила доступа

TCS_22 Правило доступа указывает режим доступа, т. е. команду, и соответствующие условия обеспечения безопасности. Если эти условия соблюдены, обрабатывается соответствующая команда.

TCS_23 Для карточки тахографа применяются следующие условия безопасности:

Сокращение	Значение
ALW	Действие возможно во всех случаях и может быть выполнено без каких бы то ни было ограничений. Команда и ответ APDU отправляются открытым текстом, т. е. без защищенного обмена сообщениями
NEV	Действие невозможно ни в каких случаях
PLAIN-C	Команда и ответ APDU отправляются открытым текстом, т. е. без защищенного обмена сообщениями
PWD	Действие может быть выполнено только в том случае, если PIN-код карточки мастерской был успешно проверен, т. е. если внутренний статус безопасности карточки установлен на «PIN_Verified». Эта команда отправляется открытым текстом без защищенного обмена сообщениями
EXT-AUT-G1	Это действие может быть выполнено только в том случае, если успешно выполнена команда External Authenticate для аутентификации поколения 1 (см. также приложение подраздел 11, часть A)
SM-MAC-G1	APDU (команда и ответ) должны применяться в условиях безопасного обмена сообщениями поколения 1 в режиме только аутентификации (см. приложение подраздел 11, часть A)
SM- C-MAC-G1	Команда APDU должна использоваться в условиях безопасного обмена сообщениями поколения 1 в режиме только аутентификации (см. приложение подраздел 11, часть A)
SM-R-ENC-G1	Ответ APDU должен применяться в условиях безопасного обмена сообщениями поколения 1 в режиме шифрования (см. приложение подраздел 11, часть A), т. е. без возвращения кода аутентификации сообщения

Сокращение	Значение
SM-R-ENC-MAC-G1	Ответ APDU должен применяться в условиях безопасного обмена сообщениями поколения 1 в режиме шифрования и последующей аутентификации (см. приложение подраздел 11, часть А)
SM-MAC-G2	APDU (команда и ответ) должны применяться в условиях безопасного обмена сообщениями поколения 2 в режиме только аутентификации (см. приложение подраздел 11, часть В)
SM-C-MAC-G2	Команда APDU должна применяться в условиях безопасного обмена сообщениями поколения 2 в режиме только аутентификации (см. приложение подраздел 11, часть В)
SM-R-ENC-MAC-G2	Ответ APDU должен применяться в условиях безопасного обмена сообщениями поколения 2 в режиме шифрования и последующей аутентификации (см. приложение подраздел 11, часть В)

TCS_24 Данные условия обеспечения безопасности могут быть увязаны следующими способами:

И: Должны быть выполнены все условия безопасности

ИЛИ: Должно быть выполнено хотя бы одно условие безопасности

Правила доступа к системе файлов, т. е. команды SELECT, READ BINARY и UPDATE BINARY, представлены в главе 4. Правила доступа для остальных команд представлены в таблицах ниже. **Термин «неприменимо» используется, если поддерживать команду нет необходимости. В этом случае команда может поддерживаться или не поддерживаться, но условие доступа неприменимо.**

TCS_25 В случае приложения DF Tachograph G1 соблюдаются следующие правила доступа:

Команда	Карточка водителя	Карточка мастерской	Карточка контролера	Карточка предприятия
Внешняя аутентификация				
• Аутентификация в случае поколения 1	ALW	ALW	ALW	ALW
• Аутентификация в случае поколения 2	ALW	PWD	ALW	ALW
Внутренняя аутентификация	ALW	PWD	ALW	ALW
Общая аутентификация	ALW	ALW	ALW	ALW
Получение запроса	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Обработка сообщения DSRC	неприменимо	неприменимо	неприменимо	неприменимо
PSO: расчет цифровой подписи	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	неприменимо	неприменимо
PSO: хеширование	неприменимо	неприменимо	ALW	неприменимо
ХЕШИРОВАНИЕ ФАЙЛА	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	неприменимо	неприменимо
PSO: проверка сертификата	ALW	ALW	ALW	ALW
PSO: проверка цифровой подписи	неприменимо	неприменимо	ALW	неприменимо
Проверка	неприменимо	ALW	неприменимо	неприменимо

TCS_26 В приложении DF Tachograph_G2 используются следующие правила доступа:

Команда	Карточка водителя	Карточка мастерской	Карточка контролера	Карточка предприятия
Внешняя аутентификация				
• Аутентификация для поколения 1	неприменимо	неприменимо	неприменимо	неприменимо
• Аутентификация для поколения 2	ALW	PWD	ALW	ALW
Внутренняя аутентификация	неприменимо	неприменимо	неприменимо	неприменимо
Общая аутентификация	ALW	ALW	ALW	ALW
Получение запроса	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Обработка сообщения DSRC	неприменимо	ALW	ALW	неприменимо
PSO: расчет цифровой подписи	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	неприменимо	неприменимо
PSO: хеширование	неприменимо	неприменимо	ALW	неприменимо
ХЕШИРОВАНИЕ ФАЙЛА	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	неприменимо	неприменимо
PSO: проверка сертификата	ALW	ALW	ALW	ALW
PSO: проверка цифровой подписи	неприменимо	неприменимо	ALW	неприменимо
Проверка	неприменимо	ALW	неприменимо	неприменимо

TCS_27 В случае MF соблюдаются следующие правила доступа:

Команда	Карточка водителя	Карточка мастерской	Карточка контролера	Карточка предприятия
Внешняя аутентификация				
• Аутентификация в случае поколения 1	неприменимо	неприменимо	неприменимо	неприменимо
• Аутентификация в случае поколения 2	ALW	PWD	ALW	ALW
Внутренняя аутентификация	неприменимо	неприменимо	неприменимо	неприменимо
Общая аутентификация	ALW	ALW	ALW	ALW
Получение запроса	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Обработка сообщения DSRC	неприменимо	неприменимо	неприменимо	неприменимо
PSO: расчет цифровой подписи	неприменимо	неприменимо	неприменимо	неприменимо
PSO: хеширование	неприменимо	неприменимо	неприменимо	неприменимо
ВЫПОЛНИТЬ ХЕШИРОВАНИЕ ФАЙЛА PSO: хеширование файла	неприменимо	неприменимо	неприменимо	неприменимо
PSO: проверка сертификата	ALW	ALW	ALW	ALW
PSO: проверка цифровой подписи	неприменимо	неприменимо	неприменимо	неприменимо
Проверка	неприменимо	ALW	неприменимо	неприменимо

TCS_28 Карточка тахографа может принимать или не принимать команду с более высоким уровнем защиты, чем тот, который указан в условиях

безопасности. Например, если условием безопасности является ALW (или PLAIN-C), то карточка может принять команду в условиях защищенного обмена сообщениями (режим шифрования и/или аутентификации). Если по условию безопасности требуется защищенный обмен сообщениями в режиме аутентификации, то карточка тахографа может принять команду в условиях защищенного обмена сообщениями того же поколения в режиме аутентификации и шифрования.

Примечание: Описания команд предлагают более подробную информацию о поддержке команд различными типами карточек тахографов и различными DF.

3.4 Обзор команд и кодов ошибок

Команды и организация файлов определяются стандартом ISO/IEC 7816-4 и соответствуют ему.

В настоящем разделе описаны следующие пары команд и ответов APDU. Варианты команд, которые поддерживает приложение поколений 1 и 2, представлены в соответствующих описаниях команд.

<i>Команда</i>	<i>ИНС</i>
SELECT (ВЫБОР)	'A4h'
READ BINARY (СЧИТЫВАНИЕ ДАННЫХ)	'B0h', 'B1h'
UPDATE BINARY (ОБНОВЛЕНИЕ ДАННЫХ)	'D6h', 'D7h'
GET CHALLENGE (ПОЛУЧЕНИЕ ЗАПРОСА)	'84h'
VERIFY (ПРОВЕРКА)	'20h'
GET RESPONSE (ПОЛУЧЕНИЕ ОТВЕТА)	'C0h'
PERFORM SECURITY OPERATION (ВЫПОЛНИТЬ ОПЕРАЦИЮ ПО ЗАЩИТЕ)	'2Ah'
– VERIFY CERTIFICATE (ПРОВЕРКА СЕРТИФИКАТА)	
– COMPUTE DIGITAL SIGNATURE (РАСЧЕТ ЦИФРОВОЙ ПОДПИСИ)	
– VERIFY DIGITAL SIGNATURE (ПРОВЕРКА ЦИФРОВОЙ ПОДПИСИ)	
– HASH (ХЕШИРОВАНИЕ)	
– PERFORM HASH OF FILE (ХЕШИРОВАНИЕ ФАЙЛА)	
– DSRC PROCESS DSRC MESSAGE (ОБРАБОТКА СООБЩЕНИЯ)	
INTERNAL AUTHENTICATE (ВНУТРЕННЯЯ АУТЕНТИФИКАЦИЯ)	'88h'
EXTERNAL AUTHENTICATE (ВНЕШНЯЯ АУТЕНТИФИКАЦИЯ)	'82h'
MANAGE SECURITY ENVIRONMENT (УПРАВЛЕНИЕ СРЕДОЙ ЗАЩИТЫ)	'22h'
• SET DIGITAL SIGNATURE TEMPLATE (УСТАНОВКА ШАБЛОНА ЦИФРОВОЙ ПОДПИСИ)	
• SET AUTHENTICATION TEMPLATE (УСТАНОВКА ШАБЛОНА АУТЕНТИФИКАЦИИ)	
GENERAL AUTHENTICATE (ОБЩАЯ АУТЕНТИФИКАЦИЯ)	'86h'

TCS_29 Метки статуса SW1 SW2 возвращаются в любом ответном сообщении и обозначают состояние обработки команды.

<i>SW1</i>	<i>SW2</i>	<i>Значение</i>
90	00	Нормальная обработка
61	XX	Нормальная обработка. XX = количество доступных байтов ответа

<i>SW1</i>	<i>SW2</i>	<i>Значение</i>
62	81	Обработка предупреждения. Часть передаваемых обратно данных может быть повреждена
63	00	Аутентификация не прошла (Предупреждение)
63	CX	Неправильный код CHV (PIN). Счетчик оставшихся попыток указывается с помощью 'X'
64	00	Ошибка исполнения — состояние постоянной памяти не изменилось. Ошибка целостности
65	00	Ошибка исполнения — состояние постоянной памяти изменилось.
65	81	Ошибка исполнения — состояние постоянной памяти изменилось — отказ памяти
66	88	Ошибка защиты: неправильная криптографическая контрольная сумма (во время криптозащищенного обмена сообщениями) или неправильный сертификат (во время проверки сертификата) или неправильная криптограмма (во время внешней аутентификации) или неправильная подпись (во время проверки подписи)
67	00	Неправильная длина (неправильные значения Lc или Le) 68 82 Безопасный обмен сообщениями не поддерживается
68	83	Последняя команда последовательности ожидается
69	00	Запрещенная команда (отсутствие ответа: T = 0)
69	82	Статус защиты неприемлем
69	83	Метод аутентификации заблокирован
69	85	Условия использования не удовлетворены
69	86	Команда не разрешена (текущий файл EF отсутствует)
69	87	Отсутствие ожидаемых криптозащищенных объектов данных
69	88	Неправильные криптозащищенные объекты данных
6A	80	Неправильные параметры в поле данных
6A	82	Файл не найден
6A	86	Неправильные параметры P1-P2
6A	88	Исходные данные не найдены
6B	00	Неправильные параметры (выход за пределы EF)
6C	XX	Неправильная длина, SW2 указывает правильную длину. Поле данных не выдается
6D	00	Командный код не поддерживается или недействителен
6E	00	Класс не поддерживается
6F	00	Другие контрольные ошибки

Дополнительные характеристики состояния, определенные в ISO/IEC 7816-4, могут быть возвращены, если их поведение в данном подразделе четко не указано.

Например, следующие определители состояния могут быть возвращены в произвольном порядке:

6881: Логический канал не поддерживается

6882: Безопасный обмен сообщениями не поддерживается

TCS_30 Если выполняется более чем одно условие ошибки в одной команде APDU, то карточка может выдать любое из соответствующих состояний.

3.5 Описания команд

В настоящей главе описываются параметры обязательных команд для карточек тахографа.

Дополнительные соответствующие данные, относящиеся к криптографическим операциям, представлены в ~~приложении~~ **подразделе 11** «Общие механизмы защиты» для тахографов поколения 1 и поколения 2.

Все команды описываются независимо от используемого протокола (T=0 или T=1). Байты APDU: CLA, INS, P1, P2, Lc и Le указываются всегда. Если байты Lc или Le для данной команды не нужны, то относящиеся к ней параметры длины, значения и описания не заполняются.

TCS_31 Если запрашиваются оба байта длины (Lc и Le), то описываемая команда должна разделяться на две части; если IFD использует протокол T=0 : IFD передает команду, описанную с помощью данных P3=Lc + данные, после чего направляет команду GET_RESPONSE (см. пункт **3.5.6**) с P3 = Le.

TCS_32 Если запрашиваются оба байта длины и если Le=0 (защищенный обмен сообщениями):

- В случае использования протокола T=1 карточка выдает Le=0, передавая все имеющиеся выходные данные.
- Если используется протокол T=0, то IFD передает первую команду с P3=Lc + данные, а карточка передает ответ (на это имплицитное значение Le=0) с помощью байтов состояния '**61La**', где La — число байтов, имеющихся для ответа. После этого IFD генерирует команду GET REPONSE с P3 = La для считывания этих данных.

TCS_33 Карточка тахографа может поддерживать, в соответствии с ISO/IEC 7816-4, поля расширенной длины соответствующей факультативной функции. Карточка тахографа, поддерживающая поля расширенной длины:

- указывает на поддержку полей расширенной длины в ATR;
- обеспечивает поддерживаемые размеры буфера с помощью информации расширенной длины в EF ATR/INFO; см. **TCS_146**;
- указывает, поддерживает ли она поля расширенной длины для T = 1 и/или T = 0 в EF расширенной длины; см. **TCS_147**;
- поддерживает поля расширенной длины для приложений тахографов первого и второго поколений.

Примечания:

Все команды указываются для полей короткой длины. Применение APDU расширенной длины разъясняется в ISO/IEC 7816-4.

В целом, команды указываются в режиме простого текста, т. е. без защищенного обмена сообщениями, поскольку уровень защищенного обмена сообщениями описан

в ~~приложении~~ подразделе 11. Правила доступа к той или иной команде однозначно показывают, поддерживает ли данная команда защищенный обмен сообщениями или нет и поддерживает ли данная команда защищенный обмен сообщениями первого и/или второго поколений. Некоторые варианты команды описываются в режиме защищенного обмена сообщениями с целью проиллюстрировать применение именно защищенного обмена сообщениями.

TCS_34 БУ полностью выполняет протокол взаимной аутентификации БУ и карточки поколения 2 во время того или иного сеанса использования карточки, включая проверку сертификата (если требуется) в DF Tachograph, DF Tachograph_G2 или MF.

3.5.1 SELECT (ВЫБОР)

Данная команда соответствует стандарту ISO/IEC 7816-4, однако ее использование ограничено по сравнению с командой, определенной в указанном стандарте.

Команда SELECT используется:

- для выбора приложения DF (должен использоваться выбор по названию);
- для выбора элементарного файла, соответствующего представленному ID файла.

3.5.1.1 Выбор по названию (AID)

Данная команда позволяет выбрать приложение DF на карточке.

TCS_35 Данная команда может быть выполнена из любой точки структуры файла (после ATR или в любое время).

TCS_36 Выбор приложения приводит к перезагрузке текущей среды защиты. После выбора приложения текущий открытый ключ больше не выбирается. Условие доступа EXT-AUT-G1 также теряется. Если команда выполняется без защищенного обмена сообщениями, то ключи предыдущего сеанса защищенного обмена сообщениями больше не доступны.

TCS_37 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Выбор по названию (AID)
P2	1	'0Ch'	Ответ не ожидается
Lc	1	'NNh'	Количество байтов, отправленных на карточку (длина AID): '06h' для приложения тахографа
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' для приложения тахографа поколения 1 AID: 'FF 53 4D 52 44 54' для приложения тахографа поколения 2

Ответ на команду SELECT не требуется (в случае T = 1 Lc отсутствует, а в случае T = 0 запрос на ответ не передается).

TCS_38 Ответное сообщение (запрос на ответ не требуется)

<i>Байт</i>	<i>Длина</i>	<i>Значение</i>	<i>Описание</i>
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)
<ul style="list-style-type: none"> ◆ Если команда проходит, карточка выдает '9000'. ◆ Если приложение, соответствующее AID, не найдено, статус обработки выдается в виде '6A82'. ◆ В случае T=1, если присутствует байт Le, состояние выдается в виде '6700'. ◆ В случае T=0, если запрос на ответ поступает после команды SELECT, статус выдается в виде '6900'. ◆ Если выбранное приложение считается поврежденным (в атрибутах файла обнаружена ошибка целостности), статус обработки выдается в виде '6400' или 6584 '6500'. 			

3.5.1.2 Выбор элементарного файла с использованием идентификатора файла**TCS_39 Командное сообщение**

TCS_40 Карточка тахографа поддерживает защищенный обмен сообщениями второго поколения, как указано в части В подраздела 11 для данного варианта команды.

<i>Байт</i>	<i>Длина</i>	<i>Значение</i>	<i>Описание</i>
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Выбор EF в соответствии с действующим DF
P2	1	'0Ch'	Ответ не ожидается
Le	1	'02h'	Количество байтов, отправленных на карту
#6-#7	2	'XXXXh'	Идентификатор файла

Ответ на команду SELECT не требуется (в случае T = 1 Le отсутствует, а в случае T = 0 запрос на ответ не передается).

TCS_41 Ответное сообщение (запроса на ответ нет)

<i>Байт</i>	<i>Длина</i>	<i>Значение</i>	<i>Описание</i>
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)
<ul style="list-style-type: none"> ◆ Если команда проходит, карточка выдает '9000'. ◆ Если файл, соответствующий идентификатору файла, не найден, то статус обработки выдается в виде '6A82'. ◆ При T=1, если присутствует байт Le, состояние выдается в виде '6700'. ◆ При T=0, если запрос на ответ поступает после команды SELECT, статус выдается в виде '6900'. ◆ Если выбранный файл считается поврежденным (в атрибутах файла обнаружена ошибка целостности), статус обработки выдается в виде '6400' или 6584 '6500'. 			

3.5.2 READ BINARY (СЧИТЫВАНИЕ ДАННЫХ)

Данная команда соответствует стандарту ISO/IEC 7816-4, однако ее использование ограничено по сравнению с командой, определенной в указанном стандарте.

Команда READ BINARY используется для считывания данных с прозрачного файла.

Ответ карточки сводится к обратной передаче считанных данных, которые могут быть включены в структуру защищенного обмена сообщениями.

3.5.2.1 Команда со смещением в P1-P2

Эта команда позволяет IFD считывать данные с выбранного в данный момент файла EF в незащищенном виде.

Примечание: Данная команда без защищенного обмена сообщениями может использоваться только для считывания файла, который поддерживает условие безопасности ALW для режима доступа Read.

TCS_42 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'B0h'	Считывание данных
P1	1	'XXh'	Смещение байтов с начала файла: байт самого старшего разряда
P2	1	'XXh'	Смещение байтов с начала файла: байт самого младшего разряда
Le	1	'XXh'	Ожидается указание длины данных. Число байтов, подлежащих извлечению.

Примечание: Бит 8 байта P1 должен быть установлен на 0.

TCS_43 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#X	X	'XX..XXh'	Считывание данных
SW	2	'XXXXh'	Характеристики состояния (SW1,SW2)

- ◆ Если команда проходит, карточка выдает '9000'.
- ◆ Если EF не выбран, статус обработки выдается в виде '6986'.
- ◆ Если условия защиты выбранного файла не удовлетворены, команда прерывается с выдачей '6982'.
- ◆ Если смещение не соответствует размеру EF (смещение > размера EF), то статус обработки выдается в виде '6B00'.
- ◆ Если размер данных, подлежащих извлечению, не соответствует размеру EF (смещение + Le > размера EF), то статус обработки выдается в виде '6700' или '6Cxx', где 'xx' указывает точную длину.
- ◆ Если в атрибутах файла обнаружена ошибка целостности, то карточка считает файл поврежденным и не подлежащим восстановлению, и статус обработки выдается в виде '6400' или '6581-6500'.
- ◆ Если в хранящихся данных обнаружена ошибка целостности, карточка выдает требуемые данные, и статус обработки выдается в виде '6281'.

3.5.2.1.1 Команда с защищенным обменом сообщениями (примеры)

Данная команда позволяет IFD считывать данные из EF, выбранного для защищенного обмена сообщениями, с целью проверить целостность получаемых данных и обеспечить их конфиденциальность в случае применения условия безопасности SM-R-ENC-MAC-G1 (поколение 1) или SM-R-ENC-MAC-G2 (поколение 2).

TCS_44 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'0Ch'	Запрос на защищенный обмен сообщениями
INS	1	'B0h'	Считывание данных
P1	1	'XXh'	P1 (смещение байтов с начала файла): байт самого старшего разряда
P2	1	'XXh'	P2 (смещение байтов с начала файла): Значащий байт самого младшего разряда
Lc	1	'XXh'	Длина входных данных для безопасного обмена сообщениями
#6	1	'97h'	T _{LE} : метка, указывающая спецификацию на ожидаемую длину
#7	1	'01h'	L _{LE} : Длина ожидаемой длины
#8	1	'NNh'	Спецификация ожидаемой длины (изначальная длина L _c): число байтов, подлежащих считыванию
#9	1	'8Eh'	T _{CC} : Метка для криптографической контрольной суммы
#10	1	'XXh'	L _{CC} : Длина следующей криптографической контрольной суммы '04h' для безопасного обмена сообщениями поколения 1 (см. приложение подраздел 11, часть А) '08h', '0Ch' или '10h' в зависимости от длины ключа AES для безопасного обмена сообщениями поколения 2 (см. приложение подраздел 11, часть В)
#11-#(10+L)	L	'XX..XXh'	Криптографическая контрольная сумма
L _c	1	'00h'	Как указано в стандарте ISO/IEC 7816-4

TCS_45 Ответное сообщение, если не требуется SM-R-ENC-MAC-G1 (поколение 1)/SM-R-ENC-MAC-G2 (поколение 2) и если формат ввода защищенного обмена сообщениями правильный:

Байт	Длина	Значение	Описание
#1	1	'81h'	T _{RV} : метка, указывающая значение обычных данных
#2	L	'NNh' или '81 NNh'	L _{RV} : длина переданных обратно данных (=изначальной длине L _c) L равен 2 байтам, если L _{RV} > 127 байтов
#(2+L)- #(1+L+NN)	NN	'XX..XXh'	Значения обычных данных
#(2+L+NN)	1	'99h'	Метка статуса обработки (SW1-SW2) — факультативно для безопасного обмена сообщениями поколения 1
#3+L+NN)	1	'02h'	Длина статуса обработки — факультативно для безопасного обмена сообщениями поколения 1
#4+L+NN)- #(5+L+NN)	2	'XX..XXh'	Статус обработки незащищенного ответа APDU — факультативно для безопасного обмена сообщениями поколения 1
#(6+L+NN)	1	'8Eh'	T _{CC} : Метка для криптографической контрольной суммы

Байт	Длина	Значение	Описание
#(7+L+NN)	1	'XXh'	LCC: Длина следующей криптографической контрольной суммы '04h' для безопасного обмена сообщениями поколения 1 (см. приложение подраздел 11, часть А) '08h', '0Ch' или '10h' в зависимости от длины ключа AES для безопасного обмена сообщениями поколения 2 (см. приложение подраздел 11, часть В)
#(8+L+NN)- #(7+M+L+NN)	M	'XX..XXh'	Криптографическая контрольная сумма
SW	2	'XXXXh'	Характеристики состояния (SW1,SW2)

TCS_46 Ответное сообщение, если требуется SM-R-ENC-MAC-G1 (поколение 1)/ SM-R-ENC-MAC-G2 (поколение 2) и если формат ввода защищенного обмена сообщениями правильный:

Байт	Длина	Значение	Описание
#1	1	'87h'	T_{PCG} : Метка для зашифрованных данных (криптограмма)
#2	L	'MMh' или '81 MMh'	L_{PCG} : длина выданных зашифрованных данных (отличная от изначальной длины L_e команды, что обусловлено заполнением) L составляет 2 байта, если $L_{PCG} > 127$ байтов
#(2+L)- #(1+L+MM)	MM	'01XX..XXh'	Зашифрованные данные: показатель заполнения и криптограмма
#(2+L+MM)	1	'99h'	Метка статуса обработки (SW1-SW2) — факультативно для безопасного обмена сообщениями поколения 1
#3+L+MM)	1	'02h'	Длина статуса обработки — факультативно для безопасного обмена сообщениями поколения 1
#4+L+MM)- #(5+L+MM)	2	'XX..XXh'	Статус обработки незащищенного ответа APDU — факультативно для безопасного обмена сообщениями поколения 1
#(6+L+MM)	1	'8Eh'	TCC: Метка для криптографической контрольной суммы
#(7+L+MM)	1	'XXh'	LCC: Длина следующей криптографической контрольной суммы '04h' для безопасного обмена сообщениями поколения 1 (см. приложение подраздел 11, часть А) '08h', '0Ch' или '10h' в зависимости от длины ключа AES для безопасного обмена сообщениями поколения 2 (см. приложение подраздел 11, часть В)
#(8+L+MM)- #(7+N+L+MM)	N	'XX..XXh'	Криптографическая контрольная сумма
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- Команда READ BINARY может выдавать статусы регулярной обработки, перечисленные в **TCS_43** с меткой '99h', как описано в **TCS_59** с применением структуры ответов в режиме защищенного обмена сообщениями.

- Кроме того, могут иметь место некоторые ошибки, которые конкретно связаны с криптозащищенным обменом сообщениями. В этом случае данные о состоянии обработки просто возвращаются, не задействуя использованную структуру защиты данных:

TCS_47 Ответное сообщение, если формат ввода защищенного обмена данными неправильный

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если ключ текущего сеанса отсутствует, то статус обработки выдается в виде '6A88'. Это происходит либо по той причине, что ключ сеанса еще не создан, либо по той, что ключ сеанса больше недействителен (в этом случае IFD должен повторить процесс взаимной аутентификации в порядке генерации нового ключа сеанса).
- ◆ Если некоторые ожидаемые объекты данных (как указано выше) в формате криптозащищенного обмена данными отсутствуют, то состояние обработки выдается в виде '6987': эта ошибка возникает в том случае, если ожидаемая метка отсутствует или если основная часть команды составлена неправильно.
- ◆ Если некоторые объекты данных неправильны, то состояние обработки выдается в виде '6988': эта ошибка возникает в том случае, если требуемые метки есть, но длина некоторых из них отличается от ожидаемой длины.
- ◆ Если проверка криптографической контрольной суммы показала неправильный результат, статус обработки выдается в виде '6688'.

3.5.2.2 Команда с коротким идентификатором EF (элементарного файла)

Данный вариант команды позволяет IFD выбирать EF при помощи короткого идентификатора EF и считывать данные из этого EF.

TCS_48 Карточка тахографа поддерживает данный вариант команды для всех элементарных файлов с соответствующим указанным коротким идентификатором EF. Такие короткие идентификаторы EF представлены в главе 0.

TCS_49 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'B0h'	Считывание данных
P1	1	'XXh'	Бит 8 устанавливается на 1 Биты 7 и 6 устанавливаются на 00 Биты 5–1 кодируют короткий идентификатор соответствующего EF
P2	1	'XXh'	Кодирует смещение с 0 до 255 байтов в EF, который указан в P1
Le	1	'XXh'	Ожидается указание длины данных. Число байтов, подлежащих отображению

Примечание: Короткие идентификаторы EF, используемые в тахографах поколения 2, указаны в главе 4.

Если P1 кодирует короткий идентификатор EF и если команда прошла, то идентифицированный EF становится в данный момент выбранным EF (текущий EF).

TCS_50 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#L	L	'XX..XXh'	Считывание данных
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда проходит, карточка выдает '9000'.
- ◆ Если файл, соответствующий идентификатору файла, не найден, то статус обработки выдается в виде '6A82'.
- ◆ Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей статуса '6982'.
- ◆ Если смещение не соответствует размеру EF (смещение > размера EF), то статус обработки выдается в виде '6B00'.
- ◆ Если размер данных, подлежащих считыванию, не соответствует размеру EF (смещение + Le > размера EF), то статус обработки выдается в виде '6700' или '6Схх', где 'хх' указывает точную длину.
- ◆ Если в атрибутах файла обнаружена ошибка целостности, то карточка считает файл поврежденным и не подлежащим восстановлению, и статус обработки выдается в виде '6400' или '6581' '6500'.
- ◆ Если в хранящихся данных обнаружена ошибка целостности, то карточка выдает требуемые данные, и статус обработки выдается в виде '6281'.

3.5.2.3 Команда с нечетным командным байтом

Данный вариант команды позволяет IFD считывать данные с EF размером 32768 байтов или более.

TCS_51 Карточка тахографа, которая поддерживает EF размером 32 768 байтов или более, поддерживает и данный вариант команды для этих файлов EF. Карточка тахографа может поддерживать или не поддерживать данный вариант команды для других EF, за исключением «EF Sensor_Installation_Data»; См. TCS_156 и TCS_160.

TCS_52 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'B1h'	Считывание данных
P1	1	'00h'	Текущий EF
P2	1	'00h'	
Lc	1	'NNh'	Lc — длина объекта данных со смещением.
#6-#(5+NN)	NN	'XX..XXh'	Объект данных со смещением: Метка '54h' Длина '01h' или '02h' Смещение значения

Байт	Длина	Значение	Описание
Le	1	'XXh'	Как указано в стандарте ISO/IEC 7816-4

IFD кодирует длину объекта данных со смещением с минимальным возможным числом октетов, т. е. с помощью байта длины '01h' IFD кодирует смещение от 0 до 255, а с помощью байта длины '02h' — смещение от '256' до '65 535' байтов.

Если режим защищенного обмена сообщениями не применяется, то в случае $T = 0$ карточка принимает значение $Le = '00h'$.

Если $Le = '01h'$, то в случае $T = 1$ статус обработки отображается в виде '6700'.

TCS_53 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#L	L	'XX..XXh'	Считанные данные включаются в дискретный объект данных с меткой '53h'
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда проходит, карточка выдает '9000'.
- ◆ Если EF не выбран, то статус обработки выдается в виде '6986'.
- ◆ Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей статуса в виде '6982'.
- ◆ Если смещение не соответствует размеру EF (смещение > размера EF), то статус обработки выдается в виде '6B00'.
- ◆ Если размер данных, подлежащих извлечению, не соответствует размеру EF (смещение + Le > размера EF), то статус обработки выдается в виде '6700' или '6Cxx', где 'xx' указывает точную длину.
- ◆ Если в атрибутах файла обнаружена ошибка целостности, то карточка считает файл поврежденным и не подлежащим восстановлению, и статус обработки выдается в виде '6400' или '6500'.
- ◆ Если в хранящихся данных обнаружена ошибка целостности, то карточка выдает требуемые данные, и статус обработки выдается в виде '6281'.

3.5.2.3.1 Команда с защищенным обменом сообщениями (примеры)

Следующий пример иллюстрирует применение защищенного обмена сообщениями в том случае, если применяется условие безопасности SM-MAC-G2.

TCS_54 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'0Ch'	Запрос на защищенный обмен сообщениями
INS	1	'B1h'	Считывание данных
P1	1	'00h'	Текущий EF
P2	1	'00h'	
Lc	1	'XXh'	Длина поля защищенных данных
#6	1	'B3h'	Метка, указывающая значение обычных данных в кодировке BER-TLV
#7	1	'NNh'	L _{PV} : длина передаваемых данных

Байт	Длина	Значение	Описание
#(8)-#(7+NN)	NN	'XX..XXh'	Обычные данные в кодировке BER-TLV, т. е. объект данных со смещением с меткой '54'
#(8+NN)	1	'97h'	T _{LE} : метка, указывающая на спецификацию ожидаемой длины
#(9+NN)	1	'01h'	L _{LE} : ожидаемая длина
#(10+NN)	1	'XXh'	Спецификация ожидаемой длины (изначальная длина L _e): число байтов, подлежащих считыванию
#(11+NN)	1	'8Eh'	T _{CC} : Метка для криптографической контрольной суммы
#(12+NN)	1	'XXh'	L _{CC} : длина следующей криптографической контрольной суммы '08h', '0Ch' или '10h' в зависимости от длины ключа AES для безопасного обмена сообщениями поколения 2 (см. приложение подраздел 11, часть B)
#(13+NN)- #(12+M+NN)	M	'XX..XXh'	Криптографическая контрольная сумма
L _e	1	'00h'	Как указано в стандарте ISO/IEC 7816-4
TCS_55 Ответное сообщение, если команда прошла			
Байт	Длина	Значение	Описание
#1	1	'B3h'	Обычные данные в кодировке BER-TLV
#2	L	'NNh' или '81 NNh'	L _{PV} : длина переданных обратно данных (=изначальная длина L _e) L равно 2 байтам, если L _{PV} > 127 байтов
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Значение обычных данных в кодировке BER-TLV, т. е. считанные данные, заключенные в дискретный объект данных с меткой '53h'
#(2+L+NN)	1	'99h'	Статус обработки незащищенного ответа APDU
#3+L+NN)	1	'02h'	Продолжительность статуса обработки
#4+L+NN)- #(5+L+NN)	2	'XX..XXh'	Статус обработки незащищенного ответа APDU
#(6+L+NN)	1	'8Eh'	T _{CC} : Метка для криптографической контрольной суммы
#(7+L+NN)	1	'XXh'	L _{CC} : Длина следующей криптографической контрольной суммы '08h', '0Ch' или '10h' в зависимости от длины ключа AES для безопасного обмена сообщениями поколения 2 (см. приложение подраздел 11, часть B)
#(8+L+NN)- #(7+M+L+NN)	M	'XX..XXh'	Криптографическая контрольная сумма
SW	2	'XXXXh'	Знаки состояния (SW1, SW2)

3.5.3 UPDATE BINARY (ОБНОВЛЕНИЕ ДАННЫХ)

Данная команда соответствует стандарту ISO/IEC 7816-4, однако ее использование ограничено по сравнению с командой, определенной в указанном стандарте.

Командное сообщение UPDATE BINARY начинает обновление (удаление + запись) битов, которые уже присутствуют в данных файла EF с помощью битов, содержащихся в команде APDU.

3.5.3.1 Команда со смещением в P1-P2

Эта команда позволяет IFD записывать соответствующие данные в файл EF, выбранный в данный момент, без проверки целостности полученных карточкой данных.

Примечание: Данная команда без защищенного обмена сообщениями может использоваться только для обновления файла, который поддерживает условие безопасности ALW в режиме доступа Update.

TCS_56 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'D6h'	Обновление данных
P1	1	'XXh'	Смещение байтов с начала файла: байт самого старшего разряда
P2	1	'XXh'	Смещение байтов с начала файла: байт самого младшего разряда
Lc	1	'NNh'	Lc — длина данных для обновления. Число байтов, подлежащих записи
#6-#(5+NN)	NN	'XX..XXh'	Данные, подлежащие записи

Примечание: Бит 8 байта P1 должен быть установлен на 0.

TCS_57 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда проходит, карточка выдает '9000'.
- ◆ Если EF не выбран, статус обработки выдается в виде '6986'.
- ◆ Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей статуса '6982'.
- ◆ Если смещение не соответствует размеру EF (смещение > размера EF), то статус обработки выдается в виде '6B00'.
- ◆ Если размер данных, подлежащих записи, не соответствует размеру EF (смещение + Lc > размера EF), статус обработки выдается в виде '6700'.
- ◆ Если в атрибутах файла обнаружена ошибка целостности, то карточка считает файл поврежденным и не подлежащим восстановлению, и статус обработки выдается в виде '6400' или '6500'.
- ◆ Если запись EF не прошла, то статус обработки выдается в виде '6581'.

3.5.3.1.1 Команда с защищенным обменом сообщениями (примеры)

Данная команда позволяет IFD записывать данные в файл EF, выбранный в данный момент, с проверкой целостности полученных карточкой данных. Поскольку требование конфиденциальности отсутствует, данные не шифруются.

TCS_58 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'0Ch'	Запрос на криптозащищенный обмен сообщениями
INS	1	'D6h'	Обновление данных
P1	1	'XXh'	Смещение байтов с начала файла: байт самого старшего разряда
P2	1	'XXh'	Смещение байтов от начала файла: самый младший значащий байт
Lc	1	'XXh'	Длина поля защищенных данных
#6	1	'81h'	T _{PV} : метка, указывающая значение обычных данных
#7	L	'NNh' или '81 NNh'	L _{PV} : длина передаваемых данных L равен 2 байтам, если L _{PV} > 127 байтов
#(7+L)- #(6+L+NN)	NN	'XX..XXh'	Значение обычных данных (данные, подлежащие записи)
#(7+L+NN)	1	'8Eh'	T _{CC} : метка для криптографической контрольной суммы
#(8+L+NN)	1	'XXh'	L _{CC} : Длина следующей криптографической контрольной суммы '04h' для безопасного обмена сообщениями поколения 1 (см. приложение подраздел 11, часть А) '08h', '0Ch' или '10h' в зависимости от длины ключа AES для безопасного обмена сообщениями поколения 2 (см. приложение подраздел 11, часть В)
#(9+L+NN)- #(8+M+L+NN)	M	'XX..XXh'	Криптографическая контрольная сумма
Le	1	'00h'	Как указано в стандарте ISO/IEC 7816-4

TCS_59 Ответное сообщение, если формат ввода в режиме защищенного обмена данными неправильный

Байт	Длина	Значение	Описание
#1	1	'99h'	T _{SW} : Метка для знаков состояния (должна быть защищена с помощью криптографической суммы)
#2	1	'02h'	L _{SW} : длина возвращаемых знаков состояния
#3-#4	2	'XXXXh'	Статус обработки незащищенного ответа APDU
#5	1	'8Eh'	T _{CC} : Метка для криптографической контрольной суммы
#6	1	'XXh'	L _{CC} : Длина следующей криптографической контрольной суммы

Байт	Длина	Значение	Описание
			'04h' для безопасного обмена сообщениями поколения 1 (см. приложение подраздел 11, часть А)
			'08h', '0Ch' или '10h' в зависимости от длины ключа AES для безопасного обмена сообщениями поколения 2 (см. приложение подраздел 11, часть В)
#7-#(6+L)	L	'XX..XXh'	Криптографическая контрольная сумма,
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

Данные о статусах «нормальной» обработки, описанные для команды UPDATE BINARY, передаваемой в незащищенном виде (см. пункт 3.5.3.1), могут возвращаться с использованием структуры ответного сообщения, описанного выше.

Кроме того, могут иметь место некоторые ошибки, которые конкретно связаны с криптозащищенным обменом сообщениями. В этом случае данные о статусе обработки просто возвращаются, не задействуя использованную структуру защиты данных:

TCS_60 Ответное сообщение в случае ошибки в защищенном обмене сообщениями

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если ключ текущего сеанса отсутствует, статус обработки выдается в виде '6A88'.
- ◆ Если некоторые ожидаемые объекты данных (как указано выше) в формате криптозащищенного обмена данными отсутствуют, то статус обработки выдается в виде '6987': эта ошибка возникает в том случае, если ожидаемая метка отсутствует или если основная часть команды составлена неправильно.
- ◆ Если некоторые объекты данных неправильны, то статус обработки выдается в виде '6988': эта ошибка возникает в том случае, если требуемые метки есть, но длина некоторых из них отличается от ожидаемой длины.
- ◆ Если проверка криптографической контрольной суммы показала неправильный результат, то статус обработки выдается в виде '6688'.

3.5.3.2 Команда с коротким идентификатором EF

Данный вариант команды позволяет IFD выбрать EF при помощи короткого идентификатора EF и записывать данные из этого EF.

TCS_61 Карточка тахографа поддерживает данный вариант команды для всех элементарных файлов с соответствующим указанным коротким идентификатором EF. Такие короткие идентификаторы EF представлены в главе 4.

TCS_62 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'D6h'	Обновление данных

Байт	Длина	Значение	Описание
P1	1	'XXh'	Бит 8 устанавливается на 1 Биты 7 и 6 устанавливаются на 00 Биты 5–1 кодируют короткий идентификатор соответствующего EF
P2	1	'XXh'	кодирует смещение с 0 до 255 байтов в EF, который указан в P1
Lc	1	'NNh'	Lc — длина данных для обновления. Число байтов, подлежащих записи
#6-#(5+NN)	NN	'XX..XXh'	Данные, подлежащие записи

TCS_63 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

Примечание: Короткие идентификаторы EF, используемые в тахографах поколения 2, указаны в главе 4.

Если P1 кодирует короткий идентификатор EF и если команда прошла, то идентифицированный EF становится в данный момент выбранным (т. е. текущим) EF.

- ◆ Если команда проходит, карточка выдает '9000'.
- ◆ Если файл, соответствующий идентификатору файла, не найден, то статус обработки выдается в виде '6A82'.
- ◆ Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей статуса '6982'.
- ◆ Если смещение не соответствует размеру EF (смещение > размера EF), то статус обработки выдается в виде '6B00'.
- ◆ Если размер данных, подлежащих записи, не соответствует размеру EF (смещение + Lc > размера EF), то статус обработки выдается в виде '6700'.
- ◆ Если в атрибутах файла обнаружена ошибка целостности, то карточка считает файл поврежденным и не подлежащим восстановлению, и статус обработки выдается в виде '6400' или ~~6581~~'6500'.
- ◆ Если запись не прошла, то статус обработки выдается в виде '6581'.

3.5.3.3 Команда с нечетным командным байтом

Данный вариант команды позволяет IFD записывать данные в EF размером 32 768 байтов или более.

TCS_64 Карточка тахографа, поддерживающая EF размером 32 768 байтов или более, поддерживает данный вариант команды для этих EF. В случае других EF карточка тахографа может поддерживать или не поддерживать данный вариант команды.

TCS_65 Командное сообщение

<i>Байт</i>	<i>Длина</i>	<i>Значение</i>	<i>Описание</i>
CLA	1	'00h'	
INS	1	'D7h'	Обновление данных
P1	1	'00h'	Текущий EF
P2	1	'00h'	
Lc	1	'NNh'	Lc — длина данных в поле данных команды
#6-#(5+NN)	NN	'XX..XXh'	Объект данных со смещением с меткой '54h' Объект дискреционных данных с меткой '53h', который никапсулирует данные для записи

IFD кодирует длину смещенного объекта данных и длину дискретного объекта данных с минимальным возможным числом октетов, т. е. с помощью байта длины '01h' IFD кодирует смещение/длину от 0 до 255, а с помощью байта длины '02h' — смещение/длину от '256' до '65 535' байтов.

TCS_66 Ответное сообщение

<i>Байт</i>	<i>Длина</i>	<i>Значение</i>	<i>Описание</i>
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда проходит, карточка выдает '**9000**'.
- ◆ Если EF не выбран, статус обработки выдается в виде '**6986**'.
- ◆ Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей статуса '**6982**'.
- ◆ Если смещение не соответствует размеру EF (смещение > размера EF), то статус обработки выдается в виде '**6B00**'.
- ◆ Если размер данных, подлежащих записи, не соответствует размеру EF (смещение + Lc > размера EF), статус обработки выдается в виде '**6700**'.
- ◆ Если в атрибутах файла обнаружена ошибка целостности, то карточка считает файл поврежденным и не подлежащим восстановлению, и статус обработки выдается в виде '**6400**' или '**6500**'.
- ◆ Если запись не прошла, то статус обработки выдается в виде '**6581**'.

3.5.3.3.1 Команда с защищенным обменом сообщениями (пример)

Следующий пример иллюстрирует применение защищенного обмена сообщениями, если применяется условие безопасности SM-MAC-G2.

TCS_67 Командное сообщение

<i>Байт</i>	<i>Длина</i>	<i>Значение</i>	<i>Описание</i>
CLA	1	'0Ch'	Запрос на криптозащищенный обмен сообщениями
INS	1	'D7h'	Обновление данных
P1	1	'00h'	Текущий EF
P2	1	'00h'	

Байт	Длина	Значение	Описание
Lc	1	'XXh'	Длина поля защищенных данных
#6	1	'B3h'	Метка, указывающая значение обычных данных в кодировке BER-TLV
#7	L	'NNh' или '81 NNh'	L _{PV} : длина передаваемых данных L равен 2 байтам, если L _{PV} > 127 байтов
#(7+L)- #(6+L+NN)	NN	'XX..XXh'	Обычные данные в кодировке BER-TLV, т. е. объект данных со смещением с меткой '54h' Объект дискреционных данных с меткой '53h', который инкапсулирует данные для записи
#(7+L+NN)	1	'8Eh'	T _{CC} : Метка для криптографической контрольной суммы
#(8+L+NN)	1	'XXh'	L _{CC} : Длина следующей криптографической контрольной суммы '08h', '0Ch' или '10h' в зависимости от длины ключа AES для безопасного обмена сообщениями поколения 2 (см. приложение подраздел 11, часть B)
#(9+L+NN)- #(8+M+L+NN)	M	'XX..XXh'	Криптографическая контрольная сумма
Le	1	'00h'	Как указано в стандарте ISO/IEC 7816-4
TCS_68 Ответное сообщение, если команда прошла			
Байт	Длина	Значение	Описание
#1	1	'99h'	T _{SW} : Метка для знаков состояния (должна быть защищена с помощью криптографической суммы)
#2	1	'02h'	L _{SW} : длина возвращаемых знаков состояния
#3-#4	2	'XXXXh'	Статус обработки незащищенного ответа APDU
#5	1	'8Eh'	T _{CC} : Метка для криптографической контрольной суммы
#6	1	'XXh'	L _{CC} : Длина следующей криптографической контрольной суммы' '08h', '0Ch' или '10h' в зависимости от длины ключа AES для безопасного обмена сообщениями поколения 2 (см. приложение подраздел 11, часть B)
#7-#(6+L)	L	'XX..XXh'	Криптографическая контрольная сумма,
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

3.5.4 GET CHALLENGE (ПОЛУЧЕНИЕ ЗАПРОСА)

Данная команда соответствует стандарту ISO/IEC 7816-4, однако ее использование ограничено по сравнению с командой, определенной в указанном стандарте.

Команда GET CHALLENGE направляет карточке запрос с целью использовать ее в процедуре, связанной с безопасностью, в которой криптограмма или некоторые зашифрованные данные отправляются на карточку.

TCS_69 Запрос, выданный карточкой, действителен только для следующей команды, которая использует запрос, переданный карточке.

TCS_70 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (длина ожидаемого запроса)

TCS_71 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#8	8	'XX..XXh'	Get Challenge (получение запроса)
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда проходит, карточка выдает '9000'.
- ◆ Если Le отличается от '08h', статус обработки выдается в виде '6700'.
- ◆ Если параметры P1–P2 неправильны, статус обработки выдается в виде '6A86'.

3.5.5 VERIFY (ПРОВЕРКА)

Данная команда соответствует стандарту ISO/IEC 7816-4, однако ее использование ограничено по сравнению с командой, определенной в указанном стандарте.

Для поддержки этой команды требуется только карточка мастерской.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду, но для таких карточек исходное значение CHV не персонализируется. Как следствие, такие карточки не способны выполнять данную команду должным образом. Если команда отправлена, то в случае других типов карточек тахографов, кроме карточек мастерской, поведение, т. е. передаваемый обратно код ошибки, окажется вне сферы применения данной спецификации.

Команда Verify инициирует сравнение на уровне карточки между переданными данными CHV (PIN) и исходными данными CHV, записанными на карточке.

TCS_72 ПИН-код, введенный пользователем, должен быть закодирован в ASCII ASCII и заполнен IFD с правой стороны байтами 'FFh' до достижения длины 8 байтов; см. также тип данных WorkshopCardPIN в **приложении подраздел 1**.

TCS_73 Приложения тахографа первого и второго поколений используют одно и то же исходное значение CHV.

TCS_74 Карточка тахографа проверяет, правильно ли закодирована команда. Если команда закодирована неправильно, карточка не сравнивает значения CHV, не понижает показания счетчика оставшихся попыток CHV и не восстанавливает статус безопасности «PIN_Verified», а отменяет команду. Команда закодирована правильно, если байтам CLA,

INS, P1, P2, Lc присвоены конкретные значения, Le отсутствует, а поле командных данных имеет правильную длину.

TCS_75 Если команда проходит, счетчик оставшихся попыток CHV выставляется на исходное значение. Исходное значение счетчика оставшихся попыток CHV составляет 5. Если команда проходит, карточка передает внутренний статус безопасности «PIN_Verified». Карточка сбрасывает этот статус безопасности, если ее перезагрузили или если переданный в команду код CHV не соответствует сохранившемуся исходному значению CHV.

Примечание: Использование одного и того же исходного значения CHV и глобального статуса безопасности лишают работника мастерской возможности снова ввести ПИН-код после выбора другого приложения тахографа DF.

TCS_76 Сравнение, которое дало неправильные результаты, регистрируется на карточке, т. е. значение счетчика оставшихся попыток CHV понижается на единицу с целью ограничить число дальнейших попыток использования исходных данных CHV.

TCS_77 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (проверенные данные CHV известны по косвенным признакам)
Lc	1	'08h'	Длина передаваемого кода CHV
#6-#13	8	'XX..XXh'	CHV

TCS_78 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда проходит, карточка выдает '9000'.
- ◆ Если ссылка на CHV не найдена, статус обработки выдается в виде '6A88'.
- ◆ Если данные CHV заблокированы (счетчик оставшихся попыток CHV показывает ноль), статус обработки выдается в виде '6983'. В этом состоянии данные CHV больше никогда не принимаются.
- ◆ Если сравнение дало неправильные результаты, показание счетчика оставшихся попыток уменьшается и статус обработки выдается в виде '63CX' (X > 0 и X равен показанию счетчика оставшихся попыток CHV).
- ◆ Если исходное значение CHV считается поврежденным, то статус обработки выдается в виде '6400' или '6581'.
- ◆ Если Lc отличается от '08h', то статус обработки выдается в виде '6700'.

3.5.6 GET RESPONSE (ПОЛУЧЕНИЕ ОТВЕТА)

Данная команда соответствует стандарту ISO/IEC 7816-4.

Данная команда (необходимая и доступная только для протокола T = 0) используется для передачи подготовленных данных с карточки на интерфейс (случай, когда команда включает в себя оба байта Lc и Le).

Команда GET_RESPONSE должна выдаваться сразу же после команды на подготовку данных, в противном случае данные потеряются. После выполнения команды GET RESPONSE (за исключением случаев ошибки '61xx' или '6Cxx', см. ниже) данные, подготовленные ранее, становятся недоступны.

TCS_79 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Число ожидаемых байтов

TCS_80 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#X	X	'XX..XXh'	Данные
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда проходит, карточка выдает '9000'.
- ◆ Если данные карточкой подготовлены не были, статус обработки выдается в виде '6900' или '6F00'.
- ◆ Если Le превышает число имеющихся байтов или если Le равна нулю, статус обработки выдается в виде '6Cxx', где 'xx' указывает на точное число имеющихся байтов. В этом случае подготовленные данные все еще доступны для следующей команды GET RESPONSE.
- ◆ Если Le не равна нулю и меньше, чем число имеющихся байтов, то требуемые данные нормально передаются карточкой, а статус обработки выдается в виде '61xx', где 'xx' указывает на число дополнительных байтов, все еще имеющихся для выполнения следующей команды GET RESPONSE.
- ◆ Если команда не поддерживается (протокол T=1), карточка выдает '6D00'.

3.5.7 PSO: VERIFY CERTIFICATE (ПРОВЕРКА СЕРТИФИКАТА)

Данная команда соответствует стандарту ISO/IEC 7816-8, однако ее использование ограничено по сравнению с командой, определенной в указанном стандарте.

Команда VERIFY CERTIFICATE используется карточкой для получения открытого ключа извне и проверки его действительности.

3.5.7.1 Поколение 1: парное сообщение «команда — ответ»

TCS_81 Данный вариант команды поддерживается только приложением тахографа первого поколения.

TCS_82 Если команда VERIFY CERTIFICATE проходит, открытый ключ записывается для будущего использования в среде защиты. Этот ключ

должен конфигурироваться непосредственно для использования команд, связанных с защитой (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE или VERIFY CERTIFICATE) с помощью команды MSE (см. 3.5.11), использующей идентификатор этого ключа.

TCS_83 В любом случае команда VERIFY CERTIFICATE использует открытый ключ, ранее выбранный командой MSE для открытия сертификата. Этот открытый ключ должен быть ключом ~~государства-члена или европейской~~ **Договаривающейся стороны или корневым открытым ключом.**

TCS_84 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'2Ah'	Выполнить операцию по обеспечению безопасности
P1	1	'00h'	P1
P2	1	'AEh'	P2: данные не в кодировке BER-TLV (конкатенация элементов данных)
Lc	1	'C2h'	Lc: длина сертификата, 194 байта
#6-#199	194	'XX..XXh'	Сертификат: конкатенация элементов данных (как описано в приложении подразделе 11)

TCS_85 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда проходит, карточка выдает **'9000'**.
- ◆ Если проверка сертификата показала неправильный результат, статус обработки выдается в виде **'6688'**. Процесс проверки и расшифровки сертификата для поколений 1 и 2 описан в ~~приложении~~ **подразделе 11**.
- ◆ Если открытый ключ среды защиты отсутствует, выдается **'6A88'**.
- ◆ Если выбранный открытый ключ (используемый для расшифровки сертификата) считается поврежденным, статус обработки выдается в виде **'6400'** или **'6581'**.
- ◆ Только для первого поколения: Если параметр выбранного открытого ключа (используемого для расшифровки сертификата) CHA.LSB (CertificateHolder Authorisation.equipmentType) отличается от '00' (т. е. не является ни ключом ~~государства-члена или Европы~~ **Договаривающейся стороны**, ни корневым сертификатом), статус обработки выдается в виде **'6985'**.

3.5.7.2 Поколение 2: парное сообщение «команда — ответ»

В зависимости от размера кривой сертификаты ECC могут быть столь длинными, что передать их с помощью одной команды APDU будет невозможно. В подобном случае необходимо применять систему формирования цепочки команд в соответствии с ISO/IEC 7816-4, и передавать сертификат двумя последовательными командами APDU PSO: Verify Certificate.

Структура сертификата и параметры домена представлены в **подразделе 11**.

TCS_86 Команда может выполняться в MF, DF Tachograph и DF Tachograph_G 2; см. также TCS_343.

TCS_87 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'X0h'	Байт CLA, указывающий на цепочку команд: '00h' — единственная или последняя команда цепочки '10h' не является последней командой в цепочке
INS	1	'2Ah'	Выполнить операцию по обеспечению безопасности
P1	1	'00h'	
P2	1	'BEh'	Проверка сертификата с самоописанием
Lc	1	'XXh'	Длина поля данных команды, см. TCS_88 и TCS_89
#6-#5+L	L	'XX..XXh'	Кодированные данные DER-TLV: объект данных основной части сертификата ECC в качестве первого объекта данных, соединенного с объектом данных подписи сертификата ECC в качестве второго объекта данных или соответствующей части этой конкатенации. Метка '7F21' и соответствующая длина не передаются Порядок этих объектов данных фиксирован

TCS_88 В случае коротких APDU применяются следующие положения: IFD использует минимальное число APDU, требуемое для передачи необходимых данных команды, и передает максимальное число байтов в первой команде APDU ~~в соответствии со значением байтов карточки размера информационного поля; см. TCS_14. Если IFD ведет себя по-другому, поведение карточки в область применения не попадает.~~ **Однако любое значение 'Lc' вплоть до 255 байтов должно поддерживаться карточкой.**

TCS_89 В случае APDU расширенной длины применяются следующие положения: если сертификат не помещается в одну APDU, формирование цепочек команд поддерживается карточкой. IFD использует минимальное число APDU, требуемое для передачи команды, и передает максимальное число байтов в первой команде APDU. **Если требуется цепочка, то любое значение 'Lc' вплоть до указанного максимального размера расширенной длины должно поддерживаться карточкой.** ~~IFD ведет себя по-другому, поведение карточки считается неприменимым.~~

Примечание: В соответствии с ~~приложением~~ **подразделом 11** карточка сохраняет сертификат или соответствующее содержание сертификата и обновляет его параметр currentAuthenticatedTime (текущее время аутентификации).

Структура ответного сообщения и характеристики статуса представлены в **TCS_85**.

TCS_90 Помимо кодов ошибок, перечисленных в позиции 0, карточка может выдавать следующие коды ошибок:

- ◆ Если выбранный открытый ключ (используемый для расшифровки сертификата) относится к типу CHA.LSB (CertificateHolderAuthorisation.equipmentType), который не подходит для проверки сертификата в соответствии с **приложением подразделом 11**, то статус обработки выдается в виде **‘6985’**.
- ◆ Если текущая дата currentAuthenticatedTime карточки позднее, чем дата истечения срока действия сертификата, то статус обработки выдается в виде **‘6985’**.
- ◆ Если ожидается последняя команда цепочки, то карточка выдает **‘6883’**.
- ◆ Если в поле командных данных передаются неверные параметры, карточка выдает **‘6A80’** (как и в случае, когда объекты данных не передаются в установленном порядке).

3.5.8 INTERNAL AUTHENTICATE (ВНУТРЕННЯЯ АУТЕНТИФИКАЦИЯ)

Данная команда соответствует стандарту ISO/IEC 7816-4.

TCS_91 Данную команду поддерживают все карточки тахографов в файле DF Tachograph поколения 1. В MF и/или DF Tachograph_G2 эта команда может быть доступной или недоступной. В этом случае она прерывается с помощью соответствующего кода ошибки, так как закрытый ключ карточки (Card.SK) для протокола аутентификации поколения 1 доступен только в DF_Tachograph поколения 1.

Используя команду INTERNAL AUTHENTICATE, IFD может аутентифицировать карточку. Процесс аутентификации описан в **приложении подразделе 11**. Он включает в себя следующие позиции:

TCS_92 Команда INTERNAL AUTHENTICATE использует закрытый ключ карточки (выбранный по косвенным признакам) для подписания данных аутентификации, включая K1 (первый элемент для согласования ключей сеанса) и RND1, и использует открытый ключ, выбранный в данный момент (с помощью последней команды MSE), для шифрования подписи и формирования маркера аутентификации (более подробно в **приложении подразделе 11**).

TCS_93 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	CLA
INS	1	‘88h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Lc	1	‘10h’	Длина данных, отправленных на карточку
#6-#13	8	‘XX..XXh’	Запрос, использованный для аутентификации карточки
#14-#21	8	‘XX..XXh’	VU.CHR (см. приложение подраздел 11)
Le	1	‘80h’	Длина данных, ожидаемых от карточки

TCS_94 Ответное сообщение			
Байт	Длина	Значение	Описание
#1-#128	128	'XX..XXh'	Маркер аутентификации карты (см. приложение подраздел 11)
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ♦ Если команда проходит, карточка выдает '9000'.
- ♦ Если открытый ключ среды защиты отсутствует, выдается '6A88'.
- ♦ Если закрытый ключ среды защиты отсутствует, выдается '6A88'.
- ♦ Если VU.CHR не соответствует данному идентификатору открытого ключа, статус обработки выдается в виде '6A88'.
- ♦ Если выбранный закрытый ключ считается поврежденным, статус обработки выдается в виде '6400' или '6581'.

TCS_95 Если команда INTERNAL AUTHENTICATE проходит, ключ текущего сеанса **поколения 1**, если он существует, стирается и более не доступен. Для создания нового ключа сеанса **поколения 1** должна быть успешно выполнена команда EXTERNAL AUTHENTICATE для механизма аутентификации поколения 1.

Примечание: Ключи сеанса поколения 2 см. CSM_193 и CSM_195 в подразделе 11 добавления. Если ключи сеанса поколения 2 созданы и карточка тахографа получает команду APDU INTERNAL AUTHENTICATE обычным текстом, она прерывает сеанс защищенного обмена сообщениями поколения 2 и уничтожает ключи сеанса поколения 2.

3.5.9 EXTERNAL AUTHENTICATE (ВНЕШНЯЯ АУТЕНТИФИКАЦИЯ)

Данная команда соответствует стандарту ISO/IEC 7816-4.

Используя команду EXTERNAL AUTHENTICATE, карточка может произвести аутентификацию IFD. Процесс аутентификации описывается в **приложении подраздела 11** для тахографов первого и второго поколений (аутентификация БУ).

TCS_96 Вариант команды для механизма взаимной аутентификации поколения 1 поддерживается только приложением тахографа поколения 1.

TCS_97 Вариант команды для взаимной аутентификации БУ и карточки поколения 2 может выполняться в MF, DF Tachograph и DF Tachograph_G2; см. также TCS_34. Если команда EXTERNAL AUTHENTICATE поколения 2 проходит, то ключ текущего сеанса поколения 1, если он существует, стирается и более не доступен.

Примечание: Ключи сеанса поколения 2 см. CSM_193 и CSM_195 в подразделе 11. Если ключи сеанса поколения 2 созданы и, если карточка тахографа получает обычную команду APDU «EXTERNAL AUTHENTICATE», она прерывает сеанс защищенного обмена сообщениями поколения 2 и уничтожает ключи сеанса поколения 2.

TCS_98 Командное сообщение			
Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Ключи и алгоритмы по косвенным признакам известны

Байт	Длина	Значение	Описание
P2	1	'00h'	
Lc	1	'XXh'	Lc (Длина данных, отправленных на карточку)
#6-#(5+L)	L	'XX..XXh'	Аутентификация поколения 1: криптограмма (см. приложение подраздел 11 добавления , часть A) Аутентификация поколения 2: подпись, генерируемая IFD (см. приложение подраздел 11 , часть B)

TCS_99 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

Если команда проходит, карточка выдает '9000'.

Если СНА выбранного открытого ключа не соответствует конкатенации AID приложения тахографа и типа БУ, то статус обработки выдается в виде '6F00'.

Если этой команде не предшествует непосредственно команда GET CHALLENGE, то статус обработки выдается в виде '6985'.

Приложение тахографа поколения 1 может выдавать следующие дополнительные коды ошибок:

- ◆ Если открытый ключ среды защиты отсутствует, выдается '6A88'.
- ◆ Если закрытый ключ среды защиты отсутствует, выдается '6A88'.
- ◆ Если проверка криптографической контрольной суммы показала неправильный результат, статус обработки выдается в виде '6688'.
- ◆ Если выбранный закрытый ключ считается поврежденным, статус обработки выдается в виде '6400' или '6581'.

Вариант команды для аутентификации в случае поколения 2 может выдать следующий дополнительный код ошибки:

Если проверка подписи не удалась, карточка выдает '6300'.

3.5.10 GENERAL AUTHENTICATE (ОБЩАЯ АУТЕНТИФИКАЦИЯ)

Данная команда используется для протокола аутентификации микросхемы поколения 2, как указано в части В приложения **подраздела 11**, и соответствует ISO/IEC 7816-4.

TCS_100 Команда может выполняться в MF, DF Tachograph и DF Tachograph_G 2; см. также **TCS_34**.

TCS_101 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Ключи и протокол по косвенным признакам известны

Байт	Длина	Значение	Описание
P2	1	'00h'	
Lc	1	'NNh'	Lc: длина поля последующих данных
#6-#(5+L)	L	'7Ch' + L _{7C} + '80h' + L ₈₀ + 'XX..XXh'	Значение кратковременного открытого ключа в кодировке DER-TLV (см. приложение подраздел 11) БУ отправляет объекты данных в следующем порядке:
5+Le+1	1	'00h'	Как указано в стандарте ISO/IEC 7816-4

TCS_102 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#L	L	'7Ch' + L _{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L ₈₂ + 'XX..XXh'	Данные динамической аутентификации в кодировке DER-TLV: факультативное временное значение и маркер аутентификации (см. приложение подраздел 11).
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда проходит, карточка выдает **'9000'**.
- ◆ Если параметры в поле данных неверны, карточка выдает **'6A80'**.
- ◆ Если команду External Authenticate выполнить успешно не удалось, карточка выдает **'6982'**.

Ответ объекта данных динамической аутентификации '7Ch':

- должен выдаваться в том случае, если операция выполнена успешно, т. е. если Характеристики состояния — **'9000'**,
- должен отсутствовать в случае ошибки выполнения или проверки, т. е. в том случае, если характеристики состояния находятся в интервале **'6400'**–**'6FFF'**,
- может отсутствовать в случае предупреждения, т. е. в том случае, если характеристики состояния находятся в интервале **'6200'**–**'63FF'**.

3.5.11 MANAGE SECURITY ENVIRONMENT (УПРАВЛЕНИЕ СРЕДОЙ ЗАЩИТЫ)

Данная команда используется для определения открытого ключа в целях аутентификации.

3.5.11.1 Поколение 1: парное сообщение «команда — ответ»

Данная команда соответствует стандарту ISO/IEC 7816-4. Использование этой команды по сравнению с указанным стандартом ограничено.

TCS_103 Данная команда поддерживается только приложением тахографа поколения 1.

TCS_104 Ключ, указанный в поле данных MSE, продолжает оставаться действующим открытым ключом до следующей правильной команды MSE, выбора DF или перезагрузки карточки.

TCS_105 Если указанный ключ (пока еще) отсутствует на карточке, среда защиты остается без изменений.

TCS_106 Командное сообщение

<i>Байт</i>	<i>Длина</i>	<i>Значение</i>	<i>Описание</i>
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: исходный ключ, действительный для всех криптографических операций
P2	1	'B6h'	P2 (исходные данные, относящиеся к цифровой подписи)
Lc	1	'0Ah'	Lc: длина поля последующих данных
#6	1	'83h'	Метка, указывающая на открытый ключ в асимметричных случаях
#7	1	'08h'	Длина исходных данных ключа (идентификатор ключа)
#8-#15	8	'XX..XXh'	Идентификатор ключа, как указано в приложении подразделе 11

TCS_107 Ответное сообщение

<i>Байт</i>	<i>Длина</i>	<i>Значение</i>	<i>Описание</i>
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда проходит, карточка выдает **'9000'**.
- ◆ Если исходный ключ на карточке отсутствует, статус обработки выдается в виде **'6A88'**.
- ◆ Если некоторые ожидаемые объекты данных в формате защищенного обмена сообщениями отсутствуют, статус обработки выдается в виде **'6987'**. Это может произойти, если отсутствует метка '83h'.
- ◆ Если некоторые объекты данных неверны, статус обработки выдается в виде **'6988'**. Это может произойти в том случае, если длина идентификатора ключа не соответствует '08h'.
- ◆ Если выбранный закрытый ключ считается поврежденным, статус обработки выдается в виде **'6400'** или **'6581'**.

3.5.11.2 Поколение 2: парное сообщение «команда — ответ»

Для аутентификации поколения 2 карточка тахографа поддерживает следующую команду MSE: Установленные версии команды, которые соответствуют стандарту ISO/IEC 7816-4. В случае аутентификации поколения 1 данные версии команды не поддерживаются.

3.5.11.2.1 Команда MSE:SET AT для аутентификации микросхемы

Следующая команда MSE:SET AT используется для выбора параметров аутентификации микросхемы, которая выполняется с помощью последующей команды General Authenticate.

TCS_108 Эта команда может выполняться в MF, DF Tachograph и DF Tachograph_G 2; см. также TCS_34.

TCS_109 Командное сообщение MSE:SET AT для аутентификации микросхемы

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'41h'	Устанавливается для внутренней аутентификации
P2	1	'A4h'	Аутентификация
Lc	1	'NNh'	Lc: длина поля последующих данных
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Ссылка на криптографический механизм в кодировке DER-TLV: Идентификатор объекта аутентификации микросхемы (только значение, метка '06h' опущена) Значения идентификаторов объектов см. в приложении подразделе 1 ; используется байтовая нотация. Руководство по выбору одного из идентификаторов этих объектов см. в приложении подразделе 11

3.5.11.2.2 MSE:SET AT для аутентификации БУ

Следующая команда MSE:SET AT используется для выбора параметров и ключа аутентификации БУ, которая выполняется с помощью последующей команды External Authenticate.

TCS_110 Команда может выполняться в MF, DF Tachograph и DF Tachograph_G 2; см. также TCS_34.

TCS_111 Командное сообщение MSE:SET AT для аутентификации БУ

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Устанавливается для внешней аутентификации
P2	1	'A4h'	Аутентификация
Lc	1	'NNh'	Lc: длина поля последующих данных
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Ссылка на криптографический механизм в кодировке DER-TLV: Идентификатор объекта аутентификации микросхемы (только значение, метка '06h' опущена)

Байт	Длина	Значение	Описание
			Значения идентификаторов объектов см. в приложении подразделе 1 ; используется байтовая нотация. Руководство по выбору одного из этих идентификаторов объектов см. в приложении подразделе 11
		'83h' + '08h' + 'XX..XXh'	Ссылка в кодировке DER-TLV на открытый ключ БУ держателя сертификата, указанная в ссылке держателя сертификата, упомянутой в его сертификате
		'91h' + L91 + 'XX..XXh'	Сжатое отображение кратковременного открытого ключа БУ в кодировке DER-TLV, который будет использоваться во время аутентификации микросхемы (см. приложение подраздел 11 добавления)

3.5.11.2.3 MSE:SET DST

Следующая команда MSE:SET DST используется для создания открытого ключа:

- ◆ либо для проверки подписи, которая передается в последующей команде PSO: Verify Digital Signature (проверка цифровой подписи);
- ◆ либо для проверки подписи сертификата при помощи последующей команды PSO: Verify Digital Signature (проверка цифровой подписи).

TCS_112 Команда может выполняться в MF, DF Tachograph и DF Tachograph_G 2; см. также TCS_33.

TCS_113 Командное сообщение MSE:SET DST

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Установить для проверки
P2	1	'B6h'	Цифровая подпись
Lc	1	'NNh'	Lc: длина поля последующих данных
#6-#(5+L)	L	'83h' + '08h' + 'XX..XXh'	Ссылка на открытый ключ в кодировке DER-TLV, т. е. ссылка на держателя сертификата в сертификате открытого ключа (см. приложение подраздел 11).

Для всех версий этой команды структура ответного сообщения и характеристики статуса задаются следующим образом:

TCS_114 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда проходит, карточка выдает **'9000'**. Протокол выбран и активирован.
- ◆ **'6A80'** указывает на неверные параметры в поле данных команды.
- ◆ **'6A88'** указывает на то, что указанные данные (т. е. указанный ключ) не доступны.
- ◆ Если текущая дата **CurrentAuthenticatedTime** карточки позднее, чем дата истечения срока действия выбранного открытого ключа, то статус обработки выдается в виде **'6A88'**.

Примечание: В случае команды **MSE: SET AT** для аутентификации БУ, исходный ключ является открытым ключом **VU_MA**. Карточка устанавливает открытый ключ **VU_MA** в режим пользования, если он заложен в ее память и соответствует ссылке на держателя сертификата (**CHR**), указанной в поле данных команды (карточка может идентифицировать открытые ключи **VU_MA** с помощью поля **CHA** сертификата). В ответ на эту команду карточка возвращает **"6A 88"**, если доступен только открытый ключ **VU_Sign** или если нет открытого ключа бортового устройства. См. определение поля **CHA** в подразделе 11 добавления и типа данных **equipmentType** в подразделе 1 добавления.

Аналогичным образом, если команда **MSE: SET DST** со ссылкой на **EQT** (т. е. БУ или карточку), отправлена на соответствующую карточку контролера, то, согласно **CSM_234**, исходный ключ будет всегда являться ключом **EQT_Sign**, который должен использоваться для проверки цифровой подписи. Согласно рисунку 13 в подразделе 11 добавления, на карточке контролера всегда будет храниться соответствующий открытый ключ **EQT_Sign**. В некоторых случаях на карточке контролера может храниться соответствующий открытый ключ **EQT_MA**. Карточка контролера всегда переводит открытый ключ **EQT_Sign** в режим использования, когда она получает команду **MSE: SET DST**.

3.5.12 PSO: HASH (ХЕШИРОВАНИЕ)

Данная команда используется для передачи карточке результата расчета хеширования некоторых данных. Она используется для проверки цифровых подписей. Значение хеш-функции временно хранится для последующей команды **PSO: Verify Digital Signature**.

Данная команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению с указанным стандартом ограничено.

Для поддержки данной команды в **DF Tachograph** и **DF Tachograph_G2** требуется только карточка контролера.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду. В **MF** эта команда может быть доступной или недоступной.

Приложение карточки контролера поколения 1 поддерживает только **SHA-1**.

TCS_115 Временно хранящееся значение хеш-функции удаляется, если при помощи команды **PSO: HASH** вычисляется новое значение хеш-функции, если выбран **DF** и если произведена перезагрузка карточки тахографа.

TCS_116 Командное сообщение

<i>Байт</i>	<i>Длина</i>	<i>Значение</i>	<i>Описание</i>
CLA	1	'00h'	CLA
INS	1	'2Ah'	Выполнение операции по безопасности
P1	1	'90h'	Возвращение хеш-кода
P2	1	'A0h'	Метка: поле данных содержит объекты данных, необходимые для хеширования
Lc	1	'XXh'	Длина Lc последующего поля данных
#6	1	'90h'	Метка для хеш-кода
#7	1	'XXh'	Длина L хеш-кода: '14h' в приложении поколения 1 (см. приложение подраздел 11, часть А) '20h', '30h' или '40h' в приложении поколения 2 (см. приложение подраздел 11, часть В)
#8-#(7+L)	L	'XX..XXh'	Хеш-код

TCS_117 Ответное сообщение

<i>Байт</i>	<i>Длина</i>	<i>Значение</i>	<i>Описание</i>
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда прошла, карточка выдает **'9000'**.
- ◆ Если некоторые ожидаемые объекты данных (как указано выше) отсутствуют, статус обработки выдается в виде '6987'. Это может произойти, если отсутствует одна из меток '90h'.
- ◆ Если некоторые объекты данных неверны, то статус обработки выдается в виде **'6988'**. Данная ошибка возникает, если требуемая метка присутствует, но ее длина отличается от '14h' в случае SHA-1, от '20h' в случае SHA-256, от '30h' в случае SHA-384, от '40h' в случае SHA-512 (приложение поколения 2).

3.5.13 PERFORM HASH of FILE (ХЕШИРОВАНИЕ ФАЙЛА)

Данная команда соответствует стандарту ISO/IEC 7816-8. Поэтому байт CLA этой команды указывает на собственное использование команды PERFORM SECURITY OPERATION / HASH.

Для поддержки данной команды в DF Tachograph и DF Tachograph_G2 требуется только карточка водителя и карточка мастерской.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду. Если карточка предприятия или карточка контролера выполняют данную команду, то она выполняется, как указано в настоящей главе.

В MF эта команда может быть доступной или недоступной. Если она доступна, то команда выполняется так, как указано в настоящей главе, т. е. не позволяет вычислять значение хеширования и прерывается с выдачей соответствующего кода ошибки.

- TCS_118** Команда PERFORM HASH FILE используется для хеширования зоны данных выбранного в данный момент транспарентного EF.
- TCS_119** Карточка тахографа поддерживает данную команду только в случае EF, перечисленных в главе 0 в DF_Tachograph и DF_Tachograph_G2 с учетом следующего исключения. Карточка тахографа не поддерживает команду в случае EF Sensor_Installation_Data в DF Tachograph_G2.
- TCS_120** Результат операции хеширования временно хранится на карточке. Затем его можно использовать для получения цифровой подписи файла, используя команду PSO: COMPUTE DIGITAL SIGNATURE (вычисление цифровой подписи).
- TCS_121** При вычислении нового значения хеш-файла с помощью команды PSO:PERFORM HASHhash of FILEfile (хеширование файла) и в случае выбора DF и перезагрузки карточки тахографа временно сохраненное значение хеш-файла удаляется.
- TCS_122** Приложение тахографа поколения 1 поддерживает SHA-1.
- TCS_123** Приложение тахографа поколения 2 поддерживает алгоритм ~~SHA-1~~ и SHA-2 (SHA-256, SHA-384 и или SHA-512 бит), указанный в наборе шифров в подразделе 11, часть B, для ключа подписи карточки «Card Sign».
- TCS_124** Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'80h'	CLA
INS	1	'2Ah'	Выполнение операции по безопасности
P1	1	'90h'	Метка: хеш
P2	1	XXh '00h'	P2: Указывает алгоритм, который будет использоваться для хеширования данных выбранного в данный момент прозрачного файла: Алгоритм неявно неизвестен по косвенным признакам В случае приложения тахографа поколения 1: SHA-1 В случае приложения «Тахограф поколения 2»: алгоритм SHA-2 (SHA-256, SHA-384 или SHA-512), определенный набором шифров в подразделе 11 добавления, часть B, для ключа подписи карточки «Card_Sign» 00h для SHA-1 01h для SHA-256 02h для SHA-384 03h для SHA-512

TCS_125 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ♦ Если команда проходит, карточка выдает '9000'.
- ♦ Если текущий EF не позволяет выполнять эту команду (EF Sensor_Installation_Data в DF Tachograph_G2), статус обработки выдается в виде '6985'.

- ◆ Если выбранный EF считается поврежденным (в атрибутах файла обнаружена ошибка целостности), статус обработки выдается в виде '6400' или '6581'.
- ◆ Если выбранный файл не является транспарентным или если текущий EF отсутствует, то статус обработки выдается в виде '6986'.

3.5.14 PSO: COMPUTE DIGITAL SIGNATURE (РАСЧЕТ ЦИФРОВОЙ ПОДПИСИ)

Эта команда используется для вычисления цифровой подписи ранее вычисленного хеш-кода (см. PERFORM HASH of FILE (хеширование файла), см. § 3.5.13-3.5.13).

Для поддержки данной команды в DF Tachograph и DF Tachograph_G2 требуется только карточка водителя и карточка мастерской.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду. В случае приложения тахографа поколения 2 ключ подписи поколения 2 имеет только карточка водителя и карточка мастерской. Таким образом, такие Другие карточки не могут в состоянии успешно выполнить эту команду и прерывают ее, выдавая соответствующий код ошибки.

В MF эта команда может быть доступной или недоступной. Если да, то команда недоступна в MF, то она завершается с выдачей соответствующего кода ошибки.

Данная команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды в связи с указанным стандартом ограничено.

TCS_126 Данная команда не вычисляет цифровую подпись ранее рассчитанного хеш-кода по команде PSO: HASH.

TCS_127 Закрытый ключ карточки используется для расчета цифровой подписи и известен карточке по косвенным признакам.

TCS_128 Приложение тахографа поколения 1 выполняет цифровую подпись с использованием метода заполнения, соответствующего PKCS1 (более подробно см. приложение подраздел 11).

TCS_129 Приложение тахографа поколения 2 рассчитывает цифровую подпись на основе эллиптической кривой (более подробно см. приложение подраздел 11).

TCS_130 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Выполнение операции по безопасности
P1	1	'9Eh'	Цифровая подпись, подлежащая возврату
P2	1	'9Ah'	Метка: поле данных содержит данные, подлежащие подписи. Поскольку поле данных не включено, то предполагается, что эти данные уже записаны на карточке (хеширование файла)
Le	1	'NNh'	Длина ожидаемой подписи

TCS_131 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#L	L	'XX..XXh'	Подпись ранее рассчитанной хеш-функции
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда прошла, карточка выдает '9000'.
- ◆ Если выбранный закрытый ключ считается поврежденным, то статус обработки выдается в виде '6400' или '6581'.
- ◆ Если хеш-функция, рассчитанная в связи с предыдущей командой Perform Hash of File, недоступна, то статус обработки выдается в виде '6985'.

3.5.15 PSO: VERIFY DIGITAL SIGNATURE (ПРОВЕРКА ЦИФРОВОЙ ПОДПИСИ)

Эта команда используется для проверки цифровой подписи, выданной в качестве входных данных, хеш-значение которой карточке известен. Алгоритм подписи известен карточке по косвенным признакам.

Данная команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению с указанным стандартом ограничено.

Для поддержки данной команды в DF Tachograph и DF Tachograph_G2 требуется только карточка контролера.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду. В MF эта команда может быть доступной или недоступной.

TCS_132 Команда VERIFY DIGITAL SIGNATURE всегда использует открытый ключ, выбранный на основании предыдущей команды Manage Security Environment MSE (управление средой защиты): Set DST, а предыдущий хеш-код вносится командой PSO: HASH.

TCS_133 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Выполнение операции по безопасности
P1	1	'00h'	
P2	1	'A8h'	Метка: поле данных содержит объекты данных, необходимые для хеширования
Lc	1	83h 'XXh'	Длина Lc последующего поля данных
#6	1	'9Eh'	Метка для цифровой подписи
#7 или #7-#8	L	81-XXh 'NNh' или '81 NNh'	Длина цифровой подписи (L равна 2 байтам, если длина цифровой подписи превышает 127 байтов): 128 байтов, закодированных в соответствии с приложением подразделом 11, часть А , для приложения тахографа поколения 1 В зависимости от выбранной кривой для приложения тахографа поколения 2 (см. приложение подраздел 11, часть В)
#(7+L)- #(6+L+NN)	NN	'XX..XXh'	Содержание цифровой подписи

TCS_134 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда проходит, карточка выдает **‘9000’**.
- ◆ Если проверка подписи показала неправильный результат, статус обработки выдается в виде **‘6688’**. Процесс проверки описывается в **приложении подразделе 11**.
- ◆ Если открытый ключ не выбран, статус обработки выдается в виде **‘6A88’**.
- ◆ Если некоторые ожидаемые объекты данных (как указано выше) отсутствуют, статус обработки выдается в виде **‘6987’**. Это может произойти, если отсутствует одна из требуемых меток.
- ◆ Если для обработки команды хеш-код недоступен (в результате выполнения предыдущей команды PSO: Hash), статус обработки выдается в виде **‘6985’**.
- ◆ Если некоторые объекты данных неверны, статус обработки выдается в виде **‘6988’**. Это может произойти в том случае, если отсутствует одна из требуемых меток.
- ◆ Если выбранный открытый ключ считается поврежденным, статус обработки выдается в виде **‘6400’** или **‘6581’**.
- ◆ Если параметр выбранного открытого ключа (используемого для расшифровки сертификата) имеет вид CHA.LSB (CertificateHolder Authorisation.equipmentType), который не подходит для проверки цифровой подписи в соответствии с **приложением подразделом 11**, то статус обработки выдается в виде **‘6985’**.

3.5.16 ОБРАБОТКА СООБЩЕНИЯ DSRC

Данная команда используется для проверки целостности и аутентичности сообщения DSRC и для расшифровки данных, передаваемых БУ контрольному органу или мастерской через соединение DSRC. Карточка генерирует ключ шифрования и ключ MAC, используемые для защиты сообщения DSRC, как описано в **приложении подразделе 11**, часть B, глава 13.

Для поддержки данной команды в DF Tachograph требуется только контрольная карточка и карточка мастерской.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду, но главный ключ DSRC для них не предусмотрен. Таким образом, эти карточки не могут успешно выполнить эту команду и прерывают ее, выдавая соответствующий код ошибки.

В MF и/или DF Tachograph эта команда может быть доступной или недоступной. Если да, то в итоге она выдает соответствующий код ошибки.

TCS_135 Главный ключ DSRC доступен только в DF Tachograph_G2, т. е. контрольная карточка и карточка мастерской поддерживают успешное выполнение команды только в DF Tachograph_G2.

TCS_136 Команда расшифровывает только данные DSRC и проверяет криптографическую контрольную сумму, но не интерпретирует входные данные.

TCS_137 Порядок объектов данных в поле данных команды фиксируется в соответствии с настоящей спецификацией.

TCS_138 Командное сообщение

<i>Байт</i>	<i>Длина</i>	<i>Значение</i>	<i>Описание</i>
CLA	1	‘80h’	Собственный CLA
INS	1	‘2Ah’	Выполнение операции по безопасности
P1	1	‘80h’	Данные ответа: обычное значение

Байт	Длина	Значение	Описание
P2	1	'B0h'	Данные команды: обычное значение в кодировке BER-TLV и включающее объекты данных SM
Lc	1	'NNh'	Длина Lc последующего поля данных
#6-#(5+L)	L	'87h' + L ₈₇ + 'XX..XXh'	<p>DER-TLV — кодированный байт индикатора содержимого заполнения, за которым следуют зашифрованные данные тахографа. Для байта индикатора содержимого заполнения используется значение '00h' («без дополнительных указаний» согласно таблице 52 ISO/IEC 7816-4:2013). Механизм шифрования см. приложение подраздел 11, часть В, глава 13</p> <p>Допустимые значения длины L₈₇ кратны длине блока AES плюс 1 для байта индикатора содержимого заполнения, т. е. от 17 байтов до 193 байтов включительно</p> <p>Примечание: Объект данных SM с меткой '87h' см. таблицу 49 ISO/IEC 7816-4:2013</p>
		'81h' + '10h'	<p>Шаблон контрольной ссылки в кодировке DER-TLV в целях конфиденциальности, вложенный в систему конкатенации следующих элементов данных (см. добавление 1 к DSRCSecurityData и приложение подраздел 11, часть В, глава 13):</p> <p>4-х байтовая метка времени</p> <p>3-х байтовый счетчик</p> <p>8-ми байтовый серийный номер БУ</p> <p>1-байтовая версия главного ключа DSRC</p> <p>Примечание: Объект данных SM с меткой '81h' см. таблицу 49 ISO/IEC 7816-4:2013</p>
		'8Eh' + L _{8E} + 'XX..XXh'	<p>MAC в кодировке DER-TLV в сочетании с сообщением DSRC. Алгоритм и расчет MAC, см. приложение подраздел 11, часть В, глава 13</p> <p>Примечание: Объект данных SM с меткой '8Eh' см. таблицу 49 ISO/IEC 7816-4:2013</p>
5+Le+1	1	'00h'	Как указано в стандарте ISO/IEC 7816-4
TCS_139 Ответное сообщение			
Байт	Длина	Значение	Описание
#1-#L	L	'XX..XXh'	Отсутствующие (в случае ошибки) или расшифрованные данные (заполнение удалено)
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- ◆ Если команда проходит, карточка выдает ‘9000’.
- ◆ ‘6A80’ указывает на неверные параметры в поле данных команды (как и в случае, когда объекты данных не передаются в установленном порядке).
- ◆ ‘6A88’ указывает на то, что исходные данные отсутствуют, т. е. исходный главный ключ DSRC не доступен.
- ◆ ‘6900’ указывает на то, что проверка криптографической контрольной суммы или расшифровка данных дали неверный результат.
- ◆ ‘6985’ указывает на то, что 4-х байтовая временная метка, содержащаяся в поле данных команды, предшествует cardValidityBegin или отображается позже, чем cardExpiryDate.

4. Структура карточек тахографов

В настоящем пункте уточняются структуры файлов карточек тахографа для хранения доступных данных.

В нем не указываются внутренние структуры, определяемые по усмотрению изготовителя, такие как заголовки файлов, а также элементы хранения и обработки данных, необходимые только для внутреннего пользования, например, EuropeanPublicKey, CardPrivateKey, TDesSessionKey или WorkshopCardPin.

TCS_140 Карточка тахографа второго поколения хранит главный файл MF и приложение тахографа поколений 1 и 2 одного и того же типа (например, приложения карточки водителя).

TCS_141 Карточка тахографа поддерживает по крайней мере минимальное число записей, указанное для соответствующих приложений, и не поддерживает число записей, превышающее максимальное число записей, указанное для соответствующих приложений.

Максимальное и минимальное число записей в настоящей главе указывается для различных приложений. **В версии 2 карточки водителя и мастерской поколения 2 приложение 1 поколения 1 должно поддерживать максимальное число записей, указанное в TCS_150 и TCS_158.**

Условия безопасности, применяемые в правилах доступа в настоящей главе в целом, см. главу 3.3. В целом режим доступа «read» обозначает команду READ BINARY с четным и, если поддерживается, нечетным байтом INS, за исключением EF Sensor_Installation_Data на карточке мастерской, см. в этой связи **TCS_156 и TCS_160**. Режим доступа «update» обозначает команду Update Binary с четным и, если поддерживается, нечетным байтом INS, а режим доступа «select» — команду SELECT.

4.1 Главный файл MF

TCS_142 После персонализации главный файл MF должен иметь следующую постоянную структуру файла и следующие правила доступа к файлам:

Примечание: Короткий идентификатор SFID файла EF присваивается в виде десятичного числа, например значение 30 в двоичной системе соответствует величине 11 110.

Файл	ИД файла	SFID	Правила доступа	
			Считывание/выбор	Обновление
MF		'3F00h'		
└─EF	ICC	'0002h'	ALW	NEV
└─EF	IC	'0005h'	ALW	NEV
└─EF	DIR	'2F00h'	30 ALW	NEV
└─EF	ATR/INFO (условно)	'2F01h'	29 ALW	NEV
└─EF	Extended_Length	'0006h'	28 ALW	NEV
└─DF	Tachograph	'0500h'	SC1	
└─DF	Tachograph_G2		SC1	

В настоящей таблице для условия безопасности используется следующее сокращение:

SC1 ALW ИЛИ OR SM-MAC-G2

TCS_143 Все структуры EF прозрачны.

TCS_144 Главный файл MF имеет следующую структуру данных:

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
MF	63	63	184	
└─EF ICC	25	25	25	
└─┬─CardIccIdentification	25	25	25	
└─┬─┬─clockStop	1	1	1	{00}
└─┬─┬─cardExtendedSerialNumber	8	8	8	{00..00}
└─┬─┬─cardApprovalNumber	8	8	8	{20..20}
└─┬─┬─cardPersonaliserID	1	1	1	{00}
└─┬─┬─embedderIcAssemblerId	5	5	5	{00..00}
└─┬─┬─icIdentifier	2	2	2	{00 00}
└─EF IC	8	8	8	
└─┬─CardChipIdentification	8	8	8	
└─┬─┬─icSerialNumber	4	4	4	{00..00}
└─┬─┬─icManufacturingReferences	4	4	4	{00..00}
└─EF DIR	20	20	20	
└─┬─См. TCS_145	20	20	20	{00..00}
└─EF ATR/INFO	7	7	128	
└─┬─См. TCS_146	7	7	128	{00..00}
└─EF EXTENDED_LENGTH	3	3	3	
└─┬─См. TCS_147	3	3	3	{00..00}
└─DF Tachograph				
└─DF Tachograph_G2				

TCS_145 Элементарный файл EF DIR содержит следующие объекты данных, связанные с приложением: '61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54'.

TCS_146 Элементарный файл EF TR/INFO присутствует, если карточка тахографа в своем ответе ATR указывает, что поддерживает поля расширенной длины. В данном случае EF ATR/INFO содержит информационный объект данных расширенной длины (DO'7F66'), как указано в стандарте ISO/IEC 7816-4:2013, положение 12.7.1.

TCS_147 Элементарный файл расширенной длины EF Extended_Length присутствует, если карточка тахографа в своем ответе ATR указывает, что поддерживает поля расширенной длины. В данном случае EF содержит следующий объект данных: '02 01 xx', в котором значение 'xx'

показывает, поддерживаются ли поля расширенной длины в случае протокола T = 1 и/или T = 0.

Значение '01' указывает на то, что поле расширенной длины поддерживается для протокола T = 1.

Значение '10' указывает на то, что поле расширенной длины поддерживается для протокола T = 0.

Значение '11' указывает на то, что поле расширенной длины поддерживается для протоколов T = 1 и T = 0.

4.2 Приложения карточки водителя

4.2.1 Приложение карточки водителя поколения 1

TCS_148 После персонализации приложение карточки водителя поколения 1 должно иметь следующую постоянную структуру файла и правила доступа к файлам:

Файл	ИД файла	Правила доступа		
		Считывание	Выбор	Обновление
└─ DF Tachograph	'0500h'		SC1	
└─ EF Application_Identification	'0501h'	SC2	SC1	NEV
└─ EF Card_Certificate	'C100h'	SC2	SC1	NEV
└─ EF CA_Certificate	'C108h'	SC2	SC1	NEV
└─ EF Identification	'0520h'	SC2	SC1	NEV
└─ EF Card_Download	'050Eh'	SC2	SC1	SC1
└─ EF Driving_Licence_Info	'0521h'	SC2	SC1	NEV
└─ EF Events_Data	'0502h'	SC2	SC1	SC3
└─ EF Faults_Data	'0503h'	SC2	SC1	SC3
└─ EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
└─ EF Vehicles_Used	'0505h'	SC2	SC1	SC3
└─ EF Places	'0506h'	SC2	SC1	SC3
└─ EF Current_Usage	'0507h'	SC2	SC1	SC3
└─ EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─ EF Specific_Conditions	'0522h'	SC2	SC1	SC3

В настоящей таблице для условий безопасности используются следующие сокращения:

SC1 ALW ИЛИ SM-MAC-G2

SC2 ALW ИЛИ SM-MAC-G1 ИЛИ SM-MAC-G2

SC3 SM-MAC-G1 ИЛИ SM-MAC-G2

TCS_149 Все структуры EF прозрачны.

TCS_150 Приложение карточки водителя поколения 1 имеет следующую структуру данных:

Файл/элемент данных	Количество записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
└─ DF DF Tachograph		11378	24926	
└─ EF Application_Identification		10	10	
└─ DriverCardApplicationIdentification		10	10	
└─ typeOfTachographCardId		1	1	{00}
└─ cardStructureVersion		2	2	{00 00}
└─ noOfEventsPerType		1	1	{00}
└─ noOfFaultsPerType		1	1	{00}
└─ activityStructureLength		2	2	{00 00}

Файл/элемент данных	Количество записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
└─ noOfCardVehicleRecords		2	2	{00 00}
└─ noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		194	194	
└─ CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
└─ MemberStateCertificate		194	194	{00..00}
EF Identification		143	143	
└─ CardIdentification		65	65	
└─ cardIssuingMemberState		1	1	{00}
└─ cardNumber		16	16	{20..20}
└─ cardIssuingAuthorityName		36	36	{00,20..20}
└─ cardIssueDate		4	4	{00..00}
└─ cardValidityBegin		4	4	{00..00}
└─ cardExpiryDate		4	4	{00..00}
└─ DriverCardHolderIdentification		78	78	
└─ cardHolderName		72	72	
└─ holderSurname		36	36	{00, 20..20}
└─ holderFirstNames		36	36	{00, 20..20}
└─ cardHolderBirthDate		4	4	{00..00}
└─ cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		4	4	
└─ LastCardDownload		4	4	{00...00}
EF Driving_Licence_Info		53	53	
└─ CardDrivingLicenceInformation		53	53	
└─ drivingLicenceIssuingAuthority		36	36	{00, 20..20}
└─ drivingLicenceIssuingNation		1	1	{00}
└─ drivingLicenceNumber		16	16	{20..20}
EF Events_Data		864	1728	
└─ CardEventData		864	1728	
└─ cardEventRecords	6	144	288	
└─ CardEventRecord	n ₁	24	24	
└─ eventType		1	1	{00}
└─ eventBeginTime		4	4	{00..00}
└─ eventEndTime		4	4	{00..00}
└─ eventVehicleRegistration				
└─ vehicleRegistrationNation		1	1	{00}
└─ vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		576	1152	
└─ CardFaultData		576	1152	
└─ cardFaultRecords	2	288	576	
└─ CardFaultRecord	n ₂	24	24	
└─ faultType		1	1	{00}
└─ faultBeginTime		4	4	{00..00}
└─ faultEndTime		4	4	{00..00}
└─ faultVehicleRegistration				
└─ vehicleRegistrationNation		1	1	{00}
└─ vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		5548	13780	
└─ CardDriverActivity		5548	13780	
└─ activityPointerOldestDayRecord		2	2	{00 00}
└─ activityPointerNewestRecord		2	2	{00 00}
└─ activityDailyRecords	n ₆	5544	13776	{00..00}
EF Vehicles_Used		2606	6202	
└─ CardVehiclesUsed		2606	6202	
└─ vehiclePointerNewestRecord		2	2	{00 00}
└─ cardVehicleRecords		2604	6200	
└─ CardVehicleRecord	n ₃	31	31	

Файл/элемент данных	Количество записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		841	1121	
CardPlaceDailyWorkPeriod		841	1121	
placePointerNewestRecord		1	1	{00}
placeRecords		840	1120	
PlaceRecord	n ₄	10	10	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		19	19	
CardCurrentUse		19	19	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
CardControlActivityDataRecord		46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		280	280	
SpecificConditionRecord	56	5	5	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_151 Следующие значения, используемые для указания размеров в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые необходимы в структуре данных карточки водителя для работы приложения поколения 1:

	Мин.	Макс.
n ₁ NoOfEventsPerType	6	12
n ₂ NoOfFaultsPerType	12	24
n ₃ NoOfCardVehicleRecords	84	200
n ₄ NoOfCardPlaceRecords	84	112
n ₆ CardActivityLengthRange	5 544 байта (28 дней * 93 изменения вида деятельности)	13 776 байтов (28 дней * 240 изменений вида деятельности)

4.2.2 Приложение карточки водителя поколения 2

TCS_152 После персонализации приложение карточки водителя поколения 2 должно иметь следующую постоянную структуру файлов и правила доступа к файлам.

Примечания:-

- Короткий идентификатор SFID файла EF присваивается как десятичное число, например значение 30 в двоичной системе соответствует величине 11 110.
- EF Application_Identification_V2, EF Places_Authentication, EF GNSS_Places_Authentication, EF Border_Crossings, EF Load_Unload_Operations, EF VU_Configuration и EF Load_Type_Entries присутствуют только в версии 2 карточки водителя поколения 2.
- Атрибут cardStructureVersion в EF Application_Identification равен {01 01} для версии 2 карточки водителя поколения 2, тогда как для версии 1 карточки водителя поколения 2 он был равен {01 00}.

Файл	Идентификатор файла	SFID	Правила доступа	
			Чтение/выбор	Обновление
└─ DF Tachograph_G2			SC1	
└─ EF Application_Identification	'0501h'	1	SC1	NEV
└─ EF CardMA_Certificate	'C100h'	2	SC1	NEV
└─ EF CardSignCertificate	'C101h'	3	SC1	NEV
└─ EF CA_Certificate	'C108h'	4	SC1	NEV
└─ EF Link_Certificate	'C109h'	5	SC1	NEV
└─ EF Identification	'0520h'	6	SC1	NEV
└─ EF Card_Download	'050Eh'	7	SC1	SC1
└─ EF Driving_Licence_Info	'0521h'	10	SC1	NEV
└─ EF Events_Data,	'0502h'	12	SC1	SM-MAC-G2
└─ EF Faults_Data,	'0503h'	13	SC1	SM-MAC-G2
└─ EF Driver_Activity_Data,	'0504h'	14	SC1	SM-MAC-G2
└─ EF Vehicles_Used,	'0505h'	15	SC1	SM-MAC-G2
└─ EF Places	'0506h'	16	SC1	SM-MAC-G2
└─ EF Current_Usage	'0507h'	17	SC1	SM-MAC-G2
└─ EF Control_Activity_Data	'0508h'	18	SC1	SM-MAC-G2
└─ EF Specific_Conditions	'0522h'	19	SC1	SM-MAC-G2
└─ EF VehicleUnits_Used	'0523h'	20	SC1	SM-MAC-G2
└─ EF GNSS_Places	'0524h'	21	SC1	SM-MAC-G2

Файл	ИД файла	SFID	Правила доступа	
			Считывание/выбор	Обновление
└─ DF Tachograph_G2			SC1	
└─ EF Application_Identification	'0501h'	1	SC1	NEV
└─ EF CardMA Certificate	'C100h'	2	SC1	NEV
└─ EF CardSignCertificate	'C101h'	3	SC1	NEV
└─ EF CA_Certificate	'C108h'	4	SC1	NEV
└─ EF Link_Certificate	'C109h'	5	SC1	NEV
└─ EF Identification	'0520h'	6	SC1	NEV
└─ EF Card_Download	'050Eh'	7	SC1	SC1
└─ EF Driving_Licence_Info	'0521h'	10	SC1	NEV
└─ EF Events_Data	'0502h'	12	SC1	SM-MAC-G2
└─ EF Faults_Data	'0503h'	13	SC1	SM-MAC-G2
└─ EF Driver_Activity_Data	'0504h'	14	SC1	SM-MAC-G2
└─ EF Vehicles_Used	'0505h'	15	SC1	SM-MAC-G2
└─ EF Places	'0506h'	16	SC1	SM-MAC-G2
└─ EF Current_Usage	'0507h'	17	SC1	SM-MAC-G2

Файл	ИД файла	SFID	Правила доступа	
			Считывание/выбор	Обновление
— EF Control_Activity_Data	'0508h'	18	SC1	SM-MAC-G2
— EF Specific_Conditions	'0522h'	19	SC1	SM-MAC-G2
— EF VehicleUnits_Used	'0523h'	20	SC1	SM-MAC-G2
— EF GNSS_Places	'0524h'	21	SC1	SM-MAC-G2
— EF Application_Identification_V2	'0525h'	22	SC1	NEV
— EF Places_Authentication	'0526h'	23	SC1	SM-MAC-G2
— EF GNSS_Places_Authentication	'0527h'	24	SC1	SM-MAC-G2
— EF Border_Crossings	'0528h'	25	SC1	SM-MAC-G2
— EF Load_Unload_Operations	'0529h'	26	SC1	SM-MAC-G2
— EF Load_Type_Entries	'0530h'	27	SC1	SM-MAC-G2
— EF Vu_Configuration	'0540h'	30	SC5/SC1	SM-MAC-G2

В настоящей таблице для условий безопасности используются следующие сокращения:

SC1 ALW ИЛИ SM-MAC-G2

SC5 Для команды Read Binary с четным байтом INS: SM-C-MAC-G2 AND SM-R-ENC-MAC-G2

Для команды Read Binary с нечетным байтом INS (если поддерживается):

TCS_153 Структуры всех файлов EF должны быть прозрачны.

TCS_154 Приложение карточки водителя поколения 2 имеет следующую структуру данных:

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
DF				
Tachograph_G2		98300	98848	
EF Application_Identification		17	17	
DriverCardApplicationIdentification		17	17	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{01 01}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00 00}
noOfGNSSADRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00 00}
noOfCardVehicleUnitRecords		2	2	{00 00}
EF CardMA_Certificate		204	341	
CardMA_Certificate		204	341	{00..00}
EF CardSignCertificate		204	341	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		204	341	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		204	341	
LinkCertificate		204	341	{00..00}
EF Identification		143	143	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
DriverCardHolderIdentification		78	78	
cardHolderName		72	72	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		4	4	
LastCardDownload		4	4	{00..00}
EF Driving_Licence_Info		53	53	
CardDrivingLicenceInformation		53	53	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		3168	3168	
CardEventData		3168	3168	
cardEventRecords	11	288	288	
CardEventRecord	n1	24	24	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		1152	1152	
CardFaultData		1152	1152	
cardFaultRecords	2	576	576	
CardFaultRecord	n2	24	24	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		13780	13780	
CardDriverActivity		13780	13780	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n6	13776	13776	{00..00}
EF Vehicles_Used		9602	9602	
CardVehiclesUsed		9602	9602	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		9600	9600	
cardVehicleRecord	n3	48	48	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		17	17	{20..20}
EF Places		2354	2354	
CardPlaceDailyWorkPeriod		2354	2354	
placePointerNewestRecord		2	2	{00 00}
placeRecords		2352	2352	
PlaceRecord	n4	21	21	

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
entryGNSSPlaceRecord		11	11	
timestamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
EF Current_Usage		19	19	
CardCurrentUse		19	19	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
CardControlActivityDataRecord		46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		562	562	
SpecificConditions		562	562	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		560	560	
SpecificConditionRecord	n9	5	5	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		2002	2002	
CardVehicleUnitsUsed		2002	2002	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		2000	2000	
CardVehicleUnitRecord	n7	10	10	
timestamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		6050	6050	
GNSSAccumulatedDriving		6050	6050	
gnssADPointerNewestRecord		2	2	{00 00}
gnssAccumulatedDrivingRecords		6048	6048	
GNSSAccumulatedDrivingRecord	n8	18	18	
timestamp		4	4	{00..00}
gnssPlaceRecord		14	14	
timestamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
EF Application_Identification_V2		10	10	
DriverCardApplicationIdentificationV2		10	10	
lengthOfFollowingData		2	2	{00 00}
noOfBorderCrossingRecords		2	2	{00 00}
noOfLoadUnloadRecords		2	2	{00 00}
noOfLoadTypeEntryRecords		2	2	{00 00}
VuConfigurationLengthRange		2	2	{00 00}
EF Places_Authentication		562	562	
CardPlaceAuthDailyWorkPeriod		562	562	
placeAuthPointerNewestRecord		2	2	{00 00}
placeAuthStatusRecords		560	560	
PlaceAuthStatusRecord	n4	5	5	
entryTime		4	4	{00..00}
authenticationStatus		1	1	{00}
EF GNSS_Places_Authentication		1682	1682	
GNSSAuthAccumulatedDriving		1682	1682	
gnssAuthADPointerNewestRecord		2	2	{00 00}
gnssAuthStatusADRecords		1680	1680	
GNSSAuthStatusADRecord	n8	5	5	
timestamp		4	4	{00..00}
authenticationStatus		1	1	{00}
EF Border_Crossings		19042	19042	
CardBorderCrossings		19042	19042	
borderCrossingPointerNewestRecord		2	2	{00 00}
cardBorderCrossingRecords		19040	19040	
CardBorderCrossingRecord	n10	17	17	
countryLeft		1	1	{00}
countryEntered		1	1	{00}
gnssPlaceAuthRecord		12	12	
timestamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
authenticationStatus		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Load_Unload_Operations		32482	32482	
CardLoadUnloadOperations		32482	32482	
loadUnloadPointerNewestRecord		2	2	{00 00}
cardloadUnloadRecords		32480	32480	
CardLoadUnloadRecord	n11	20	20	
Timestamp		4	4	{00}
operationType		1	1	{00..00}
gnssPlaceAuthRecord		12	12	
timestamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
authenticationStatus		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Load_Type_Entries		1682	1682	
CardLoadTypeEntries		1682	1682	
loadtypeEntryPointerNewestRecord		2	2	{00 00}
cardLoadTypeEntryRecords		1680	1680	
CardLoadTypeEntryRecord	n12	5	5	
Timestamp		4	4	{00..00}
loadTypeEntered		1	1	{00}
EF VU_Configuration		3072	3072	
VuConfigurations	n13	3072	3072	

TCS_155 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки водителя в приложении второго поколения:

		Мин.	Макс.
n ₁	NoOfEventsPerType	612	12
n ₂	NoOfFaultsPerType	1224	24
n ₃	NoOfCardVehicleRecords	84200	200
n ₄	NoOfCardPlaceRecords	84112	112
n ₆	CardActivityLengthRange	5-544 13 776 байтов (28-56 дней * 93-117 изменений деятельности)	13 776 байтов (28-56 дней * 240-117 изменений деятельности)
n ₇	NoOfCardVehicleUnitRecords	84200	200
n ₈	NoOfGNSSCDRRecords NoOfGNSSADRecords	252336	336
n ₉	NoOfSpecificConditionRecords	56112	112
n ₁₀	NoOfBorderCrossingRecords	1120	1 120
n ₁₁	NoOfLoadUnloadRecords	1 624	1 624
n ₁₂	NoOfLoadTypeEntryRecords	336	336
n ₁₃	VuConfigurationLengthRange	3 072 байтов	3 072 байтов

Файл	ИД файла	Правила доступа		
		Считывание	Выбор	Обновление
└ DF Tachograph	'0500h'		SC1	
└ EF Application_Identification	'0501h'	SC2	SC1	NEV
└ EF Card_Certificate	'C100h'	SC2	SC1	NEV
└ EF CA_Certificate	'C108h'	SC2	SC1	NEV
└ EF Identification	'0520h'	SC2	SC1	NEV
└ EF Card_Download	'0509h'	SC2	SC1	SC1
└ EF Calibration	'050Ah'	SC2	SC1	SC3
└ EF Sensor_Installation_Data	'050Bh'	SC4	SC1	NEV
└ EF Events_Data	'0502h'	SC2	SC1	SC3
└ EF Faults_Data	'0503h'	SC2	SC1	SC3
└ EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
└ EF Vehicles_Used	'0505h'	SC2	SC1	SC3
└ EF Places	'0506h'	SC2	SC1	SC3
└ EF Current Usage	'0507h'	SC2	SC1	SC3
└ EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└ EF Specific_Conditions	'0522h'	SC2	SC1	SC3

4.3 Приложения карточки мастерской

4.3.1 Приложение контрольной карточки поколения 1

TCS_156 После персонализации приложение карточки мастерской поколения 1 должно иметь следующую постоянную структуру файлов и правила доступа к файлам:

В настоящей таблице для условий безопасности используются следующие сокращения:

SC1 ALW ИЛИ SM-MAC-G2

SC2 ALW ИЛИ SM-MAC-G1 ИЛИ SM-MAC-G2

SC3 SM-MAC-G1 ИЛИ SM-MAC-G2

SC4 Для команды READ BINARY с четным байтом INS:

(SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR

(SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)

Для команды READ BINARY с нечетным байтом INS (если поддерживается): NEV

TCS_157 Все структуры EF прозрачны.

TCS_158 Приложение карточки мастерской поколения 1 имеет следующую структуру данных:

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
DF Tachograph		11055	29028	
EF Application_Identification		11	11	
└ WorkshopCardApplicationIdentification		11	11	
└ typeOfTachographCardId		1	1	{00}
└ cardStructureVersion		2	2	{00 00}
└ noOfEventsPerType		1	1	{00}
└ noOfFaultsPerType		1	1	{00}
└ activityStructureLength		2	2	{00 00}
└ noOfCardVehicleRecords		2	2	{00 00}
└ noOfCardPlaceRecords		1	1	{00}
└ noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		194	194	
└ CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
└ MemberStateCertificate		194	194	{00..00}
EF Identification		211	211	
└ CardIdentification		65	65	
└ cardIssuingMemberState		1	1	{00}
└ cardNumber		16	16	{20..20}
└ cardIssuingAuthorityName		36	36	{00, 20..20}
└ cardIssueDate		4	4	{00..00}
└ cardValidityBegin		4	4	{00..00}
└ cardExpiryDate		4	4	{00..00}
└ WorkshopCardHolderIdentification		146	146	
└ workshopName		36	36	{00, 20..20}
└ workshopAddress		36	36	{00, 20..20}
└ cardHolderName				
└ holderSurname		36	36	{00, 20..20}
└ holderFirstNames		36	36	{00, 20..20}
└ cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		2	2	
└ NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		9243	26778	
└ WorkshopCardCalibrationData		9243	26778	
└ calibrationTotalNumber		2	2	{00 00}
└ calibrationPointerNewestRecord		1	1	{00}
└ calibrationRecords		9240	26775	
└ WorkshopCardCalibrationRecord	n5	105	105	
└ calibrationPurpose		1	1	{00}
└ vehicleIdentificationNumber		17	17	{20..20}
└ vehicleRegistration				
└ vehicleRegistrationNation		1	1	{00}
└ vehicleRegistrationNumber		14	14	{00, 20..20}
└ wVehicleCharacteristicConstant		2	2	{00 00}

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
└─ kConstantOfRecordingEquipment		2	2	{00 00}
└─ lTyreCircumference		2	2	{00 00}
└─ tyreSize		15	15	{20..20}
└─ authorisedSpeed		1	1	{00}
└─ oldOdometerValue		3	3	{00..00}
└─ newOdometerValue		3	3	{00..00}
└─ oldTimeValue		4	4	{00..00}
└─ newTimeValue		4	4	{00..00}
└─ nextCalibrationDate		4	4	{00..00}
└─ vuPartNumber		16	16	{20..20}
└─ vuSerialNumber		8	8	{00..00}
└─ sensorSerialNumber		8	8	{00..00}
EF Sensor_Installation_Data		16	16	
└─ SensorInstallationSecData		16	16	{00..00}
EF Events_Data		432	432	
└─ CardEventData		432	432	
└─ cardEventRecords	6	72	72	
└─ CardEventRecord	n1	24	24	
└─ event_type		1	1	{00}
└─ eventBeginTime		4	4	{00..00}
└─ eventEndTime		4	4	{00..00}
└─ eventVehicleRegistration				
└─ vehicleRegistrationNation		1	1	{00}
└─ vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		288	288	
└─ CardFaultData		288	288	
└─ cardFaultRecords	2	144	144	
└─ CardFaultRecord	n2	24	24	
└─ faultType		1	1	{00}
└─ faultBeginTime		4	4	{00..00}
└─ faultEndTime		4	4	{00..00}
└─ faultVehicleRegistration				
└─ vehicleRegistrationNation		1	1	{00}
└─ vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		202	496	
└─ CardDriverActivity		202	496	
└─ activityPointerOldestDayRecord		2	2	{00 00}
└─ activityPointerNewestRecord		2	2	{00 00}
└─ activityDailyRecords	n6	198	492	{00..00}
EF Vehicles_Used		126	250	
└─ CardVehiclesUsed		126	250	
└─ vehiclePointerNewestRecord		2	2	{00 00}
└─ cardVehicleRecords		124	248	
└─ CardVehicleRecord	n3	31	31	
└─ vehicleOdometerBegin		3	3	{00..00}
└─ vehicleOdometerEnd		3	3	{00..00}
└─ vehicleFirstUse		4	4	{00..00}
└─ vehicleLastUse		4	4	{00..00}
└─ vehicleRegistration				
└─ vehicleRegistrationNation		1	1	{00}
└─ vehicleRegistrationNumber		14	14	{00, 20..20}
└─ vuDataBlockCounter		2	2	{00 00}
EF Places		61	81	
└─ CardPlaceDailyWorkPeriod		61	81	
└─ placePointerNewestRecord		1	1	{00}
└─ placeRecords		60	80	
└─ PlaceRecord	n4	10	10	

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		19	19	
CardCurrentUse		19	19	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
CardControlActivityDataRecord		46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		10	10	
SpecificConditionRecord	2	5	5	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки мастерской в приложении поколения 1:

		Мин.	Макс.
n ₁	NoOfEventsPerType	3	3
n ₂	NoOfFaultsPerType	6	6
n ₃	NoOfCardVehicleRecords	4	8
n ₄	NoOfCardPlaceRecords	6	8
n ₅	NoOfCalibrationRecords	88	255
n ₆	CardActivityLengthRange	198 байтов (1 день * 93 изменения видов деятельности)	492 байта (1 день * 240 изменений видов деятельности)

4.3.2 Приложение карточки мастерской поколения 2

TCS_160 После персонализации приложение карточки мастерской поколения 2 должно иметь следующую постоянную структуру файлов и правила доступа к файлам:

Примечания:

- Короткий идентификатор SFID файла EF присваивается как десятичное число, например значение 30 в двоичной системе соответствует величине — 11110.
- **EF Application_Identification_V2, EF Places_Authentication, EF GNSS_Places_Authentication, EF Border_Crossings, EF Load_Unload_Operations, EF Load_Type_Entries, EF VU_Configuration** и **EF Calibration_Add_Data** присутствуют только в версии 2 карточки мастерской поколения 2.

- cardStructureVersion в EF Application_Identification равна {01 01} для версии 2 карточки мастерской поколения 2, в то время как для версии 1 карточки мастерской поколения 2 она была равна {01 00}.

Файл	Ид файла	SFID	Правила доступа		
			Чтение	Выбор	Обновление
└ DF Tachograph_G2			SC1	SC1	
├ EF Application_Identification	'0501h'	1	SC1	SC1	NEV
├ EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
├ EF CardSignCertificate	'C101h'	3	SC1	SC1	NEV
├ EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
├ EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
├ EF Identification	'0520h'	6	SC1	SC1	NEV
├ EF Card_Download	'0509h'	7	SC1	SC1	SC1
├ EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
├ EF Sensor_Installation_Data	'050Bh'	11	SC5	SM-MAC-	NEV
├ EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
├ EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
├ EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
├ EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
├ EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
├ EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
├ EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
├ EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
├ EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
├ EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2

Файл	Ид файла	SFID	Правила доступа		
			Чтение	Выбор	Обновление
└ DF Tachograph_G2			SC1	SC1	
├ EF Application_Identification	'0501h'	1	SC1	SC1	NEV
├ EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
├ EF CardSignCertificate	'C101h'	3	SC1	SC1	NEV
├ EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
├ EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
├ EF Identification	'0520h'	6	SC1	SC1	NEV
├ EF Card_Download	'0509h'	7	SC1	SC1	SC1
├ EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
├ EF Sensor_Installation_Data	'050Bh'	11	SC5	SM-MAC-G2	NEV
├ EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
├ EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
├ EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
├ EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
├ EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
├ EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
├ EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
├ EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
├ EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
├ EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2
├ EF Application_Identification_V2	'0525h'	22	SC1	SC1	NEV
├ EF Places_Authentication	'0526h'	23	SC1	SC1	SM-MAC-G2
├ EF GNSS_Places_Authentication	'0527h'	24	SC1	SC1	SM-MAC-G2
├ EF Border_Crossings	'0528h'	25	SC1	SC1	SM-MAC-G2
├ EF Load_Unload_Operations	'0529h'	26	SC1	SC1	SM-MAC-G2
├ EF Load_Type_Entries	'0530h'	27	SC1	SC1	SM-MAC-G2
├ EF Calibration_Add_Data	'0531h'	28	SC1	SC1	SM-MAC-G2
├ EF VU_Configuration	'0540h'	30	SC5	SC1	SM-MAC-G2

В настоящей таблице для условий безопасности используются следующие сокращения:

SC1 ALW ИЛИ SM-MAC-G2

SC5 Для команды READ BINARY с четным байтом INS: SM-C-MAC-G2 и SM-R-ENC-MAC-G2

Для команды READ BINARY с нечетным байтом INS (если поддерживается):NEV

TCS_161 Все структуры EF прозрачны.

TCS_162 Приложение карточки мастерской поколения 2 имеет следующую структуру данных:

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
DF Tachograph_G2		18783	49787	
EF Application_Identification		19	19	
WorkshopCardApplicationIdentification		19	19	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00..00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00..00}
noOfCardVehicleRecords		2	2	{00..00}
noOfCardPlaceRecords		2	2	{00..00}
noOfCalibrationRecords		2	2	{00..00}
noOfGNSSADRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
noOfCardVehicleUnitRecords		2	2	{00..00}
EF CardMA_Certificate			341	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		204	341	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		204	341	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		204	341	
LinkCertificate		204	341	{00..00}
EF Identification		211	211	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		146	146	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20..20}
EF Card_Download		2	2	
NoOfCalibrationsSinceDownload		2	2	{00..00}
EF Calibration		15668	45394	
WorkshopCardCalibrationData		15668	45394	
calibrationTotalNumber		2	2	{00..00}
calibrationPointerNewestRecord		2	2	{00}
ecalibrationRecords		15664	45390	

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
└ WorkshopCardCalibrationRecord	n5	178	178	
└ calibrationPurpose		1	1	{00}
└ vehicleIdentificationNumber		17	17	{20..20}
└ vehicleRegistration				
└ vehicleRegistrationNation		1	1	{00}
└ vehicleRegistrationNumber		14	14	{00, 20..20}
└ wVehicleCharacteristicConstant		2	2	{00-00}
└ kConstantOfRecordingEquipment		2	2	{00-00}
└ lTyreCircumference		2	2	{00-00}
└ tyreSize		15	15	{20..20}
└ authorisedSpeed		1	1	{00}
└ oldOdometerValue		3	3	{00..00}
└ newOdometerValue		3	3	{00..00}
└ oldTimeValue		4	4	{00..00}
└ newTimeValue		4	4	{00..00}
└ nextCalibrationDate		4	4	{00..00}
└ vuPartNumber		16	16	{20..20}
└ vuSerialNumber		8	8	{00..00}
└ sensorSerialNumber		8	8	{00..00}
└ sensorGNSSSerialNumber		8	8	{00..00}
└ remSerialNumber		8	8	{00..00}
└ vuAbility		1	1	{00}
└ sealDataCard		56	56	
└ noOfSealRecords		1	1	{00}
└ SealRecords		55	55	
└ SealRecord	5	11	11	
└ equipmentType		1	1	{00}
└ extendedSealIdentifier		10	10	{00..00}
EF Sensor_Installation_Data		18	102	
└ SensorInstallationSecData		18	102	{00..00}
EF Events_Data		792	792	
└ CardEventData		792	792	
└ cardEventRecords	11	72	72	
└ CardEventRecord	n1	24	24	
└ eventTypes		1	1	{00}
└ eventBeginTime		4	4	{00..00}
└ eventEndTime		4	4	{00..00}
└ eventVehicleRegistration				
└ vehicleRegistrationNation		1	1	{00}
└ vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		288	288	
└ CardFaultData		288	288	
└ cardFaultRecords	2	144	144	
└ CardFaultRecord	n2	24	24	
└ faultType		1	1	{00}
└ faultBeginTime		4	4	{00..00}
└ faultEndTime		4	4	{00..00}
└ faultVehicleRegistration				
└ vehicleRegistrationNation		1	1	{00}
└ vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		202	496	
└ CardDriverActivity		202	496	
└ activityPointerOldestDayRecord		2	2	{00-00}
└ activityPointerNewestRecord		2	2	{00-00}
└ activityDailyRecords	n6	198	492	{00..00}
EF Vehicles_Used		194	386	
└ CardVehiclesUsed		194	386	

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
vehiclePointerNewestRecord		2	2	{00..00}
cardVehicleRecords		192	384	
CardVehicleRecord	n3	48	48	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00..00}
vehicleIdentificationNumber		17	17	{20..20}
EF Places		128	170	
CardPlaceDailyWorkPeriod		128	170	
placePointerNewestRecord		2	2	{00..00}
placeRecords		126	168	
PlaceRecord	n4	21	21	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
entryGNSSPlaceRecord		11	11	{00..00}
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
EF Current_Usage		19	19	
CardCurrentUse		19	19	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
CardControlActivityDataRecord		46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		42	42	
CardVehicleUnitsUsed		42	82	
vehicleUnitPointerNewestRecord		2	2	{00..00}
cardVehicleUnitRecords		40	80	
CardVehicleUnitRecord	n7	10	10	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00..00}
deviceID		1	1	{00..00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		326	432	
GNSSContinuousDriving		326	434	
gnssADPointerNewestRecord		2	2	{00..00}

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
gnssAccumulatedDrivingRecords		324	432	
GNSSContinuousDrivingRecord	n8	18	18	
timeStamp		4	4	{00..00}
gnssPlaceRecord		14	14	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}
EF Specific_Conditions		12	22	
SpecificConditions		12	22	
conditionPointerNewestRecord		2	2	{00..00}
specificConditionRecords		10	20	
SpecificConditionRecord	n9	5	5	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
DF				
Tachograph_G2		59582	60214	
EF Application_Identification		19	19	
WorkshopCardApplicationIdentification		19	19	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{01 01}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00 00}
noOfCalibrationRecords		2	2	{00 00}
noOfGNSSADRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00 00}
noOfCardVehicleUnitRecords		2	2	{00 00}
EF CardMA_Certificate		204	341	
CardMA_Certificate		204	341	{00..00}
EF CardSignCertificate		204	341	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		204	341	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		204	341	
LinkCertificate		204	341	{00..00}
EF Identification		211	211	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		146	146	
workshopName		36	36	
workshopAddress		36	36	
cardHolderName		72	72	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
EF Card_Download		2	2	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		45394	45394	
WorkshopCardCalibrationData		45394	45394	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00 00}
calibrationRecords		45390	45390	
WorkshopCardCalibrationRecord	n5	178	178	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
sensorGNSSSerialNumber		8	8	{00..00}
rcmSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		56	56	
noOfSealRecords		1	1	{00}
SealRecords		55	55	
SealRecord	5	11	11	
equipmentType		1	1	{00}
extendedSealIdentifier		10	10	{00..00}
EF Sensor_Installation_Data		18	102	
SensorInstallationSecData		18	102	{00..00}
EF Events_Data		792	792	
CardEventData		792	792	
cardEventRecords	11	72	72	
CardEventRecord	n1	24	24	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		288	288	
CardFaultData		288	288	
cardFaultRecords	2	144	144	
CardFaultRecord	n2	24	24	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
EF Driver_Activity_Data		496	496	
CardDriverActivity		496	496	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n6	492	492	{00..00}
EF Vehicles_Used		386	386	
CardVehiclesUsed		386	386	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		384	384	
cardVehicleRecord	n3	48	48	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		17	17	{20..20}
EF Places		170	170	
CardPlaceDailyWorkPeriod		170	170	
placePointerNewestRecord		2	2	{00 00}
placeRecords		168	168	
PlaceRecord	n4	21	21	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
entryGNSSPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
EF Current_Usage		19	19	
CardCurrentUse		19	19	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
CardControlActivityDataRecord		46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		82	82	
CardVehicleUnitsUsed		82	82	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		80	80	
CardVehicleUnitRecord	n7	10	10	

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		434	434	
GNSSAccumulatedDriving		434	434	
gnssADPointerNewestRecord		2	2	{00 00}
gnssAccumulatedDrivingRecords		432	432	
GNSSAccumulatedDrivingRecord	n8	18	18	
timeStamp		4	4	{00..00}
gnssPlaceRecord		14	14	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}
EF Specific_Conditions		22	22	
SpecificConditions		22	22	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		20	20	
SpecificConditionRecord	n9	5	5	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF Application_Identification_V2		10	10	
WorkshopCardApplicationIdentificationV2		10	10	
LengthOfFollowingData		2	2	{00 00}
noOfBorderCrossingRecords		2	2	{00 00}
noOfLoadUnloadRecords		2	2	{00 00}
noOfLoadTypeEntryRecords		2	2	{00 00}
VuConfigurationLengthRange		2	2	{00 00}
EF Places_Authentication		42	42	
CardPlaceAuthDailyWorkPeriod		42	42	
placeAuthPointerNewestRecord		2	2	{00 00}
placeAuthStatusRecords		40	40	
PlaceAuthStatusRecord	n4	5	5	
entryTime		4	4	{00..00}
authenticationStatus		1	1	{00}
EF GNSS_Places_Authentication		122	122	
GNSSAuthAccumulatedDriving		122	122	
gnssAuthADPointerNewestRecord		2	2	{00 00}
gnssAuthStatusADRecords		120	120	
GNSSAuthStatusADRecord	n8	5	5	
timeStamp		4	4	{00..00}
authenticationStatus		1	1	{00}
EF Border_Crossings		70	70	
CardBorderCrossings		70	70	
borderCrossingPointerNewestRecord		2	2	{00 00}
cardBorderCrossingRecords		68	68	
CardBorderCrossingRecord	n10	17	17	
countryLeft		1	1	{00}
countryEntered		1	1	{00}
gnssPlaceAuthRecord		12	12	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
authenticationStatus		1	1	{00}
vehicleOdometerValue		3	3	{00..00}

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
EF Load_Unload_Operations		162	162	
CardLoadUnloadOperations		162	162	
loadUnloadPointerNewestRecord		2	2	{00 00}
cardloadUnloadRecords		160	160	
CardLoadUnloadRecord	n11	20	20	
timestamp		4	4	{00}
operationType		1	1	{00..00}
gnssPlaceAuthRecord		12	12	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
authenticationStatus		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Load_Type_Entries		22	22	
CardLoadTypeEntries		22	22	
loadtypeEntryPointerNewestRecord		2	2	{00 00}
cardLoadTypeEntryRecords		20	20	
CardLoadTypeEntryRecord	n12	5	5	
Timestamp		4	4	{00..00}
loadTypeEntered		1	1	{00}
EF Calibration_Add_Data		6887	6887	
WorkshopCardCalibrationAddData		6887	6887	
calibrationPointerNewestRecord		2	2	{00 00}
workshopCardCalibrationAddData		6885	6885	
Records		6885	6885	
WorkshopCardCalibrationAddDataRecord	n5	27	27	
oldTimeValue		4	4	{00..00}
vehicleIdentificationNumber		17	17	{20..20}
byDefaultLoadType		1	1	{00}
calibrationCountry		1	1	{00}
calibrationCountryTimestamp		4	4	{00..00}
EF VU_Configuration		3072	3072	
VuConfigurations	n13	3072	3072	

TCS_163 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки мастерской в приложении поколения 2:

		Мин.	Макс.
n1	NoOfEventsPerType	3	3
n2	NoOfFaultsPerType	6	6
n3	NoOfCardVehicleRecords	48	8
n4	NoOfCardPlaceRecords	68	8
n5	NoOfCalibrationRecords	88255	255
n6	CardActivityLengthRange	498492 байтов 1 (1 день * 93240 изменений деятельности)	492 байта (1 день * 240 изменений деятельности)
n7	NoOfCardVehicleUnitRecords	48	8
n8	NoOfGNSSCDRRecords NoOfGNSSADRecords	1824	24
n9	NoOfSpecificConditionRecords	24	4
n10	NoOfBorderCrossingRecords	4	4
n11	NoOfLoadUnloadRecords	8	8
n12	NoOfLoadTypeEntryRecords	4	4
n13	VuConfigurationLengthRange	3 072 байта	3 072 байта

4.4 Приложения контрольной карточки

4.4.1 Приложение контрольной карточки поколения 1

TCS_164 После персонализации приложение карточки мастерской поколения 1 должно иметь следующую постоянную структуру файлов и правила доступа к файлам:

Файл	ИД	Правила доступа		
		Считывание	Выбор	Обновление
└DF Tachograph	'0500h'			
└└EF Application_Identification	'0501h'	SC2	SC1	NEV
└└EF Card_Certificate	'C100h'	SC2	SC1	NEV
└└EF CA_Certificate	'C108h'	SC2	SC1	NEV
└└EF Identification	'0520h'	SC6	SC1	NEV
└└EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

В настоящей таблице для условий безопасности используются следующие сокращения:

SC1 ALW OR SM-MAC-G2
SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2
SC3 SM-MAC-G1 OR SM-MAC-G2
SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_165 Все структуры EF должны быть прозрачны.

TCS_166 Приложение карточки контролера поколения 1 имеет следующую структуру данных:

Файл/элемент данных	Число записей	Размер (байты)	
		Мин.	Макс.
└DF Tachograph		11186	24526
└└EF Application_Identification		5	5
└└└ControlCardApplicationIdentification		5	5
└└└└typeOfTachographCardId		1	1 {00}
└└└└cardStructureVersion		2	2 {00 00}
└└└└noOfControlActivityRecords		2	2 {00 00}
└└EF Card_Certificate		194	194
└└└CardCertificate		194	194 {00..00}
└└EF CA_Certificate		194	194
└└└MemberStateCertificate		194	194 {00..00}
└└EF Identification		211	211
└└└CardIdentification		65	65
└└└└cardIssuingMemberState		1	1 {00}
└└└└cardNumber		16	16 {20..20}
└└└└cardIssuingAuthorityName		36	36 {00, 20..20}
└└└└cardIssueDate		4	4 {00..00}
└└└└cardValidityBegin		4	4 {00..00}
└└└└cardExpiryDate		4	4 {00..00}
└└└ControlCardHolderIdentification		146	146
└└└└controlBodyName		36	36 {00, 20..20}
└└└└controlBodyAddress		36	36 {00, 20..20}
└└└└cardHolderName			
└└└└└holderSurname		36	36 {00, 20..20}
└└└└└holderFirstNames		36	36 {00, 20..20}
└└└└cardHolderPreferredLanguage		2	2 {20 20}
└└EF Controller_Activity_Data		10582	23922
└└└ControlCardControlActivityData		10582	23922
└└└└controlPointerNewestRecord		2	2 {00 00}

Файл/элемент данных	Число записей	Размер (байты)		
		Мин.	Макс.	
└─controlActivityRecords		10580	23920	
└─┬─controlActivityRecord	n7	46	46	
└─┬─┬─controlType		1	1	{00}
└─┬─┬─controlTime		4	4	{00..00}
└─┬─┬─controlledCardNumber				
└─┬─┬─┬─cardType		1	1	{00}
└─┬─┬─┬─cardIssuingMemberState		1	1	{00}
└─┬─┬─┬─cardNumber		16	16	{20..20}
└─┬─┬─controlledVehicleRegistration				
└─┬─┬─┬─vehicleRegistrationNation		1	1	{00}
└─┬─┬─┬─vehicleRegistrationNumber		14	14	{00, 20..20}
└─┬─controlDownloadPeriodBegin		4	4	{00..00}
└─┬─controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки контролера в приложении поколения 1:

		Мин.	Макс.
n7	NoOfControlActivityRecords	230	520

4.4.2 Приложение карточки контролера поколения 2

TCS_168 После персонализации приложение карточки контролера поколения 1 должно иметь следующую постоянную структуру файлов и правила доступа к файлам:

Примечания: -

- Короткий идентификатор SFID файла EF присваивается как десятичное число, например значение 30 в двоичной системе соответствует величине 11 110.
- **EF Application_Identification_V2** и **EF VU_Configuration** присутствуют только в версии 2 карточки контролера поколения 2.
- **cardStructureVersion** в **EF Application_Identification** равно {01 01} для версии 2 карточки контролера поколения 2, тогда как для версии 1 карточки контролера поколения 2 оно было равно {01 00}.

Файл	ИД файла	SFID	Правила доступа	
			Read/Select	Update
└─DF Tachograph_G2			SC1	
└─┬─EF Application_Identification	'0501h'	1	SC1	NEV
└─┬─EF CardMA_Certificate	'C100h'	2	SC1	NEV
└─┬─EF CA_Certificate	'C108h'	4	SC1	NEV
└─┬─EF Link_Certificate	'C109h'	5	SC1	NEV
└─┬─EF Identification	'0520h'	6	SC1	NEV
└─┬─EF Controller_Activity_Data	'050Ch'	14	SC1	SM-MAC-G2

Файл	ИД файла	SFID	Правила доступа	
			Чтение/выбор	Обновление
└─DF Tachograph_G2			SC1	
└─┬─EF Application_Identification	'0501h'	1	SC1	NEV
└─┬─EF CardMA_Certificate	'C100h'	2	SC1	NEV
└─┬─EF CA_Certificate	'C108h'	4	SC1	NEV
└─┬─EF Link_Certificate	'C109h'	5	SC1	NEV
└─┬─EF Identification	'0520h'	6	SC1	NEV

Файл	ИД файла	SFID	Правила доступа	
			Чтение/выбор	Обновление
EF Controller_Activity_Data	'050Ch'	14	SC1	SM-MAC-G2
EF Application_Identification_V2	'0525h'	22	SC1	NEV
EF VU_Configuration	'0540h'	30	SC5/SC1	SM-MAC-G2

В настоящей таблице используются следующие сокращения, применяемые к условиям безопасности:

SC1 ALW ИЛИ SM-MAC-G2

SC5 Для команды Read Binary с четным байтом — INS: SM-C-MAC-G2 и SM-R-ENC-MAC-G2

Для команды Read Binary с нечетным байтом — INS (если поддерживается): NEV

TCS_169 Все структуры EF прозрачны.

TCS_170 Приложение карточки контролера поколения 2 имеет следующую структуру данных:

Файл/элемент данных	Число записей	Размер (байты)		
		Мин.	Макс	
└ Тахограф_G2		11410	25161	
└ EF Application_Identification		5	5	
└└ ControlCardApplicationIdentification		5	5	
└└└ typeOfTachographCardId		1	1	{00}
└└└ cardStructureVersion		2	2	{00..00}
└└└ noOfControlActivityRecords		2	2	{00..00}
└ EF CardMA_Certificate		204	341	
└└ CardMACertificate		204	341	{00..00}
└ EF CA_Certificate		204	341	
└└ MemberStateCertificate		204	341	{00..00}
└ EF Link_Certificate		204	341	
└└ LinkCertificate		204	341	{00..00}
└ EF Identification		211	211	
└└ CardIdentification		65	65	
└└└ cardIssuingMemberState		1	1	{00}
└└└ cardNumber		16	16	{20..20}
└└└ cardIssuingAuthorityName		36	36	{00, 20..20}
└└└ cardIssueDate		4	4	{00..00}
└└└ cardValidityBegin		4	4	{00..00}
└└└ cardExpiryDate		4	4	{00..00}
└└ ControlCardHolderIdentification		146	146	
└└└ controlBodyName		36	36	{00, 20..20}
└└└ controlBodyAddress		36	36	{00, 20..20}
└└└ cardHolderName				
└└└└ holderSurname		36	36	{00, 20..20}
└└└└ holderFirstNames		36	36	{00, 20..20}
└└└ cardHolderPreferredLanguage		2	2	{20 20}
└ EF Controller_Activity_Data		10582	23922	
└└ ControlCardControlActivityData		10582	23922	
└└└ controlPointerNewestRecord		2	2	{00..00}
└└└ controlActivityRecords		10580	23920	
└└└└ controlActivityRecord	n7	46	46	
└└└└└ controlType		1	1	{00}
└└└└└ controlTime		4	4	{00..00}
└└└└└ controlledCardNumber				
└└└└└└ cardType		1	1	{00}
└└└└└└ cardIssuingMemberState		1	1	{00}

Файл/элемент данных	Число записей	Размер (байты)		
		Мин.	Макс.	
└─ cardNumber		16	16	{20..20}
└─ controlledVehicleRegistration				
└─ vehicleRegistrationNation		1	1	{00}
└─ vehicleRegistrationNumber		14	14	{00, 20..20}
└─ controlDownloadPeriodBegin		4	4	{00..00}
└─ controlDownloadPeriodEnd		4	4	{00..00}
DF Tachograph_G2		14486	28237	
EF Application_Identification		5	5	
ControlCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{01 01} V2
noOfControlActivityRecords		2	2	{00 00}
EF CardMA_Certificate		204	341	
CardMA_Certificate		204	341	{00..00}
EF CA_Certificate		204	341	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		204	341	
LinkCertificate		204	341	{00..00}
EF Identification		211	211	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		146	146	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		10582	23922	
ControlCardControlActivityData		10582	23922	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		10580	23920	
controlActivityRecord	n7	46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Application_Identification_V2		4	4	
ControlCardApplicationIdentificationV2		4	4	

Файл/элемент данных	Число записей	Мин.	Макс.	Значения по умолчанию
lengthOfFollowingData		2	2	{00 00}
VuConfigurationLengthRange		2	2	{00 00}
EF VuConfiguration		3072	3072	
VuConfigurations	n13	3072	3072	
TCS_171	Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки контролера в приложении поколения 2:			
		<i>Мин..</i>	<i>Макс..</i>	
n7	NoOfControlActivityRecords	230	520	
n13	VuConfigurationLengthRange	3 072 байтов	30 72 байтов	

4.5 Приложения карточки предприятия

4.5.1 Приложение карточки предприятия поколения 1

TCS_172 После персонализации приложение карточки мастерской поколения 1 должно иметь следующую постоянную структуру файлов и правила доступа к ним:

Файл	ИД файла	Правила доступа		
		Считывание	Выбор	Обновление
└ DF Tachograph	'0500h'		SC1	
└ ─ EF Application_Identification	'0501h'	SC2	SC1	NEV
└ ─ EF Card_Certificate	'C100h'	SC2	SC1	NEV
└ ─ EF CA_Certificate	'C108h'	SC2	SC1	NEV
└ ─ EF Identification	'0520h'	SC6	SC1	NEV
└ ─ EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

В настоящей таблице используются следующие сокращения, применяемые к условиям безопасности:

SC1 ALW ИЛИ SM-MAC-G2

SC2 ALW ИЛИ SM-MAC-G1 ИЛИ SM-MAC-G2

SC3 SM-MAC-G1 ИЛИ SM-MAC-G2

SC6 EXT-AUT-G1 ИЛИ SM-MAC-G1 ИЛИ SM-MAC-G2

TCS_173 Все структуры файлов EF прозрачны.

TCS_174 Приложение карточки предприятия поколения 1 имеет следующую структуру данных:

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
DF Tachograph		11114	24454	
EF Application_Identification		5	5	
CompanyCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF Card_Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		139	139	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		74	74	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		10582	23922	
CompanyActivityData		10582	23922	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		10580	23920	
companyActivityRecord	n ₈	46	46	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_175 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки предприятия в приложении поколения 1:

	Мин..	Макс..
n ₈ NoOfCompanyActivityRecords	230	520

4.5.2 Приложение карточки предприятия поколения 2

TCS_176 После персонализации приложение карточки предприятия поколения 2 имеет следующую постоянную структуру файлов и правила доступа к ним.

Примечания:

- Короткий идентификатор SFID файла EF присваивается как десятичное число, например, значение 30 в двоичной системе соответствует величине 11110.
- **EF Application_Identification_V2** и **EF VU_Configuration** присутствуют только в версии 2 карточки предприятия поколения 2.
- **cardStructureVersion** в **EF Application_Identification** равно {01 01} для версии 2 карточки предприятия поколения 2, тогда как для версии 1 карточки предприятия поколения 2 оно было равно {01 00}.

Файл	ИД файла	SFID	Доступ к правилам	
			Считывание/выбор	Обновление
└ DF Tachograph_G2			SC1	
└ EF Application_Identification	'0501h'	1	SC1	NEV
└ EF CardMA_Certificate	'C100h'	2	SC1	NEV
└ EF CA_Certificate	'C108h'	4	SC1	NEV
└ EF Link_Certificate	'C109h'	5	SC1	NEV
└ EF Identification	'0520h'	6	SC1	NEV
└ EF Company_Activity_Data	'050Dh'	14	SC1	MS-MAC-G2

Файл	ИД файла	SFID	Доступ к правилам	
			Считывание/выбор	Обновление
└ DF Tachograph_G2			SC1	
└ EF Application_Identification	'0501h'	1	SC1	NEV
└ EF CardMA_Certificate	'C100h'	2	SC1	NEV
└ EF CA_Certificate	'C108h'	4	SC1	NEV
└ EF Link_Certificate	'C109h'	5	SC1	NEV
└ EF Identification	'0520h'	6	SC1	NEV
└ EF Company_Activity_Data	'050Dh'	14	SC1	MS-MAC-G2
└ EF Application_Identification_V2	'0525h'	22	SC1	NEV
└ EF VU_Configuration	'0540h'	30	SC5/SC1	MS-MAC-G2

В настоящей таблице используются следующие сокращения, применяемые к условиям безопасности:

SC1 ALW ИЛИ SM-MAC-G2

SC5 Для команды **Read Binary** с четным байтом INS: **SM-C-MAC-G2** и **SM-R-ENC-MAC-G2**

Для команды **Read Binary** с нечетным байтом INS (если поддерживается): **NEV**

TCS_177 Все структуры файлов EF прозрачны.

TCS_178 Приложение карточки предприятия поколения 2 имеет следующую структуру данных:

Файл/элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
DF Tachograph_G2		11338	25089	
EF Application_Identification		5	5	
CompanyCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00..00}
noOfCompanyActivityRecords		2	2	{00..00}
EF CardMA_Certificate		204	341	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		204	341	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		204	341	
LinkCertificate		204	341	{00..00}
EF Identification		139	139	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		74	74	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20..20}
EF Company_Activity_Data		10582	23922	
CompanyActivityData		10582	23922	
companyPointerNewestRecord		2	2	{00..00}
companyActivityRecords		10580	23920	
companyActivityRecord	n8	46	46	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

Файл/элемент данных	Число записей	Мин.	Макс.	Значения по умолчанию
DF Tachograph_G2		14414	28165	
EF Application_Identification		5	5	
CompanyCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{01 01} V2
noOfCompanyActivityRecords		2	2	{00 00}
EF CardMA_Certificate		204	341	
CardMA_Certificate		204	341	{00..00}
EF CA_Certificate		204	341	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		204	341	
LinkCertificate		204	341	{00..00}

Файл/элемент данных	Число записей	Мин.	Макс.	Значения по умолчанию
EF Identification		139	139	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		74	74	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		10582	23922	
CompanyActivityData		10582	23922	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		10580	23920	
companyActivityRecord	n8	46	46	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}
EF Application_Identification_V2		4	4	
CompanyCardApplicationIdentificationV2		4	4	
lengthOfFollowingData		2	2	{00 00}
VuConfigurationLengthRange		2	2	{00 00}
EF VuConfiguration		3072	3072	
VuConfigurations	n13	3072	3072	

TCS_179 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки предприятия в приложении поколения 2:

		Мин..	Макс..
n8	NoOfCompanyActivityRecords	230	520
n13	VuConfigurationLengthRange	3 072 байтов	3 072 байтов

Подраздел 3








Пиктограммы

PIC_001 Тахограф может факультативно использовать следующие пиктограммы и комбинации пиктограмм (или пиктограммы и комбинации, достаточно похожие, чтобы их можно было однозначно идентифицировать):



1. Базовые пиктограммы

	<u>Люди</u>	<u>Действия</u>	<u>Режимы работы</u>
	Компания	Режим предприятия	
	Контролер	Контроль	Режим контроля
	Водитель	Управление	Рабочий режим
	Мастерская/ испытательная станция	Инспекция/калибровка	Режим калибровки
	Изготовитель		
	<u>Деятельность</u>	<u>Продолжительность</u>	
	Готовность	Текущий период готовности	
	Управление	Непрерывное время управления	
	Отдых	Текущий период отдыха	
	Другая работа	Текущий период работы	
	Перерыв	Совокупное время перерыва	
	Неизвестно		
	<u>Оборудование</u>	<u>Функции</u>	
	Считывающее устройство водителя		
	Считывающее устройство второго водителя		
	Карточка		
	Часы		
	Дисплей	Вывод на дисплей	
	Внешнее хранение	Загрузка	
	Электропитание		
	Принтер/распечатка	Печать	
	Датчик		
	Размер шин		
	Транспортное средство/ бортовое устройство		
	Устройство ГНСС		
	Средство удаленной связи		
	Интерфейс ИТС		

Особые условия, ручной ввод данных

OUT	Неприменимо
	Переезд на пароме/поезде
	Операция по загрузке
	Операция по разгрузке
	Операция по одновременной загрузке/разгрузке
	Тип груза: пассажиры
	Тип груза: товары
	Тип груза: тип груза не определен













Разное

!	События	✕	Неисправности
▶	Начало дневного периода работы	▶	Окончание дневного периода работы
+	Место		
M	Ручной ввод данных о деятельности водителя		
	Безопасность/аутентифицированные данные/пломбы		
>	Скорость		
⊖	Время		
Σ	Итого/резюме		
	Цифровая карта/пересечение границы		

Квалификаторы

24 ч	Ежесуточно
I	Еженедельно
II	Две недели
+	С или по

2. Комбинации пиктограмм**Разное**

	Место контроля		
	Место начала дневного периода работы		Место завершения дневного периода работы
	Местоположение после 3 часов накопленного времени управления		
	Начиная с		До
	Из транспортного средства		
OUT+	Начало «Неприменимо»		OUT Конец «Неприменимо»
	Место, где транспортное средство пересекло границу между двумя странами		
	Местоположение, в котором произведена операция по загрузке		
	Местоположение, в котором произведена операция по разгрузке		
	Местоположение, в котором произведена операция по одновременной загрузке/разгрузке		

Карточки

⊙■	Карточка водителя
⊙■	Карточка предприятия
⊙■	Карточка контролера
⊙■	Карточка мастерской
■ - -	Карточки нет

Управление

⊙⊙	Управление экипажем
⊙	Время управления за одну неделю
⊙	Время управления за две недели

Распечатки

24ч. ■ ▽	Ежедневная распечатка данных о деятельности водителя, записанных на карточке
24ч. ■ ▽	Деятельность водителя из ежедневной распечатки БУ
! × ■ ▽	События и неисправности из распечатки карточки
! × ▽	События и неисправности из распечатки БУ
Т ⊙ ▽	Распечатка технических данных
>> ▽	Распечатка данных о превышении скорости
■ ■ ⊙ ▽	Распечатка архива вставленных карточек

События

! ■	Ввод недействительной карточки
! ■ ■	Несовместимость карточек
! ⊙ ⊙	Нестыковка во времени
! ⊙ ■	Управление без соответствующей карточки
! ■ ⊙	Ввод карточки во время управления
! ■ ▽	Неправильное завершение последнего сеанса использования карточки
>>	Превышение скорости
! †	Прекращение электропитания
! Л	Ошибочные данные о движении
! АЛ	Противоречивые данные о движении транспортного средства
! ■	Нарушение защиты
! ⊙	Нестыковка во времени или корректировка времени (в мастерской)
>⊙	Контроль за превышением скорости
! ×	Отсутствие информации о местоположении от приемника ГНСС или ошибка связи с внешним средством ГНСС
! †	Ошибка связи со средством удаленной связи
! ×?	Аномалия ГНСС

Неисправности

- ×■1 Неисправность карточки (считывающее устройство водителя)
- ×■2 Неисправность карточки (считывающее устройство второго водителя)
- ×□ Неисправность дисплея
- ×⚡ Ошибка при загрузке
- ×⚗ Неисправность принтера
- ×Л Неисправность датчика
- ×Д Внутренние неполадки в БУ
- ×⌘ ————— неисправность ГНСС
- ×Υ Неисправность средства удаленного обнаружения

Процедура ручного ввода данных

- ⌘?⌘ Все тот же дневной период работы?
- ⌘? Окончание предыдущего периода работы?
- ⌘*? Подтвердить или ввести местоположение, в котором заканчивается период работы
- ⊖⌘? Ввести время начала
- ⌘? Ввести место, в котором начинается период работы

Примечание: Дополнительные комбинации пиктограмм, используемые в качестве идентификаторов блоков или записей данных при распечатке, представлены в подразделе 4.

Подраздел 4

Распечатки

Содержание

	<i>Стр.</i>
1. Общие положения	329
2. Спецификация блоков данных	329
3. Спецификации распечатки данных	338
3.1 Распечатка сохраненных на карточке данных о деятельности водителя за сутки	339
3.2 Распечатка сохраненных в БУ данных о деятельности водителя за сутки	340
3.3 События и неисправности из распечатки данных карточки	341
3.4 События и неисправности из распечатки БУ	341
3.5 Распечатка технических данных	342
3.6. Распечатка данных о превышении скорости	342
3.7 Архив вставленных карточек	343

1. Общие положения

Каждая распечатка составляется из следующих друг за другом блоков различных данных, которые могут быть обозначены идентификаторами блоков.

Блок данных состоит из одной или нескольких записей, которые могут быть обозначены идентификаторами записей.


- PRT_001 Если идентификатору записи непосредственно предшествует идентификатор блока данных, идентификатор записи на печать не выводится.
- PRT_002 Если элемент данных отсутствует или не подлежит распечатке в силу режима доступа к данным, вместо него распечатывается серия пробелов.
- PRT_003 Если содержание целой строки отсутствует или не подлежит в распечатке, эта строка опускается целиком.
- PRT_004 Поля числовых данных печатаются с выравниванием по правому краю; в качестве символа, отделяющего разряды тысяч и миллионов, используется пробел; начальные нули не печатаются.
- PRT_005 Поля строковых данных печатаются с выравниванием по левому краю и заполняются пробелами на всю оставшуюся длину элемента данных, а в соответствующих случаях печатаются в форме, усеченной до длины элемента данных. (**Имена и адреса могут быть напечатаны в две строки.**)
- PRT_006 В случае разрыва строки из-за длины текста в начале новой строки первым символом печатается особый знак (точка на середине высоты строки «•»).

2. Спецификации блоков данных

В тексте данной главы применяются следующие условные обозначения:

- жирным шрифтом обозначена информация, распечатываемая в текстовой форме (при распечатке используется обычный шрифт);
- обычным шрифтом указаны переменные параметры (пиктограммы или виды данных), вместо которых распечатываются их значения;
- к названиям переменных параметров добавлены символы подчеркивания, указывающие длину элемента данных, выделенного под соответствующий параметр;
- даты указываются в формате «дд/мм/гггг» (день-месяц-год). Допускается также использование формата «дд.мм.гггг»;
- под термином «идентификационные данные карточки» понимается совокупность следующих компонентов: тип карточки, обозначаемый комбинацией соответствующих пиктограмм, код ~~государства члена~~ ~~выдавшего~~ **Договаривающейся стороны, выдавшей** карточку, наклонная черта вправо и номер карточки с индексом замены и индексом возобновления, отделенными пробелом:

Р	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x	
Комбинация пиктограмм карточки		Код государства-члена, выдавшего Договаривающейся стороне, выдавшей карточку			Первые 14 знаков номера карточки (могут включать порядковый индекс)																		Индекс замены		Индекс возобновления	

- В блоке данных текст после «ri=» относится к соответствующей пиктограмме или комбинации пиктограмм, определенных в подразделе 3 добавления,
- Если пиктограмма напечатана после указания долготы и широты зарегистрированного местоположения или после метки времени, когда было определено это местоположение, эта пиктограмма  указывает, что данное место было рассчитано на основе аутентифицированных навигационных сообщений,
- * данные доступны только в тахографах поколения 2 (все версии),
- ** данные доступны только в тахографах поколения 2 версии 2.

PRT_007 При распечатке данные делятся на блоки и/или записи данных, перечисляемые ниже с указанием их значения и формата:

Номер блока или записи	Значение	Формат данных
1	<i>Дата и время распечатки документа</i>	☐ дд/мм/гггг чч:мм (UTC)
2	<i>Вид распечатки</i> Идентификатор блока данных Поколение и версия БУ** Комбинация пиктограмм, соответствующих данной распечатке (см. подраздел 3), Настройка устройства ограничения скорости (только при распечатке данных о превышении скорости)	-----☐----- GEN2 v2 Пикто xxx км/ч
3	<i>Идентификационные данные держателя карточки</i> Идентификатор блока данных Р= пиктограмма «люди» Фамилия держателя карточки Имя (имена) держателя карточки (если есть) Идентификационные данные карточки Дата истечения срока действия карточки (если есть) и номер поколения карточки (GEN-1 или GEN-2)* и версия**	-----Р----- Р Фамилия _____ Имя _____ Идентификационные данные карточки _____ дд/мм/гггг --- GEN2 v2

На карточки, не принадлежащие конкретным лицам, вместо фамилии держателя наносится название предприятия, мастерской или контрольного органа.

* Номер поколения карточки может печатать только смарт-тахограф.

- 4 **Идентификационные данные транспортного средства**
Идентификатор блока данных
VIN
Государство-член Договаривающаяся сторона
регистрации и VRN
- Д -----
Д VIN _____
 Гос/VRN _____
- 4a **Тип груза транспортного средства по умолчанию****
pi = пиктограмма типа груза транспортного средства по умолчанию**
- pi**
- 5 **Идентификационные данные БУ**
Идентификатор блока данных
Название изготовителя БУ
Номер детали БУ
Номер поколения БУ*
- В -----
В Изготовитель_БУ _____
 Номер_детали_БУ__ _____
 GEN-2
- ~~* Номер поколения карточки может печатать только смарт тахограф.~~
- 6 **Последняя калибровка тахографа**
Идентификатор блока данных
Карточка мастерской
Идентификационные данные карточки мастерской
Дата калибровки
- Т -----
Т Фамилия _____
 Идентификационные
 данные_карточки _____
Т дд/мм/гггг
- 7 **Последний контроль (проверка контролером)**
Идентификатор блока данных
Идентификационные данные карточки контролера
Дата, время и вид контроля
- П -----
 Идентификационные
 данные_карточки _____
П дд/мм/ггг чч:мм ррррр
- Вид контроля: до пяти пиктограмм. Возможные виды контроля (в следующем сочетании):
■: Загрузка данных с карточки; **⚡**: загрузка данных с БУ; **⏏**: распечатка; **□**: вывод на дисплей; **Т**: проверки калибровки на дорогах.
- 8 **Данные о деятельности водителя, сохраняемые на карточке в хронологической последовательности**
Идентификатор блока данных
Проверяемая дата (календарный день, данные за который подлежат распечатке) + календарный счетчик вводов карточки
- В -----
 дд/мм/гггг xxx
- 8a **Позиция «неприменимо» в начале текущего дня**
(оставить незаполненной, если позиция «неприменимо» не открыта)
- OUT -----
- 8b **Тип груза в начале текущего дня** (если карточка вставлена в БУ, в противном случае оставить незаполненной), pi** = пиктограмма типа груза**
- pi -----
- 8.1 **Период, в течение которого карточка не была вставлена**
- 8.1a Идентификатор записи (начало периода)
- ? чч:мм чччмм
- 8.1b Период, за который нет данных. Время начала, продолжительность
- А чч:мм чччмм
- 8.1c **Данные о деятельности, введенные вручную.**
Пиктограмма вида деятельности, время начала, продолжительность

- 8.2 *Ввод карточки в считывающее устройство S*
Идентификатор записи; S = пиктограмма считывающего устройства
~~Государство — член Договаривающаяся сторона~~ регистрации и VRN
Показание счетчика пробега транспортного средства на момент ввода карточки
pi = тип груза транспортного средства на момент ввода карточки**
- 8.3 *Деятельность (за время, пока карточка была вставлена)*
Пиктограмма вида деятельности, время начала, продолжительность, статус экипажа (пиктограмма экипажа, если CREW; оставить незаполненной, если SINGLE)
- 8.3a *Особая ситуация*
Время ввода данных, пиктограмма (или комбинация пиктограмм) особой ситуации
- 8.4 *Извлечение карточки*
Показания счетчика пробега и расстояние, пройденное с момента последнего ввода карточки, в случае которого были зафиксированы показания счетчика пробега
- 9 *Данные о деятельности водителей, сохраненные в БУ отдельно для каждого считывающего устройства в хронологическом порядке*
Идентификатор блока данных
Проверяемая дата (календарные сутки, данные за которые подлежат распечатке)
Показания счетчика пробега на 00:00 часов и на 24:00 часов
- 10 *Данные о деятельности, записанные со считывающего устройства S*
- 10a *Позиция «неприменимо» в начале текущего дня*
(оставить незаполненной, если позиция «неприменимо» не открыта)
- 10.1 *Период, когда карточка не вставлена в считывающее устройство S*
Идентификатор записи
Карточка не введена
Показания счетчика пробега на начало периода
- 10.2 *Ввод карточки*
Идентификатор записи о вводе карточки
Фамилия водителя
Имя водителя
Идентификационные данные карточки водителя
Дата истечения срока действия карточки (если есть) и номер поколения карточки (GEN-1 или GEN-2)*
и версия**
~~Государство — член Договаривающаяся сторона~~ регистрации предыдущего транспортного средства, которое использовалось ранее, и VRN
Дата и время извлечения карточки из предыдущего транспортного средства
Пустая строка
Показания счетчика пробега на момент ввода карточки, метка ручного ввода данных о деятельности водителя (M — «да», пробел — «нет»).
Если в день, за который производится распечатка, карточка водителя не вводилась, то для блока 10.2 используются показания счетчика пробега, снятые на момент последнего записанного ввода карточки до указанного дня.

```

-----S-----
A Гос/VRN _____
x xxx xxx км
pi

```

```

A чч:мм ччмм ☐☐

```

```

чч:мм ---pppp---

```

```

x xxx xxx км; x xxx км

```

```

-----☐-----
дд/мм/гггг
x xxx xxx --- x xxx xxx км

```

```

-----S-----
-----OUT-----

```

```

-----
☐☐---
x xxx xxx км

```

```

-----
☐ Фамилия _____
Имя _____
Идентификационные данные
карточки _____
дд/мм/гггг --- GEN2 v2
A +Гос/VRN _____
дд/мм/гггг чч:мм
x xxx xxx км M

```

10.3	<i>Вид деятельности</i> Пиктограмма вида деятельности, время начала, продолжительность, статус экипажа (пиктограмма экипажа, если CREW; оставить незаполненной, если SINGLE)	A чч:мм ччмм ☐☐
10.3a	<i>Особые условия</i> Время ввода данных, пиктограмма (или комбинация пиктограмм) особых условий	чч:мм ---pppp---
10.4	<i>Извлечение карточки или окончание периода отсутствия карточки</i> Показания счетчика пробега на момент извлечения карточки или окончания периода отсутствия карточки в устройстве и расстояние, пройденное с момента ввода карточки или с начала периода отсутствия карточки в устройстве.	x xxx xxx км; x xxx км
* Номер поколения карточки может печатать только смарт-тахограф.		
11	<i>Суточная сводка</i> Идентификатор блока данных	-----Σ-----
11.1	<i>Сводка данных БУ за периоды отсутствия карточки в считывающем устройстве карточки водителя</i> Идентификатор блока данных	1 ☐ ---
11.2	<i>Сводка данных БУ за периоды отсутствия карточки в считывающем устройстве карточки второго водителя</i> Идентификатор блока данных	2 ☐ ---
11.3	<i>Суточная сводка данных БУ по каждому водителю</i> Идентификатор записи Фамилия водителя Имя (имена) водителя Идентификационные данные карточки водителя	----- ☐ Фамилия _____ Имя _____ Идент. _данные_ карточки _____
11.4	<i>Введенные данные о месте начала и/или окончания дневного периода работы</i> p1 = пиктограмма места начала / окончания, время, страна, район долгота широта зарегистрированного местоположения*, статус аутентификации** широта долгота зарегистрированного местоположения*, статус аутентификации** метка времени, когда было определено данное местоположение*, статус аутентификации** Счетчик пробега	p1чч:мм Стр Рег шир дот ±DDD°MM.M' ☐ дол дот ± DDD°MM.M' ☐ чч+мм дд/мм/гггг чч:мм ☐ x xxx xxx км
11.5	<i>Заезд в место, где начинается и/или заканчивается дневной рабочий период</i> <i>Местоположение после 3 часов накопленного времени управления*</i> p1 = местоположение после 3 часов непрерывного накопленного времени управления*, время записи * долгота широта зарегистрированного местоположения*, статус аутентификации** широта долгота зарегистрированного местоположения*, статус аутентификации** метка времени, когда было определено данное местоположение*, статус аутентификации** Счетчик пробега*	p1чч:мм шир дот ±DDD°MM.M' ☐ дол дот ± DDD°MM.M' ☐ дд/мм/гггг чч:мм ☐ x xxx xxx км

11.5a *Пересечение границы* **

ri = место, где транспортное средство пересекло границу страны **

Страна, из которой/в которую выехало/въехало транспортное средство**

Широта зарегистрированного местоположения*, статус аутентификации**

Долгота зарегистрированного местоположения*, статус аутентификации**

Метка времени, когда было определено данное местоположение*, статус аутентификации**

Счетчик пробега**

ri
Стр + Стр
шир ± ДД°ММ.М'

дол ±ДДД°ММ.М'
ДД/ММ/ГГГГ ЧЧ:ММ

x xxx xxx km

11.5b *Операция по загрузке/разгрузке***

ri = место, где была произведена операция загрузки/разгрузки, время записи**

Широта зарегистрированного местоположения*, статус аутентификации**

Долгота зарегистрированного местоположения*, статус аутентификации**

Метка времени, когда было определено местоположение**

Счетчик пробега**

riчч:мм
шир ± ДД°ММ.М'

дол ±ДДД°ММ.М'
ДД/ММ/ГГГГ ЧЧ:ММ

x xxx xxx км

11.6 *Суммарные данные о деятельности (из карточки)*

Общее время управления, пройденное расстояние

Общее время работы и готовности

Общее время отдыха и отсутствия данных

Суммарное время деятельности экипажа

чччмм x xxx км
* чччмм чччмм
h чччмм ? чччмм
 чччмм

11.7 *Суммарные данные о деятельности (периоды отсутствия карточки в считывающем устройстве для карточки водителя)*

Общее время управления, пройденное расстояние

Общее время работы и готовности

Общее время отдыха

чччмм x xxx км
* чччмм чччмм
h чччмм

11.8 *Суммарные данные о деятельности (периоды отсутствия карточки в считывающем устройстве для карточки второго водителя)*

Durée totale des périodes de travail et de disponibilité

Durée totale de la période de repos

* чччмм чччмм
h чччмм

11.9 *Totaux par activité (et par conducteur, les deux lecteurs étant inclus dans le calcul)*

Общее время управления, пройденное расстояние

Общее время работы и готовности

Общее время отдыха

Суммарное время деятельности экипажа

чччмм x xxx км
* чччмм чччмм
h чччмм
 чччмм

При вводе команды на распечатку суточной сводки за текущий день имеющиеся данные за сутки суммируются по состоянию на момент распечатки.

12 *События и/или неисправности, зарегистрированные на карточке*

12.1 Идентификатор блока данных: последние 5 «событий и неисправностей», зарегистрированных на карточке

----- ! * -----

12.2 Идентификатор блока данных: все «события», зарегистрированные на карточке

----- ! -----

12.3 Идентификатор блока данных: все «неисправности», зарегистрированные на карточке

----- * -----

12.4 *Запись о событии и/или неисправности*

Идентификатор записи
 Пиктограмма события/неисправности, назначение записи, дата и время начала
 Дополнительный код события/неисправности (если имеется), продолжительность
~~Государство-член~~ Договаривающаяся сторона регистрации транспортного средства, в котором имело место событие или неисправность, и VRN транспортного средства

```

-----
Пик (р) дд/мм/гггг чч:мм
!xx ччмм
A Гос/VRN_____

```

13 *Прошлые или текущие события и/или неисправности, зарегистрированные или регистрируемые БУ*

13.1 Идентификатор блока данных: последние 5 «событий и неисправностей», по данным БУ

```

----- !xA-----

```

13.2 Идентификатор блока данных: все «события», зарегистрированные или регистрируемые БУ

```

----- !A-----

```

13.3 Идентификатор блока данных: все прошлые или текущие «неисправности», зарегистрированные или регистрируемые БУ

```

----- xA-----

```

13.4 *Запись о событии и/или неисправности*

Идентификатор записи
 Пиктограмма события/неисправности, назначение записи, дата и время начала
 Код дополнительного события/неисправности (если есть), количество аналогичных событий за этот день, продолжительность
 Идентификационные данные карточек, находившихся в устройстве на момент начала или окончания события или неисправности (до 4 строк без повторения одних и тех же номеров карточек)

```

-----
Пик (р) дд/мм/гггг чч:мм
!xx (xxx) ччмм
Идент. _данные_карточки
_____
Идент. _данные_карточки
_____
Идент. _данные_карточки
_____
Идент. _данные_карточки
_____
Идент. _данные_карточки
_____

```

Отсутствие карточки в устройстве
 Конкретные данные по изготовителю

Цель записи (р) указывается числовым кодом, обозначающим цель регистрации события или неисправности и определяемым в порядке, предусмотренном для элемента данных EventFaultRecordPurpose.

Literal — константа, связанная с конкретным изготовителем тахографа, которая состоит не более чем из 12 символов.

ErrorCode — код ошибки конкретного изготовителя тахографа, состоящий максимум из 12 символов.

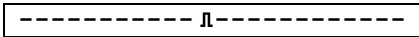
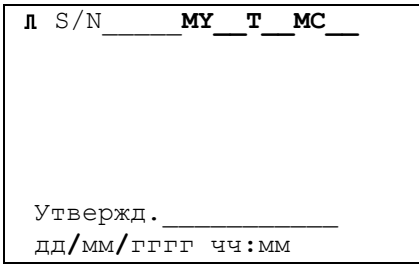
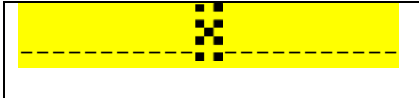
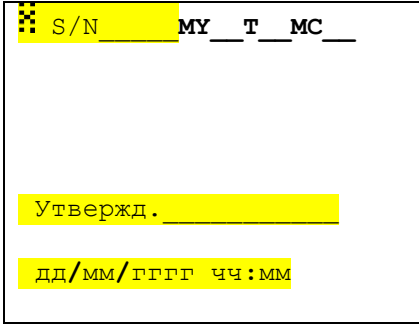
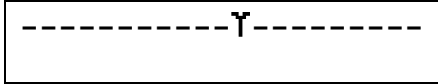
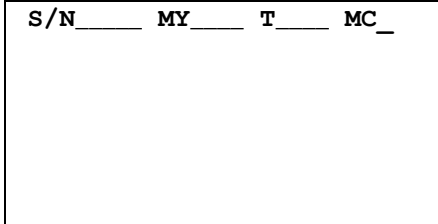
14 *Идентификационные данные БУ*

Идентификатор блока данных
 Название изготовителя БУ
 Адрес изготовителя БУ
 Номер детали БУ
 Номер официального утверждения БУ
 Серийный номер БУ
 Год выпуска БУ
Поколение и версия БУ **
 Версия программного обеспечения БУ и дата установки
Версия сохраненной цифровой карты**

```

----- B-----
B Фамилия_____
Адрес_____
Номер_детали_____
Утвержд. _____
S/N_____
Fгггг
GEN2 v2
V xxxx дд/мм/гггг
Bxxxxxxxxxxxxx

```

- 15 **Идентификация датчика**
Идентификатор блока данных 
- 15.1 **Запись сопряжения**
Серийный номер датчика (S/N = серийный номер в десятичной системе, MY = месяц и год в десятичной системе, T = type в десятичной системе, MC = Код изготовителя в шестнадцатеричной системе, см. подраздел 1 добавления, Расширенный номер серии)
Номер официального утверждения датчика
Дата первого подсоединения 
- 16 **Идентификация ГНСС***
Идентификатор блока данных* 
- 16.1 **Запись о подсоединении***
Серийный номер внешнего устройства ГНСС* (S/N = серийный номер в десятичной системе, MY = месяц и год в десятичной системе, T = type в десятичной системе, MC = Код изготовителя в шестнадцатеричной системе, см. приложение 1, Расширенный номер серии)
Номер официального утверждения внешнего устройства ГНСС*
Дата соединения с внешним устройством ГНСС* 
- ~~Цель калибровки (р) указывается числовым кодом, обозначающим причины регистрации параметров калибровки, закодированных в соответствии с элементом данных CalibrationPurpose.~~
- 16a **Идентификация устройства удаленной связи****
Идентификатор блока данных** 
- 16a.1 **Серийный номер устройства удаленной связи****
Серийный номер внешнего устройства удаленной связи** (S/N = серийный номер в десятичной системе, MY = месяц и год в десятичной системе, T = type в десятичной системе, MC = Код изготовителя в шестнадцатеричной системе, см. подраздел 1 добавления, расширенный серийный номер) 

17	Данные калибровки	Идентификатор блока данных	----- T -----
17.1	Данные калибровки	Идентификатор записи Мастерская, выполнившая калибровку Адрес мастерской Идентификационные данные карточки мастерской Срок действия карточки мастерской Пустая строка Дата и время калибровки (oldTimeValue в записи калибровки) + цель калибровки в шестнадцатеричном формате VIN Государство-член Договаривающаяся сторона регистрации и VRN «Характеристический коэффициент транспортного средства»: Постоянная величина занимающего оборудование контрольного устройства Эффективная окружность шин колес Размер установленных шин Регулировка устройства ограничения скорости Показания счетчика пробега до и после регулировки pi = пиктограмма типа груза транспортного средства по умолчанию** Страна, в которой была проведена калибровка, и дата и время Данные о пломбах (до 5 записей о пломбах, 1 строка для каждой использованной пломбы), ET = тип оборудования в десятичной системе**, MC = код изготовителя в виде двух знаков**, SI = идентификатор пломбы в виде 8 знаков**, см. добавление 1, SealRecord	----- T Название_мастерской____ Адрес_мастерской_____ Идент._данные_карточки____ дд/мм/гггг T дд/мм/гггг чч:мм (p) d VIN_____ Гос/VRN_____ w xx xxx Имп/км k xx xxx Имп/км l xx xxx мм • TyreSize_____ > xxx км/ч x xxx xxx — x xxx xxx км pi Стр дд/мм/гггг чч:мм SET_ MC SI_____
Цель калибровки (p) указывается числовым кодом, обозначающим цель регистрации события или неисправности и определяемым в порядке, предусмотренном для элемента данных CalibrationPurpose.			
18	Корректировка времени	Идентификатор блока данных	----- @ -----
18.1	Запись корректировки времени	Идентификатор записи Прежняя дата и время Новая дата и время Мастерская, выполнившая корректировку времени Адрес мастерской Идентификация карточки мастерской Дата истечения срока действия карточки мастерской	----- ! @ дд/мм/гггг чч:мм @ дд/мм/гггг чч:мм T Название_мастерской____ Адрес_мастерской_____ Идент._данные_карточки____ дд/мм/гггг
19	Самое последнее событие и Неисправность, зарегистрированные в БУ	Идентификатор блока данных Время и дата самого последнего события Время и дата самой последней неисправности	----- ! x d ----- ! дд/мм/гггг чч:мм x дд/мм/гггг чч:мм
20	Информация о контроле за превышением скорости	Идентификатор блока данных Дата и время последнего КОНТРОЛЯ ЗА ПРЕВЫШЕНИЕМ СКОРОСТИ Дата и время первого превышения скорости и количество последующих превышений скорости	----- > > ----- > @ дд/мм/ггггчч:мм >> дд/мм/гггг чч:мм (nnn)

21	Распечатка данных о превышении скорости	
21.1	Идентификатор блока «Первое превышение скорости после последней калибровки»	----->>T-----
21.2	Идентификатор блока «5 самых серьезных превышений за последние 365 дней»	----->>(365)-----
21.3	Идентификатор блока данных: «наиболее серьезное превышение за каждые из последних 10 дней, когда превышения имели место»	----->>(10)-----
21.4	Идентификатор записи Дата, время и продолжительность Максимальная и средняя скорость, количество аналогичных событий за данный день Фамилия водителя Имя (имена) водителя Идентификационные данные карточки водителя	<p style="text-align: center;">-----</p> <p>>>дд/мм/гггг чч:мм ччмм xxx км/ч xxx км/ч (xxx)</p> <p>☐ Фамилия _____ Имя _____ Идент. данные карточки _____</p>
21.5	Если в блоке данных записи о превышениях скорости отсутствуют	>>---
22	Информация, вписываемая от руки	
	Идентификатор блока данных	<p>-----</p> <p>☐ * ☐ ☐ + + ☐ ☐</p>
22.1	Место контроля	
22.2	Подпись контролера	
22.3	Время: с	
22.4	Время: до	
22.5	Подпись водителя	
	«Информация, вписываемая от руки»; над названием графы, заполняемой от руки, следует оставить достаточное количество пустых строк для вписывания необходимой информации или для собственноручной подписи.	
23	Самые последние карточки, введенные в БУ*	
	Идентификатор блока данных*	<p>----- ☐ ☐ ☐ -----</p> <p>----</p> <p>T <гэн> <версия> <МС> Идентификационные данные карточки Серийный номер карточки дд/мм/гггг чч:мм</p>
23.1	Введенная карточка* Идентификатор записи* Тип карточки, поколение, версия, изготовитель* ¹ Идентификация карточки* Серийный номер карточки* Дата и время ввода последней карточки*	

¹ (все в одной строке)
с указанием
типа карточки: пиктограмма, один символ + пробел
поколения: GEN1 или GEN2, 4 символа + пробел
версии: до 10 символов
МС: код изготовителя, 3 символа

3. Спецификации распечатки данных

В тексте данной главы применяются следующие условные обозначения:

N	Распечатка блока или записи данных под номером N
N	Распечатка блока или записи данных под номером N нужное количество раз
X/Y	Распечатка по мере необходимости блоков или записей данных под номером X и/или Y и ее повторение нужное количество раз

3.1 Распечатка сохраненных на карточке данных о деятельности водителя за сутки

PRT_008 При распечатке сохраненных на карточке данных о деятельности водителя за сутки соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные контролера (если в БУ введена карточка контролера)
3	Идентификационные данные водителя (согласно карточке, с которой распечатываются данные + GEN)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
5	Идентификационные данные БУ (БУ, с которого получены распечатываемые данные, + GEN)
6	Последняя калибровка данного БУ
7	Последний контроль деятельности проверяемого водителя
8	Ограничитель данных о деятельности водителя
8a	Условие «неприменимо» в начале этих суток
8b	Тип груза в начале суток (если карточка вставлена в БУ)
8.1a/8.1b/8.1c/8.2/8.3/ 8.3a/8.4	Деятельность водителя в хронологическом порядке
11	Ограничитель данных суточной сводки
11.4	Въезд водителя в географические пункты в хронологическом порядке
11.5	Данные ГНСС Местоположения по истечении 3 часов накопленного времени управления, в хронологическом порядке
11.5a	Пересечение границы, в хронологическом порядке
11.5b	Операции по загрузке/разгрузке, в хронологическом порядке
11.6	Суммарные данные о деятельности
12.1	Ограничитель сохраненных на карточке данных о событиях и неисправностях
12.4	Записи о событиях/неисправностях (последние 5 событий или неисправностей, зарегистрированные на карточке)
13.1	Ограничитель данных БУ о событиях и неисправностях
13.4	Записи о событиях/неисправностях (последние 5 событий или неисправностей, зарегистрированных или регистрируемых БУ)
22.1	Место контроля
22.2	Подпись контролера
22.5	Подпись водителя

3.2 Распечатка сохраненных в БУ данных о деятельности водителя за сутки

PRT_009 При распечатке сохраненных в БУ данных о деятельности водителя за сутки соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные держателя карточки (для всех карточек, введенных в БУ + GEN)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
4a	Тип груза транспортного средства по умолчанию
5	Идентификационные данные БУ (БУ, с которого получены распечатываемые данные, + GEN)
6	Последняя калибровка данного БУ
7	Последний контроль на данном тахографе
9	Ограничитель данных о деятельности водителя
10	Ограничитель данных со считывающего устройства водителя (считывающее устройство 1)
10a	Условие «неприменимо» в начале этих суток
10.1/10.2/10.3/10.3a/ 10.4	Деятельность в хронологическом порядке (считывающее устройство водителя)
10	Ограничитель данных о деятельности (считывающее устройство второго водителя)
10a	Условие «неприменимо» в начале этих суток
10.1/10.2/10.3/10.3a/ 10.4	Деятельность в хронологическом порядке (считывающее устройство второго водителя)
11	Ограничитель данных суточной сводки
11.1	Сводка данных за периоды отсутствия карточки в считывающем устройстве водителя
11.4	Въезд в географические пункты в хронологическом порядке
11.5	Данные ГНСС Местоположения по истечении 3 часов накопленного времени управления в хронологическом порядке
11.5a	Пересечения границы, в хронологическом порядке
11.5b	Операции по загрузке/разгрузке, в хронологическом порядке
11.67	Суммарные данные о деятельности
11.2	Сводка данных за периоды отсутствия карточки в считывающем устройстве второго водителя
11.4	Въезд в географические пункты в хронологическом порядке
11.5	Данные ГНСС Местоположения по истечении 3 часов накопленного времени управления в хронологическом порядке
11.5a	Пересечение границы, в хронологическом порядке
11.5b	Местоположения, в которых производились операции по загрузке, в хронологическом порядке
11.8	Суммарные данные о деятельности

11.3	Суммарные данные о деятельности водителя по результатам обоих считывающих устройств
11.4	Въезд в географические пункты в хронологическом порядке
11.5	Данные ГИСС Местоположения по истечении 3 часов накопленного времени управления в хронологическом порядке
11.5a	Пересечение границы, в хронологическом порядке
11.5b	Операции по загрузке/разгрузке, в хронологическом порядке
11.9	Суммарные данные о деятельности данного водителя
13.1	Ограничитель данных о неисправностях
13.4	Записи о событиях/неисправностях (последние 5 событий или неисправностей, зарегистрированных или регистрируемых БУ)
22.1	Место контроля
22.2	Подпись контролера
22.3	Время: с (место для указания водителем, не имеющим карточки)
22.4	Время: до тех периодов, которые к нему относятся
22.5	Подпись водителя

3.3 События и неисправности из распечатки данных карточки

PRT_010 При распечатке сохраненных на карточке данных о событиях и неисправностях соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные контролера (если в БУ + GEN введена карточка контролера)
3	Идентификационные данные водителя (согласно карточке, с которой распечатываются данные)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
12.2	Ограничитель данных о событиях
12.4	Записи о событиях (все события, зарегистрированные на карточке)
12.3	Ограничитель данных о неисправностях
12.4	Записи о неисправностях (все неисправности, зарегистрированные на карточке)
22.1	Место контроля
22.2	Подпись контролера
22.5	Подпись водителя

3.4 События и неисправности из распечатки БУ

PRT_011 При распечатке сохраненных в БУ данных о событиях и неисправностях соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные держателя карточки (для всех карточек, введенных в БУ + GEN)

4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
13.2	Ограничитель данных о событиях
13.4	Записи о событиях (все события, зарегистрированные или регистрируемые БУ)
13.3	Ограничитель данных о неисправностях
13.4	Записи о неисправностях (все неисправности, зарегистрированные или регистрируемые БУ)
22.1	Место контроля
22.2	Подпись контролера
22.5	Подпись водителя

3.5 Распечатка технических данных

PRT_012 При распечатке технических данных соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные держателя карточки (для всех карточек, введенных в БУ + GEN)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
14	Идентификационные данные БУ
15	Идентификационные данные датчика
15.1	Данные о сопряжении датчиков (все данные доступны в хронологическом порядке)
16	Идентификационные данные ГНСС
16.1	Дата и время распечатки документа (все данные указаны в хронологическом порядке)
16a	Идентификационные данные устройства удаленной связи
16a.1	Серийный номер устройства удаленной связи
17	Ограничитель данных калибровки
17.1	Записи о калибровке (все имеющиеся записи в хронологическом порядке)
18	Ограничитель данных о корректировке времени
18.1	Записи о корректировке времени (все имеющиеся записи о корректировке времени, в том числе относящиеся к калибровке)
19	Самое последнее событие и неисправность, зарегистрированные в БУ
2	Тип распечатки (указывает на конец распечатки)

3.6 Распечатка данных о превышении скорости

PRT_013 При распечатке данных о превышении скорости соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные держателя карточки (для всех карточек, введенных в БУ + GEN)

4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
20	Информация о контроле за превышением скорости
21.1	Идентификатор данных о превышении скорости
21.4/21.5	Первое превышение скорости после последней калибровки
21.2	Идентификатор данных о превышении скорости
21.4/21.5	5 наиболее серьезных превышений скорости за последние 365 дней
21.3	Идентификатор данных о превышении скорости
21.4/21.5	Наиболее серьезное превышение скорости за каждые из последних 10 дней, когда превышения имели место
22.1	Место контроля
22.2	Подпись контролера
22.5	Подпись водителя

3.7 Архив вставленных карточек

PRT_014 При распечатке архива вставленных карточек соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные держателя карточки (для всех карточек, введенных в БУ)
23	Самые последние карточки, введенные в БУ
23.1	Вставленные карточки (до 88 записей)
12.3	Тип распечатки (указывает на конец распечатки) Разделитель ошибок

Подраздел 5

Дисплей

В тексте данного подраздела применяются следующие условные обозначения:

- **жирным шрифтом** обозначена информация, отображаемая в текстовой форме (при отображении используется обычный шрифт);
- обычным шрифтом указаны переменные параметры (пиктограммы или данные), вместо которых отображаются соответствующие значения:
- дд мм гггг: день, месяц, год;
- чч: часы;
- мм: минуты;
- П: пиктограмма продолжительности;
- EF: комбинация пиктограмм события или неисправности;
- О: пиктограмма режима работы.

DIS_001 При отображении данных тахографа используются следующие форматы:

Данные	Формат
Индикация данных по умолчанию	
Местное время	чч:мм
Режим работы	О
Информация, касающаяся водителя	1 Пчччмм чччмм
Информация, касающаяся второго водителя	2 Пчччмм
Открыто условие «неприменимо»	OUT
Предупреждающие индикаторы	
Превышение времени непрерывного управления	1 ⓪ чччмм чччмм
Событие или неисправность	EF
Прочие индикаторы	
Дата в формате UTC Время	UTC ⓪ дд/мм/гггг или UTC ⓪ дд.мм.гггг чч:мм
Непрерывное время управления и суммарная накопленная продолжительность перерывов у водителя	1 ⓪ чччмм чччмм
Непрерывное время управления и суммарная накопленная продолжительность перерывов у второго водителя	2 ⓪ чччмм чччмм
Суммарная Накопленная продолжительность времени управления за прошлую и текущую неделю у водителя	1 ⓪ чччмм
Суммарная Накопленная продолжительность времени управления за прошлую и текущую неделю у второго водителя	2 ⓪ чччмм

Подраздел 6

Передний соединитель для калибровки и загрузки

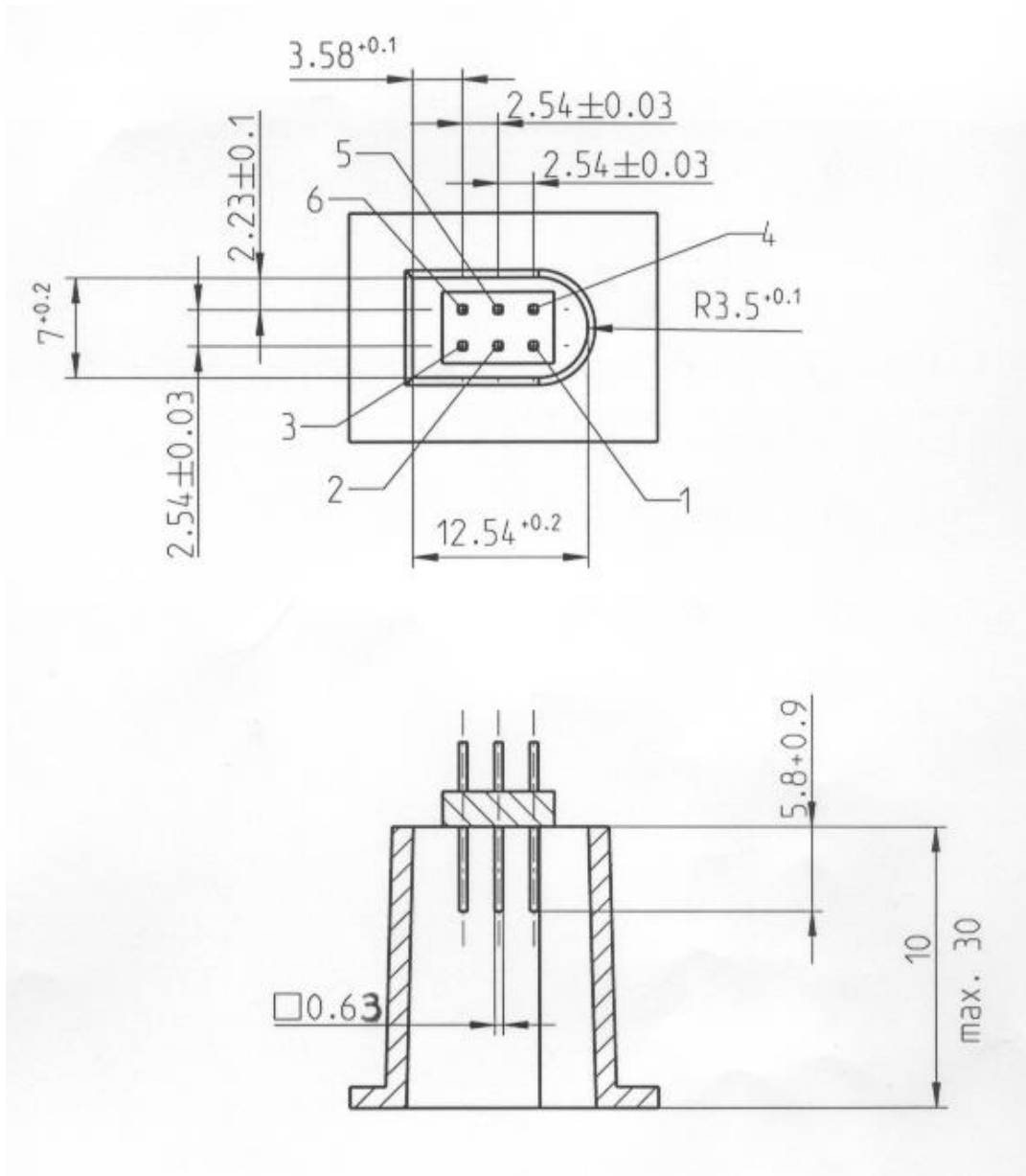
Содержание

	<i>Стр.</i>
1. Аппаратное обеспечение	346
1.1 Соединитель	346
1.2 Расположение контактов	348
1.3 Блок-схема	348
2. Интерфейс загрузки данных	348
3. Интерфейс калибровки	349

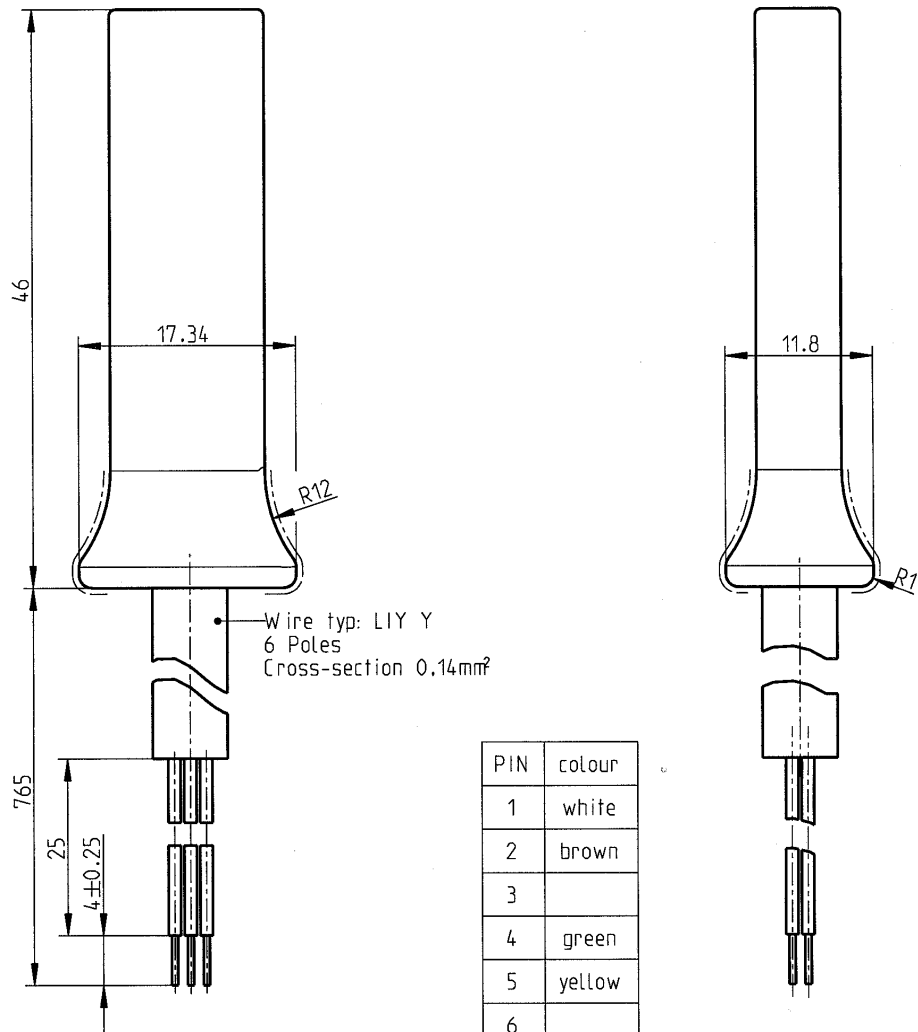
1. Аппаратное обеспечение

1.1 Соединитель

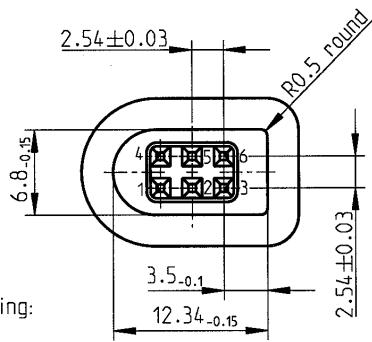
INT_001 Соединитель для загрузки данных/калибровки располагается на передней панели, доступен без снятия каких-либо деталей тахографа и представляет собой 6-контактный разъем, выполненный в соответствии с нижеследующим чертежом (все размеры указаны в миллиметрах):



Типовая схема вилки 6-контактного штепсельного разъема:



PIN	colour
1	white
2	brown
3	
4	green
5	yellow
6	



Contact:
47 745-001
Socket housing:
650 43-034

--- Surface pattern
VDI 3400 Ref. 36 Ra 6.3 μm

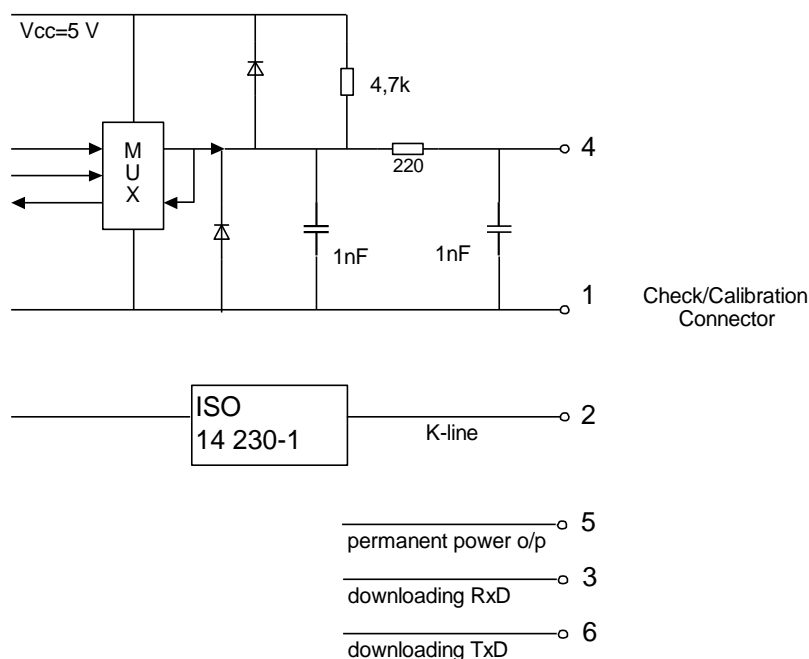
1.2 Расположение контактов

INT_002 Расположение контактов указана в таблице ниже:

Контакт	Описание	Примечание
1	Описание	Соединяется с отрицательным полюсом бортовой аккумуляторной батареи
2	Аккумуляторная батарея — отрицательный полюс	К-линия (ISO 14230-1)
3	Передача данных	Ввод данных в тахограф
4	RxD — Загрузка	Калибровка
5	Входной/выходной сигнал	Номинальный диапазон напряжений равен напряжению бортовой сети питания минус 3 В с учетом падения напряжения на предохранительных цепях Выход 40 мА
6	Постоянная выходная мощность	Вывод данных с тахографа

1.3 Блок-схема

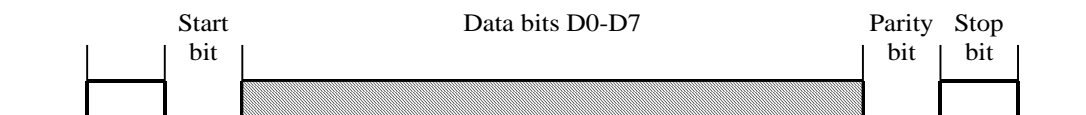
INT_003 Блок-схема соответствует приведенной ниже:



2. Интерфейс загрузки данных

INT_004 Интерфейс загрузки данных соответствует спецификациям RS232.

INT_005 Порядок загрузки данных через интерфейс: один стартовый бит, 8 битов данных начиная с LSB, один бит контроля по четности, один стоп-бит.



Структура байта данных

Стартовый бит: один бит с уровнем логического нуля;

Биты данных: бит младшего разряда (LSB) передается первым;

Бит контроля по четности: положительная четность;

Стоп-бит: один бит с уровнем логической единицы;

При передаче числовых данных объемом больше одного байта байт старшего разряда передается первым, байт младшего разряда — последним.

INT_006 Скорость передачи данных в бодах регулируется в диапазоне от 9600 бит/с до 115 200 бит/с. При инициализации обмена данными задается начальная скорость передачи в бодах 9600 бит/с; затем скорость доводится до максимальной возможной величины.

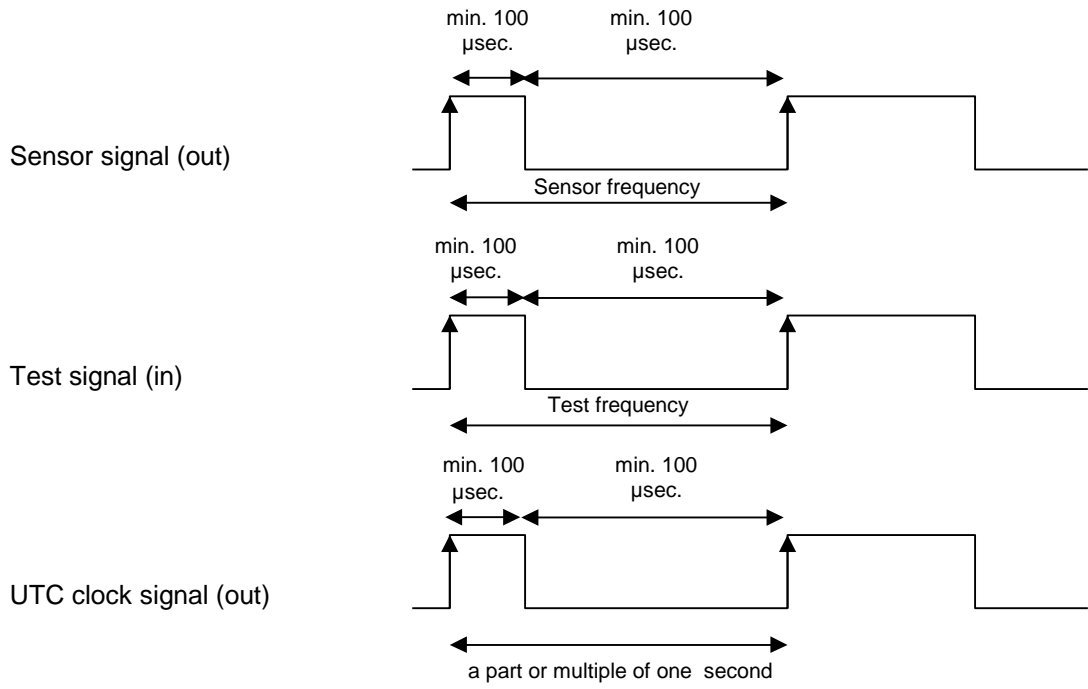
3. Интерфейс калибровки

INT_007 Обмен данных осуществляется в соответствии со стандартом ISO 14230-1 (Транспорт дорожный. Системы диагностического контроля. Протокол ключевых слов 2000 — Часть 1. Физический уровень, издание первое, 1999 год).

INT_008 Электрические характеристики сигнала ввода/вывода соответствуют указанным ниже:

Параметр	Минимум	Типичный	Максимум	Примечание
U _{ниж.} (ВХОД)			1,0 В	I = 750 мкА
U _{верх.} (ВХОД)	4 В			I = 200 мкА
Частота			4 кГц	
U _{ниж.} (ВЫХОД)			1,0 В	I = 1 мА
U _{верх.} (ВЫХОД)	4 В			I = 1 мА

INT_009 Сигнал ввода/вывода соответствует представленным ниже временным диаграммам:



Подраздел 7

Протоколы загрузки данных

Содержание

	<i>Стр.</i>
1. Введение	353
1.1 Сфера применения	353
1.2 Сокращения и обозначения	353
2. Загрузка данных из БУ	354
2.1 Процедура загрузки	354
2.2 Протокол загрузки данных	355
2.2.1 Структура сообщений	355
2.2.2 Типы сообщений	356
2.2.2.1 Запрос инициализации обмена данными (SID 81)	359
2.2.2.2 Положительный ответ: начало обмена данными (SID C1)	359
2.2.2.3 Запрос инициализации диагностического сеанса (SID 10)	359
2.2.2.4 Положительный ответ: инициализация диагностики (SID 50)	360
2.2.2.5 Функция регулировки канала обмена данными (SID 87)	360
2.2.2.6 Регулировка канала обмена данными: положительный ответ (SID C7)	360
2.2.2.7 Запрос загрузки (SID 35)	360
2.2.2.8 Положительный ответ на запрос загрузки (SID 75)	360
2.2.2.9 Запрос передачи данных (SID 36)	360
2.2.2.10 Положительный ответ: передача данных (SID 76)	361
2.2.2.11 Запрос завершения передачи (SID 37)	361
2.2.2.12 Положительный ответ: запрос завершения передачи (SID 77)	361
2.2.2.13 Запрос на прекращение связи (SID 82)	361
2.2.2.14 Положительный ответ на запрос по поводу завершения обмена данными (SID C2)	362
2.2.2.15 Подтверждение приема подсообщения (SID 83)	362
2.2.2.16 Отрицательный ответ (SID 7F)	362
2.2.3 Поток сообщений	363
2.2.4 Временные параметры	363
2.2.5 Обработка ошибок	364
2.2.5.1 Стадия инициализации обмена данными	364
2.2.5.2 Стадия обмена данными	365
2.2.6 Содержание ответного сообщения	368
2.2.6.1 Положительный ответ: передача данных — версия интерфейса загрузки	369
2.2.6.2 Положительный ответ: контроль за передачей данных	369

2.2.6.32	Положительный ответ: работа по передаче данных	371
2.2.6.43	Положительный ответ на запрос передачи данных о событиях и неисправностях	373
2.2.6.54	Положительный ответ на запрос передачи подробных данных о скоростном режиме	374
2.2.6.65	Положительный ответ на запрос передачи технических данных	375
2.	Хранение файлов на ВН	376
3.	Протокол загрузки данных с карточек тахографа	376
3.1	Сфера применения	376
3.2	Определения	376
3.3	Загрузка с карточки	376
3.3.1	Процедура инициализации	378
3.3.2	Процедура для неподписанных файлов данных	378
3.3.3	Процедура для подписанных файлов данных	379
3.3.4	Процедура обнуления счетчика калибровок	380
3.4	Формат хранения данных	380
3.4.1	Введение	380
3.4.2	Формат файла	380
4.	Загрузка данных с карточки тахографа с помощью бортового устройства	381

1. Введение

В настоящем подразделе изложены процедуры различных вариантов загрузки данных на внешний носитель (ВН), а также протоколы, применение которых необходимо для правильной передачи данных и для обеспечения универсальной совместимости формата, в котором они загружаются, с тем чтобы любой контролер имел возможность ознакомиться с этими данными и перед началом их анализа убедиться в их подлинности и целостности.

1.1. Сфера применения

На ВН могут загружаться данные:

- из бортового устройства при помощи подключенной к БУ специализированной программируемой аппаратуры (СПА);
- с карточки тахографа при помощи СПА, оснащенной устройством считывания карточек (IFD);
- с карточки тахографа через бортовое устройство путем подключения СПА к БУ.

Для целей контроля подлинности и целостности данных, сохраняемых на ВН, при загрузке они снабжаются подписью в соответствии с ~~приложением~~ **подразделом 11 «Общие механизмы защиты»**. В состав загружаемой информации включаются идентификационные данные аппаратного источника (БУ или карточки) и соответствующие ему сертификаты безопасности (~~государств-членов Договаривающихся сторон~~ и аппаратуры). Лицо, осуществляющее проверку данных, должно иметь собственный открытый криптографический ключ от надежной ~~европейской~~ **корневой** организации.

Данные, загруженные с БУ, подписываются с использованием общих механизмов защиты, предусмотренных **подразделом 11, часть В (система тахографа второго поколения)**, за исключением случаев, когда контроль водителей осуществляется контрольным органом страны, не входящей в ЕС, с использованием контрольной карточки первого поколения; в этом случае данные подписываются на основании **подраздела 11 «Общие механизмы защиты», часть А (система тахографа первого поколения)**, как того требует **подраздел 15 «Переход на новые версии, требование MIG_015»**.

По этой причине в данном подразделе указаны два типа загрузки данных с БУ:

- Тип загрузки данных с БУ поколения 2, обеспечивающий структуру данных поколения 2 и подписанный в соответствии с **подразделом 11 «Общие механизмы защиты», часть В**;
- Тип загрузки данных с БУ поколения 1, обеспечивающий структуру данных поколения 2 и подписанный в соответствии с **подразделом 11 «Общие механизмы защиты», часть А**.

Аналогичным образом существует два типа загрузки данных с карточек водителя второго поколения, вставленных в БУ, как указано в пунктах 3 и 4 настоящего подраздела.

DDP_001 Данные, загруженные за один сеанс загрузки, должны сохраняться на ВН в виде одного файла.

1.2 Сокращения и обозначения

В настоящем подразделе используются следующие сокращения:

AID	Идентификатор приложений
ATR	Ответ на сигнал перезагрузки

CS	Байт контрольной суммы
DF	Каталог
DS_	Диагностический сеанс
EF	Элементарный файл
ESM	(ВН) Внешний носитель
FID	Идентификатор файла (ИД файла)
FMT	Байт формата (первый байт в заголовке сообщения)
ICC	Карточка на интегральной микросхеме
IDE	(СПА) Специализированная программируемая аппаратура: аппаратура, используемая для загрузки данных на ВН (например, персональный компьютер)
IFD	Устройство считывания карточек (интерфейс)
KWP	Протокол ключевых слов 2000
LEN	Байт длины (последний байт в заголовке сообщения)
PPS	Выбор параметра протокола
PSO	Выполнение защитной операции
SID	Идентификатор функции
SRC	Байт адреса источника
TGT	Байт адреса приемника
TLV	Значение длины метки
TREP	Параметр ответа на запрос передачи
TRTP	Параметр запроса передачи
VU	(БУ) Бортовое устройство

2. Загрузка данных с БУ

2.1 Процедура загрузки

Для загрузки данных с БУ оператору необходимо выполнить следующие действия:

- ввести свою карточку тахографа в считывающее устройство БУ(*);
- подсоединить СПА к выходному разъему БУ;
- установить канал связи между СПА и БУ;
- с помощью СПА выбрать данные для загрузки и передать запрос в БУ;
- завершить сеанс загрузки.

(*) Ввод карточки инициирует подтверждение соответствующих прав доступа к функции загрузки и загружаемым данным. Однако данные также можно загружать с карточки водителя, введенной в одно из считывающих устройств БУ, если в другое считывающее устройство никакая карточка другого типа не вставлена.

2.2 Протокол загрузки данных

Протокол построен по принципу «ведущий-ведомый», при котором в роли ведущего выступает СПА, а в роли ведомого — БУ.

Структура, типы и поток сообщений в основном соответствуют протоколу ключевых слов KWP 2000 (ISO 14230-2 Транспорт дорожный. Системы диагностического контроля. Протокол ключевых слов 2000. Часть 2. Уровень обмена данными).

Уровень приложений в основном соответствует нынешней версии проекта стандарта ISO 14229-1 (Транспорт дорожный. Системы диагностического контроля. Часть 1. Диагностические функции, версия 6 от 22 февраля 2001 года).

2.2.1 Структура сообщений

DDP_002 Все сообщения, которыми обмениваются СПА и БУ, формируются в соответствии с трехкомпонентной структурой:

- Заголовок, состоящий из байта формата (FMT), байта адреса приемника (TGT), байта адреса источника (SRC) и в некоторых случаях также байта длины сообщения (LEN).
- Поле данных, образуемое байтом идентификатора функции (SID) и переменным числом байтов данных, включая необязательный байт диагностического сеанса (DS_) или необязательный байт параметра передачи (TRTP или TREP),
- Контрольная сумма, определяемая байтом контрольной суммы (CS).

Заголовок				Поле данных					Контрольная сумма
FMT	TGT	SRC	LEN	SID	DONNÉES	CS
4 байта				до 255 байт					1 байт

Байты TGT и SRC указывают физические адреса получателя и отправителя сообщения. Их значения — F0 Hex для СПА и EE Hex для БУ.

Байт LEN представляет собой длину поля данных в сообщении.

Байт контрольной суммы представляет собой 8-битную сумму по модулю 256 всех байтов сообщения, за исключением самой контрольной суммы.

Определения байтов FMT, SID, DS_, TRTP и TREP приводятся далее в настоящем документе.

DDP_003 Если объем передаваемых в сообщении данных превышает длину поля данных, то сообщение фактически высылается в виде нескольких подсообщений. Каждое подсообщение содержит заголовок, одни и те же байты SID и TREP, а также 2-байтовый счетчик подсообщений, указывающий порядковый номер данного подсообщения в общем сообщении. Чтобы обеспечить возможность обнаружения ошибок и отмены передачи, СПА подтверждает получение каждого подсообщения. СПА может принять подсообщение, запросить его повторную передачу, выдать БУ команду начать передачу заново или отменить ее.

DDP_004 Если поле данных последнего подсообщения содержит ровно 255 байтов, то к нему необходимо добавить заключительное подсообщение с пустым (то есть содержащим только SID, TREP и счетчик подсообщений) полем данных с целью указать на конец сообщения.

Пример:

Заголовок	SID	PRT	Сообщение			CS
4 байта	Длина более 255 байтов					

Передается как:

Заголовок	SID	PRT	00	01	Подсообщение 1	CS
4 байта	255 байтов					

Заголовок	SID	PRT	00	02	Подсообщение 2	CS
4 байта	255 байтов					

...

Заголовок	SID	PRT	xx	yy	Подсообщение n	CS
4 байта	Длина менее 255 байтов					

Или как:

Заголовок	SID	PRT	00	01	Подсообщение 1	CS
4 байта	255 байтов					

Заголовок	SID	PRT	00	02	Подсообщение 2	CS
4 байта	255 байтов					

...

Заголовок	SID	PRT	xx	yy	Подсообщение n	CS
4 байта	255 байтов					

Заголовок	SID	PRT	xx	yy+1	CS	
4 байта	4 байта					

2.2.2 Типы сообщений

Протокол загрузки данных для БУ и СПА предусматривает обязательный обмен сообщениями восьми типов.

Общая характеристика этих сообщений представлена в таблице ниже.

Структура сообщений	До 4 байтов Заголовок				До 255 байтов Данные			1 байт Контрольная сумма
	FMT	TGT	SRC	LEN	SID	DS_/TRTP	ДАнные	CS
СПА-> <-БУ								
Запрос на начало обмена сообщениями	81	EE	F0		81			E0
Положительный ответ: инициализация обмена данными	80	F0	EE	03	C1		EA, 8F	9B
Запрос инициализации диагностического сеанса	80	EE	F0	02	10	84		F4
Положительный ответ: инициализация диагностики	80	F0	EE	02	50	84		34
Функция регулировки канала обмена данными Проверка скорости передачи данных (этап 1)								
9-600 Bd	80	EE	F0	04	87		01,01,01	EC
19-200 Bd	80	EE	F0	04	87		01,01,02	ED
38-400 Bd	80	EE	F0	04	87		01,01,03	EE
57-600 Bd	80	EE	F0	04	87		01,01,04	EF
115-200 Bd	80	EE	F0	04	87		01,01,05	F0
Положительный ответ Проверить скорость передачи данных	80	F0	EE	02	C7		01	28
Скорость передачи данных при переходе (этап 2)	80	EE	F0	03	87		02,03	ED
Запрос на загрузку	80	EE	F0	0A	35		00,00,00,00 00,FF,FF, FF,FF	99
Запрос на положительный ответ Загрузка	80	F0	EE	03	75		00,FF	D5
Запрос данных передачи								
Общие сведения	80	EE	F0	02	36	01 или 21		97
Деятельность	80	EE	F0	06	36	02 или 22	Дата	CS
События и неисправности	80	EE	F0	02	36	03 или 23		99
Детальные данные о скорости	80	EE	F0	02	36	04 или 24		9A
Технические данные	80	EE	F0	02	36	05 или 25		9B
Загрузка с карточки	80	EE	F0	02	36	06	Считывающее устройство:	CS
Положительный ответ: передача данных	80	F0	EE	Len	76	TREP	Данные	CS
Запрос завершения передачи	80	EE	F0	01	37			96
Положительный ответ: запрос на завершение передачи	80	F0	EE	2	77			D6
Запрос на прекращение связи	80	EE	F0	01	82			E4
Положительная реакция прекращение связи	80	F0	EE	01	C2			24
Подтверждение приема подсообщения	80	EE	F0	Len	83		Данные	CS
Отрицательные ответы								
Общее отклонение запроса	80	F0	EE	03	7F	Sid-Req	10	CS
Услуга не поддерживается	80	F0	EE	03	7F	Sid-Req	11	CS
Подфункция не поддерживается	80	F0	EE	03	7F	Sid-Req	12	CS
Неправильная длина сообщения	80	F0	EE	03	7F	Sid-Req	13	CS
Неправильные условия или ошибка последовательности запросов	80	F0	EE	03	7F	Sid-Req	22	CS
Запрос вне установленного диапазона	80	F0	EE	03	7F	Sid-Req	31	CS
-Отказ в приеме загружаемых данных	80	F0	EE	03	7F	Sid-Req	50	CS
Ответ ожидается	80	F0	EE	03	7F	Sid-Req	78	CS
Данные недоступны	80	F0	EE	03	7F	Sid-Req	FA	CS

Структура сообщения	До 4 байтов Заголовок				До 255 байтов Данные			1 байт Контрольная сумма
	FMT	TGT	SRC	LEN	SID	DS_/TRTP	ДАнные	CS
IDE -> <- VU								
Запрос на инициализацию обмена данными	81	EE	F0		81			E0
Положительный ответ, начало сеанса	80	F0	EE	03	C1		EA, 8F	9B
Запрос на инициализацию диагностического сеанса	80	EE	F0	02	10	81		F1
Положительный ответ: инициализация диагностики	80	F0	EE	02	50	81		31
Функция регулировки канала обмена данными								
Проверка скорости передачи данных (этап 1)								
9 600 Bd	80	EE	F0	04	87	01	01,01	EC
19 200 Bd	80	EE	F0	04	87	01	01,02	ED
38 400 Bd	80	EE	F0	04	87	01	01,03	EE
57 600 Bd	80	EE	F0	04	87	01	01,04	EF
115 200 Bd	80	EE	F0	04	87	01	01,05	F0
Положительный ответ, Проверка скорости передачи данных	80	F0	EE	02	C7	01		28
Скорость передачи в бодах при переходе (этап 2)	80	EE	F0	03	87	02	03	ED
Запрос на загрузку	80	EE	F0	0A	35		00,00,00,00, 00,FF,FF, FF,FF	99
Загрузка положительного ответа на запрос	80	F0	EE	03	75		00,FF	D5
Запрос на передачу данных								
Загрузка версии интерфейса	80	EE	F0	02	36	00		96
Общие сведения	80	EE	F0	02	36	01, 21 или 31		CS
Деятельность	80	EE	F0	06	36	02, 22 или 32	Дата	CS
События и неисправности	80	EE	F0	02	36	03, 23 или 33	Дата	CS
Детальные данные о скорости	80	EE	F0	02	36	04 или 24	Дата	CS
Технические данные	80	EE	F0	02	36	05, 25 или 35	Дата	CS
Загрузка с карточки	80	EE	F0	02 или 03	36	06	Считывающее устройство	CS
Положительный ответ на передачу данных	80	F0	EE	Len	76	TREP	Данные	CS
Запрос на завершение передачи	80	EE	F0	01	37			96
Положительный ответ: запрос на завершение передачи	80	F0	EE	01	77			D6
Запрос на прекращение обмена сообщениями	80	EE	F0	2	82			E1
Положительный ответ на прекращение обмена	80	F0	EE	01	C2			21
Подтверждение приема подсообщения	80	EE	F0	Len	83		Данные	CS
Отрицательные ответы								
Общее отклонение запроса	80	F0	EE	03	7F	Sid Req	10	CS
Функция не поддерживается	80	F0	EE	03	7F	Sid Req	11	CS
Подфункция не поддерживается	80	F0	EE	03	7F	Sid Req	12	CS
Неверная длина сообщения	80	F0	EE	03	7F	Sid Req	13	CS
Неправильные условия или ошибка в очередности запросов	80	F0	EE	03	7F	Sid Req	22	CS
Нештатный запрос	80	F0	EE	03	7F	Sid Req	31	CS
Отказ в приеме загружаемых данных	80	F0	EE	03	7F	Sid Req	50	CS
Ожидается ответ	80	F0	EE	03	7F	Sid Req	78	CS
Данные недоступны	80	F0	EE	03	7F	Sid Req	FA	CS

Примечания:

- Sid Req = Sid соответствующего запроса.
- TREP = TRTP соответствующего запроса.

- Темный фон ячейки в таблице означает отсутствие передачи данных.
- Термин «upload» (загрузка со стороны СПА) используется для целей совместимости с ISO 14229. Он имеет тот же смысл, что и термин «download» (загрузка со стороны БУ).
- Потенциальные 2-байтовые счетчики подсообщений, которые могут содержаться в сообщениях, в таблице не показаны.
- Считывающее устройство — это номер считывающего устройства: «1» (для карточки водителя) или «2» (для карточки второго водителя)
- Если номер считывающего устройства не указан, БУ выбирает устройство № 1, если в него вставлена карточка, а устройство № 2 выбирается только в том случае, если его конкретно выбрал пользователь.
- TRTP 24 используется для поколения 2 в целях запросов на загрузку данных БУ версии 1 и версии 2.
- TRTP 00, 31, 32, 33 и 35 используются для запросов на загрузку данных БУ версии 2 поколения 2.
- TRTP 21, 22, 23 и 25 используются для запросов на загрузку данных БУ версии 1 поколения 2.
- TRTP 01–05 используются для запросов на загрузку данных БУ поколения 1. В качестве варианта они могут приниматься БУ поколения 2, но только в случае контроля водителей, осуществляемого контрольным органом, не относящимся к компетенции ЕС, с использованием контрольной карточки первого поколения.
- TRTP 11–1F зарезервированы для запросов на загрузку, специфичных для изготовителя.
- ~~TRTP 21–25 используются для запросов на загрузку данных БУ поколения 2, TRTP 01–05 используются для запросов на загрузку данных БУ поколения 1, которые могут приниматься БУ только в рамках контроля водителей, осуществляемого контрольным органом страны, не входящей в состав Европейского союза, с использованием карточки контроля первого поколения.~~
- ~~TRTP 11–19 и 31–39 зарезервированы для специфических запросов на загрузку со стороны изготовителя.~~

2.2.2.1 Запрос инициализации обмена данными (SID 81)

DDP_005 Это сообщение выдается СПА в целях установления канала обмена данными с БУ. Начальная скорость передачи данных во всех случаях составляет 9600 бод (до тех пор, пока она не будет изменена при помощи соответствующих функций управления передачей данных).

2.2.2.2 Положительный ответ на инициализацию обмена данными (SID C1)

DDP_006 Это сообщение выдается БУ в качестве положительного ответа на запрос инициализации обмена данными. Он включает 2-х байтовые ключи 'EA' '8F', указывающих на поддержку данного протокола этим устройством, и заголовок с информацией о получателе и длине сообщения.

2.2.2.3 Запрос инициализации диагностического сеанса (SID 10)

DDP_007 Сообщение с запросом инициализации диагностического сеанса высылается СПА с целью начать новый сеанс обмена диагностическими данными с БУ. Подфункция «default session» (81 Hex) указывает на то, что в данном случае будет начат стандартный диагностический сеанс.

2.2.2.4 Положительный ответ: инициализация диагностики (SID 50)

DDP_008 Сообщение с положительным ответом на запрос инициализации диагностики высылает БУ с целью подтвердить начало диагностического сеанса.

2.2.2.5 Функция регулировки канала обмена данными (SID 87)

DDP_052 Функция управления передачей данных используется СПА с целью инициировать изменение скорости передачи данных в бодах. Это происходит в два этапа. На первом этапе СПА предлагает изменить скорость передачи, указывая новую скорость. По получении от БУ положительного ответа СПА высылает БУ подтверждение изменения скорости (второй этап). Затем СПА переключается на новую скорость передачи данных. После получения подтверждения БУ изменяет скорость передачи данных в бодах на новую.

2.2.2.6 Регулировка канала обмена данными: положительный ответ (SID C7)

DDP_053 Это сообщение высылается БУ в качестве положительного ответа на запрос регулировки канала обмена данными (первый этап). Следует обратить внимание на то, что ответ на запрос подтверждения не высылается (второй этап).

2.2.2.7 Запрос загрузки (SID 35)

DDP_009 Сообщение с запросом загрузки высылается СПА с целью указать БУ на необходимость загрузить данные. В соответствии с требованиями **ISO 14229** в него должна включаться информация, касающаяся адреса, объема и формата запрашиваемых данных. Поскольку до загрузки данных СПА такой информацией не располагает, адрес ячейки памяти при этом устанавливается на 0, формат указывается как нешифрованный и без сжатия, а объем памяти задается максимальным.

2.2.2.8 Положительный ответ на запрос загрузки (SID 75)

DDP_010 Сообщение с положительным ответом в связи с запросом на загрузку высылается БУ с целью указать СПА на готовность БУ к загрузке данных. В соответствии с требованиями ISO 14229 в это сообщение включаются данные, указывающие СПА на то, что последующие положительные ответы на запросы передачи данных будут содержать максимум 00FF шестнадцатеричных байтов.

2.2.2.9 Запрос передачи данных (SID 36)

DDP_011 Запрос на передачу данных высылается СПА с целью указать БУ тип данных, которые должны быть загружены. Тип данных указывается однобайтовым параметром запроса передачи (TRTP).

Возможна передача ~~семи~~ типов данных. В целях загрузки данных БУ для каждого типа передачи можно использовать два различных значения TRTP:

Тип передачи данных	Значение TRTP для типа загрузки данных БУ поколения 1	Значение TRTP для типа загрузки данных БУ поколения 2 версии 1	Значение TRTP для типа загрузки данных БУ поколения 2 версии 2
Скачать версию интерфейса	Не используется	Не используется	00
Общие положения	01	21	31
Деятельность на указанную дату	02	22	32

Тип передачи данных	Значение TRTP для типа загрузки данных БУ поколения 1	Значение TRTP для типа загрузки данных БУ поколения 2 версии 1	Значение TRTP для типа загрузки данных БУ поколения 2 версии 2
События и неисправности	03	23	33
Детальные показания скорости	04	24	24
Технические данные	05	25	35

Тип передачи данных	Значение TRTP
Загрузка карточки	06

DDP_054 В ходе сеанса загрузки СПА в обязательном порядке запрашивает передачу общих сведений (TRTP 01, **21** или **231**), так как только в этом случае в загружаемом файле регистрируются сертификаты БУ (что создает возможность проверки цифровой подписи).

Во **втором третьем** случае (TRTP 02, **22** или **232**) сообщение с запросом на передачу данных включает в себя указание календарной даты (в формате TimeReal), данные за которую подлежат загрузке.

2.2.2.10 Положительный ответ: передача данных (SID 76)

DDP_012 Положительный ответ на запрос по поводу передачи данных высылается БУ по получении запроса на передачу данных. Это сообщение содержит запрошенные данные и параметр ответа на запрос по поводу передачи (TREP), который соответствует TRTP запроса.

DDP_055 В первом случае (TREP 01, 21 или **231**) БУ посылает данные, помогающие оператору СПА выбрать те данные, загрузку которых он желает продолжить. Сообщение содержит данные о:

- сертификатах безопасности;
- идентификации транспортного средства;
- текущей дате и текущем времени по хронометражу БУ;
- самой ранней и самой поздней дате, данные за которую могут быть загружены из БУ;
- наличию карточек в считывающих устройствах БУ;
- предыдущей загрузке данных соответствующему предприятию;
- блокировках, установленных предприятием;
- предыдущих проверках.

2.2.2.11 Запрос на завершение передачи (SID 37)

DDP_013 Сообщение с запросом на завершение передачи высылается СПА с целью указать БУ на завершение сеанса загрузки.

2.2.2.12 Положительный ответ на запрос по поводу завершения передачи (SID 77)

DDP_014 Сообщение с положительным ответом на запрос по поводу завершения передачи высылается БУ с целью подтвердить прием запроса на завершение передачи.

2.2.2.13 Запрос на завершение обмена данными (SID 82)

DDP_015 Сообщение с запросом на завершение обмена данными высылается СПА с целью закрыть канал обмена данными с БУ.

2.2.2.14 Положительный ответ на запрос по поводу завершения обмена данными (SID C2)

DDP_016 Сообщение с положительным ответом на запрос по поводу завершения обмена данными высылается БУ с целью подтвердить прием запроса на завершение обмена данными.

2.2.2.15 Подтверждение приема подсообщения (SID 83)

DDP_017 Подтверждение приема подсообщения высылается СПА, подтверждая тем самым получение каждой части сообщения, передаваемого в виде ряда подсообщений. Поле данных содержит SID, полученный от БУ, и двухбайтовый код со следующими возможными значениями:

- MsgC +1 подтверждает правильный прием номера подсообщения MsgC.

Запрос СПА в БУ на отправку следующего подсообщения

- MsgC указывает на проблему с получением номера подсообщения MsgC.

Запрос СПА в БУ на повторную отправку данного подсообщения.

- FFFF — запрос на прекращение передачи сообщения.

Эта функция может использоваться СПА в целях прекращения по каким-либо причинам передачи данного сообщения со стороны БУ.

Прием последнего подсообщения соответствующего сообщения (LEN < 255 байтов) может подтверждаться любым из вышеуказанных кодов или оставаться без подтверждения.

Ответы БУ, которые состоят из нескольких подсообщений, включают:

- Положительный ответ на запрос по поводу передачи данных (SID 76)

2.2.2.16 Отрицательный ответ (SID 7F)

DDP_018 Сообщение с отрицательным ответом на те или иные из перечисленных выше запросов БУ высылает в тех случаях, когда запрос не может быть выполнен. Поле данных сообщения содержит SID ответа (7F), SID запроса и код, указывающий причину отрицательного ответа. В этой связи могут использоваться следующие коды:

- 10 общее отклонение запроса

Действие не может быть выполнено по причине, не входящей в число нижеперечисленных.

- 11 функция не поддерживается

SID запроса не опознан.

- 12 подфункция не поддерживается

Не понятны DS_ или TRTP запроса или отсутствуют другие подсообщения, подлежащие передаче.

- 13 Неверная длина сообщения

Получен ответ, указывающий на неправильную длину сообщения.

- 22 Неправильные условия или ошибка в очередности запросов

Требуемая функция не активирована либо очередность запросов неверна.

- 31 Нештатный запрос

Значение параметра запроса (поле данных) недействительно.

- 50 Отказ в приеме загружаемых данных

Невозможно выполнить запрос (несоответствие режима работы БУ или внутренние неполадки в БУ).

- 78 Ожидается ответ

Запрошенная операция не может быть завершена своевременно; БУ не готов к приему нового запроса.

- Данные FA отсутствуют

Объект данных, подлежащий передаче, отсутствует в БУ (например, не введена карточка, загрузка данных с БУ поколения 1 запрошена в обход проверки водителя контрольным органом, не уполномоченным ЕС...).

2.2.3 Поток сообщений

При нормальной загрузке данных поток сообщений, как правило, выглядит следующим образом:

СПА		БУ
Запрос на инициализацию обмена данными	⇒ ⇐	Положительный ответ
Запрос на инициализацию диагностического сеанса	⇒ ⇐	Положительный ответ
Запрос на загрузку	⇒ ⇐	Положительный ответ
Запрос на передачу общих сведений	⇒ ⇐	Положительный ответ
Запрос на передачу данных #2	⇒ ⇐	Положительный ответ #1
Подтверждение приема подсообщения #1	⇒ ⇐	Положительный ответ #2
Подтверждение приема подсообщения #2	⇒ ⇐	Положительный ответ #m
Подтверждение приема подсообщения #m	⇒ ⇐	Положительный ответ (поле данных <255 байтов)
Подтверждение приема подсообщения (факультативно)	⇒	
...		
Запрос на передачу данных #n	⇒ ⇐	Положительный ответ
Запрос на завершение передачи	⇒ ⇐	Положительный ответ
Запрос на завершение обмена данными	⇒ ⇐	Положительный ответ

2.2.4 Временные параметры

DDP_019 Временные параметры для нормального режима работы указаны в таблице ниже:

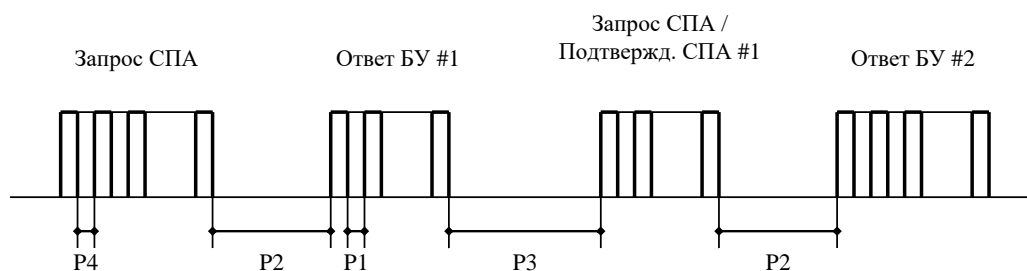


Рис. 1 — Поток сообщений и временные параметры,

где:

P1 = Межбайтовый интервал для ответа БУ.

P2 = Время между окончанием запроса СПА и началом ответа БУ или между окончанием подтверждения СПА и началом следующего ответа БУ.

P3 = Время между окончанием ответа БУ и началом нового запроса СПА или между окончанием ответа БУ и началом подтверждения СПА, или между окончанием запроса СПА и началом нового запроса СПА при отсутствии ответа от БУ.

P4 = Межбайтовый интервал для запроса СПА.

P5 = Расширенное значение P3 для загрузки данных с карточек.

Допустимые значения временных параметров приводятся в нижеследующей таблице (расширенный диапазон временных параметров протокола KWP для использования в случае физической адресации в порядке ускорения передачи данных).

Временной параметр	Нижнее предельное значение (мс)	Верхнее предельное значение (мс)
P1	0	20
P2	20	1000 (*)
P3	10	5000
P4	5	20
P5	10	20 минут

(*) если БУ выдает отрицательный ответ с кодом, означающим «запрос получен правильно — ожидается ответ», то это значение увеличивается до соответствующего верхнего предельного значения P3.

2.2.5 Обработка ошибок

В случае возникновения ошибки в процессе обмена сообщениями схема потока сообщений модифицируется в зависимости от того, каким из устройств обнаружена эта ошибка и каким сообщением она вызвана.

На рис. 2 и рис. 3 показаны процедуры обработки ошибок, соответственно, для БУ и для СПА.

2.2.5.1 Стадия инициализации обмена данными

DDP_020 Если СПА обнаруживает ошибку синхронизации или ошибку в битовом потоке на стадии инициализации обмена данными, то период ожидания СПА перед повторением запроса равен P3 min.

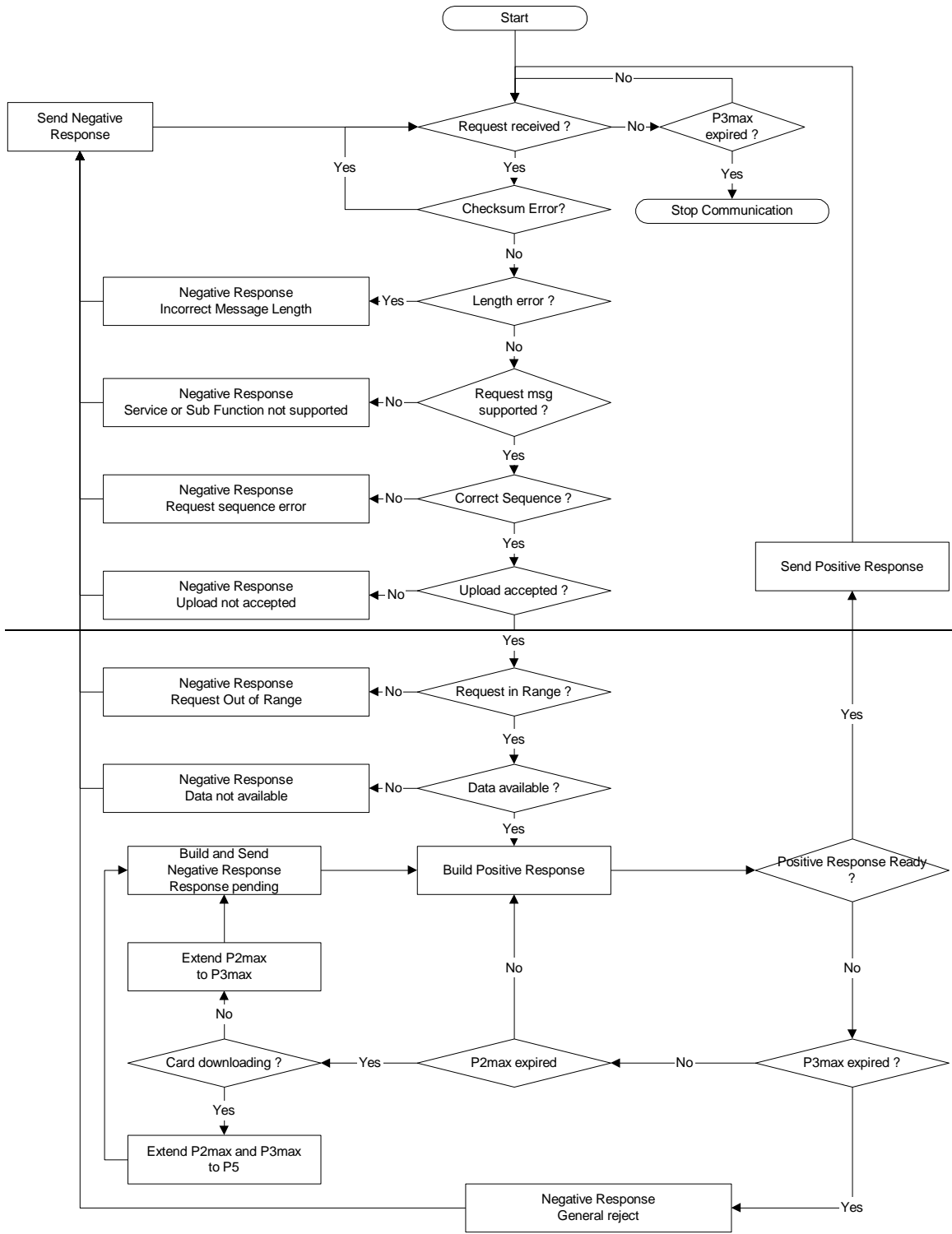
DDP_021 Если БУ обнаруживает ошибку в очередности сообщений от СПА, то оно не высылает ответ и ожидает новое сообщение с запросом на инициализацию обмена данными в течение периода, равного P3 max.

2.2.5.2 Стадия обмена данными

На этой стадии можно выделить два типовых случая обработки ошибок:

1. БУ обнаруживает ошибку в передаче данных от СПА

- DDP_022 БУ проверяет каждое полученное сообщение на ошибки синхронизации, ошибки в формате байтов (например, в стартовом и стоповом разрядах) и ошибки передачи кадров (неверное число полученных байтов, ошибки в байте контрольной суммы).
- DDP_023 При обнаружении одной из вышеназванных ошибок БУ не отвечает и игнорирует поступившее сообщение.
- DDP_024 БУ может обнаружить и другие ошибки в формате или содержании полученного сообщения (например, «сообщение не поддерживается»), даже если оно соответствует требованиям по длине и контрольной сумме; в этом случае БУ высылает СПА отрицательный ответ с указанием характера ошибки.



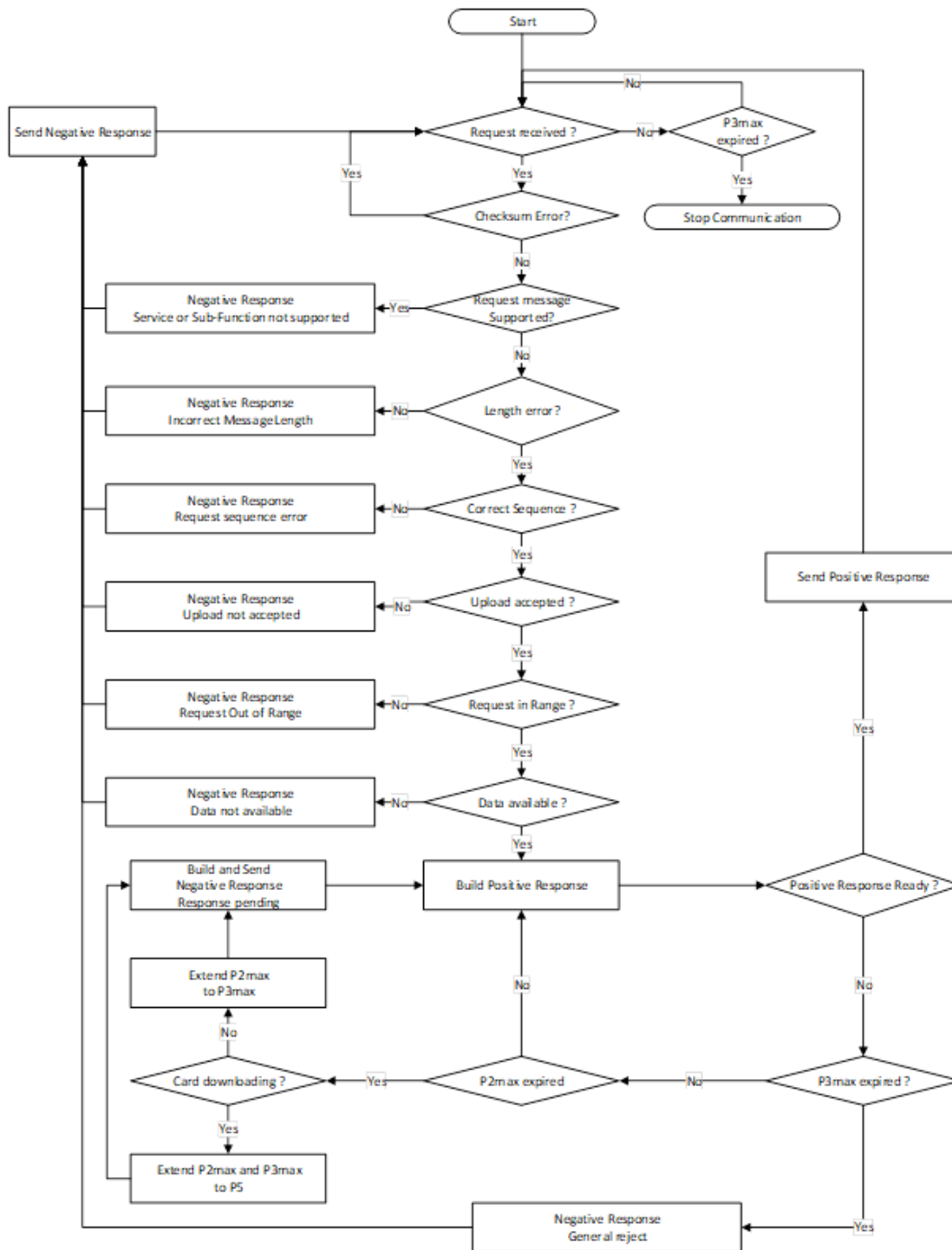


Рис. 2 — Обработка ошибок БУ

2. СПА обнаруживает ошибку в передаче данных от БУ

DDP_025 СПА проверяет каждое полученное сообщение на наличие ошибок синхронизации, ошибок в формате байтов (например, в стартовом и стоповом разрядах) и ошибок в передаче фреймов (неверное число полученных байтов, ошибки в байте контрольной суммы).

DDP_026 СПА проверяет поступающие сообщения на ошибки очередности, такие как сбои в возрастании порядковых номеров подсообщений в последовательно поступающих сообщениях.

DDP_027 Если СПА обнаруживает ошибку или не получает от БУ ответа в течение периода, равного P2max, запрос высылается повторно, причем общее число передач ограничивается тремя. В случае обнаружения ошибок данного вида подтверждение приема подсообщения рассматривается как запрос к БУ.

DDP_028 Период ожидания СПА перед началом каждой передачи составляет P3min или более; период ожидания измеряется с момента выявления последнего вычисленного стопового бита после обнаружения ошибки.

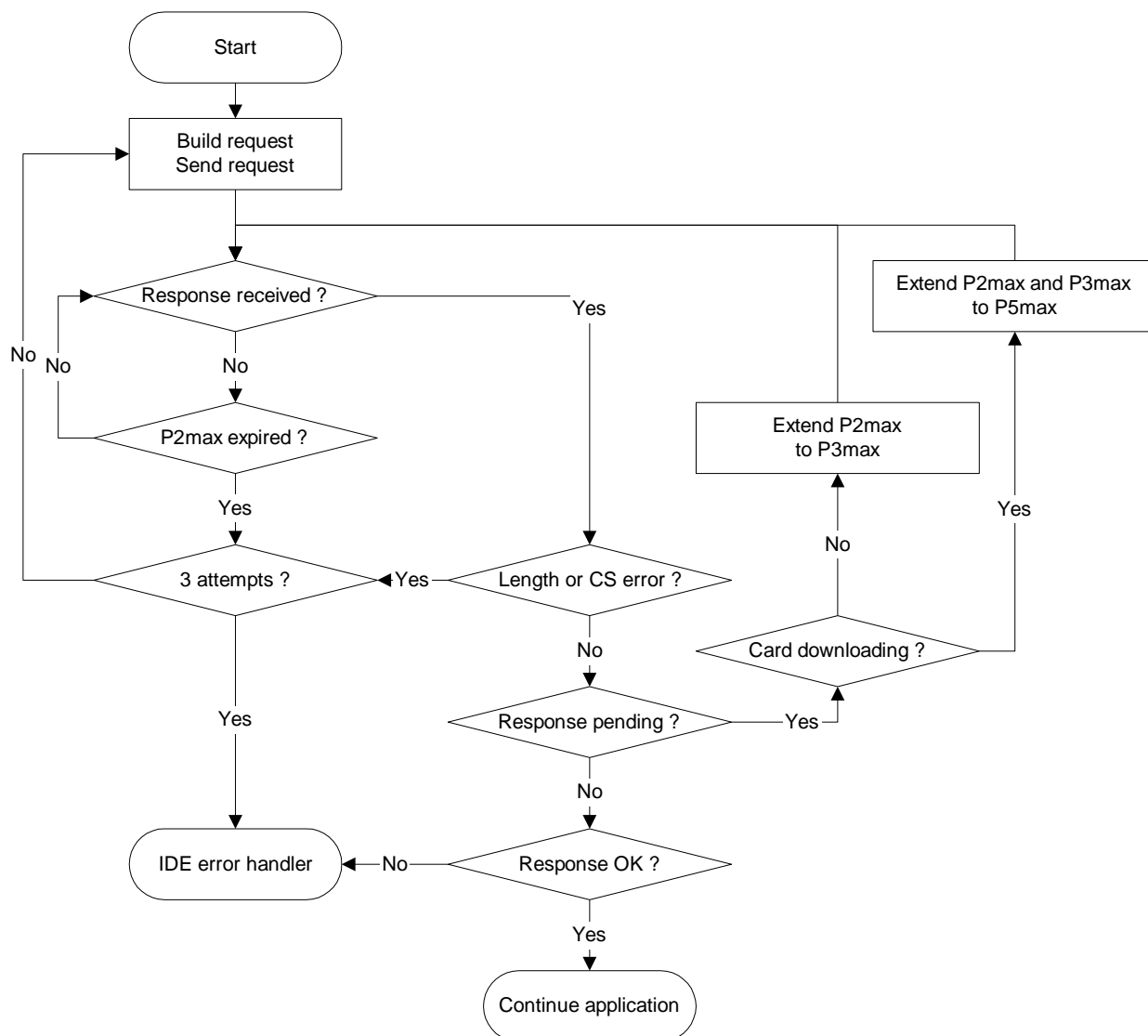


Рис. 3 — Обработка ошибок в БУ

2.2.6 Содержание ответного сообщения

В данном пункте указано содержание полей данных различных сообщений с положительным ответом.

Определения элементов данных приводятся в ~~добавлении~~ подразделе I (словарь данных).

Примечание: при загрузке данных поколения 2 каждый элемент данных высшего уровня отображается в виде массива записей, даже если в его состав входит лишь одна запись. Массив записей начинается с заголовка; данный заголовок содержит тип записи, размер записи и число записей. В нижеследующих таблицах массивы записей указаны под названием «...RecordArray» (с заголовком).

2.2.6.1 Положительный ответ: передача данных — версия интерфейса загрузки

DDP_028a Поле данных сообщения «Положительный ответ: передача данных — версия интерфейса загрузки» должно содержать следующие данные, расположенные в следующем порядке под названием SID 76 Hex, TREP 00 Hex:

Поколение структуры данных 2, версия 2 (TREP 00 Hex)

Элемент данных	Замечания
DownloadInterfaceVersion	Поколение и версия БУ: 02,02 Hex для поколения 2, версия 2 БУ поколения 1 и поколения 2 версии 1 не поддерживается, вследствие чего они будут выдавать отрицательный ответ (подфункция не поддерживается, см. DDP_018)

2.2.6.2 Положительный ответ: контроль за передачей данных

DDP_029 В поле данных сообщения «Положительный ответ: контроль за передачей данных» включаются данные, расположенные в следующем порядке под названием SID 76 Hex, TREP 01, 21 или 31 Hex, с соответствующим выделением и нумерацией подсообщений:

Поколение структуры данных 1 (TREP 01 Hex)

Элемент данных	Замечания
MemberStateCertificate	Сертификаты безопасности БУ, выдаваемые государствами-членами
VUCertificate	Сертификат БУ
VehicleIdentificationNumber	Идентификационный номер транспортного средства
VehicleRegistrationIdentification	Идентификационные данные регистрации транспортного средства
CurrentDateTime	Текущие дата и время по хронометражу БУ
VuDownloadablePeriod	Период, за который могут быть загружены данные
CardSlotsStatus	Типы карточек, вводимые в БУ
VuDownloadActivityData	Предшествующая загрузка данных в БУ
VuCompanyLocksData	Все сохраненные блокировки, установленные предприятием. Если раздел не заполнен, высылается только noOfLocks = 0
VuControlActivityData	Все сохраненные в БУ контрольные записи. Если раздел не заполнен, выдается только noOfLocks = 0
Подпись	Подпись криптосистемы RSA для всех данных (кроме сертификатов), от VehicleIdentificationNumber до последнего байта последней позиции VuControlActivityRecord

Структура данных поколения 2, версия 1 (TREP 21 Hex)

Элемент данных	Замечания
MemberStateCertificateRecordArray	Сертификат государства-члена Договаривающейся стороны (массив данных)
VuCertificateRecordArray	сертификат БУ (массив данных)
VehicleIdentificationNumberRecordArray	Идентификационные данные транспортного средства (массив данных)
VehicleRegistrationNumberRecordArray	Регистрационный номер транспортного средства (массив данных)
CurrentDateTimeRecordArray	текущие дата и время по хронометражу БУ (массив данных)
VuDownloadablePeriodRecordArray	Период, за который могут быть загружены данные (массив данных)
CardSlotsStatusRecordArray	Типы карточек, введенных в считывающие устройства БУ(массив данных)
VuDownloadActivityDataRecordArray	Предшествующая загрузка данных из БУ (массив данных)
VuCompanyLocksRecordArray	Все сохраненные блокировки, установленные предприятием. Если раздел не заполнен, высылается только noOfLocks = 0 (массив данных)
VuControlActivityRecordArray	Все сохраненные в БУ контрольные записи. Если раздел не заполнен, высылается только noOfRecords = 0 (массив данных)
SignatureRecordArray	Подпись ECC по всем предшествующим данным, за исключением сертификатов (массив данных)

Поколение структуры данных 2, версия 2 2 (TREP 31 Hex)

Элемент данных	Замечания
MemberStateCertificateRecordArray	Сертификат государства-члена Договаривающейся стороны (массив данных)
VUCertificateRecordArray	Сертификат БУ (массив данных)
VehicleIdentificationNumberRecordArray	Идентификационные данные транспортного средства (массив данных)
VehicleRegistrationNumberRecordArray	Регистрационный номер транспортного средства (массив данных)
CurrentDateTimeRecordArray	Текущие дата и время (массив данных)
VuDownloadablePeriodRecordArray	Период, за который могут быть загружены данные (массив данных)
CardSlotsStatusRecordArray	Тип карточек, введенных в считывающие устройство БУ (массив данных)
VuDownloadActivityDataRecordArray	Предшествующая загрузка данных из БУ (массив данных)
VuCompanyLocksRecordArray	Все блокировки, установленные предприятием, хранятся в БУ (массив данных)
VuControlActivityRecordArray	Все контрольные записи хранятся в БУ. Если раздел не заполнен, высылается только заголовок массива noOfControls = 0 (массив данных)

Элемент данных	Замечания
SignatureRecordArray	Подпись ECC по всем предшествующим данным, за исключением сертификатов (массив данных).

2.2.6.23 Положительный ответ: работа по передаче данных

DDP_030 Поле данных сообщения «Positive Response Transfer Data Activities» должно содержать следующие данные в следующем порядке в соответствии с SID 76 Hex, TREP 02, 22 или 232 Hex и соответствующим разделением и подсчетом подсообщений:

Структура данных поколения 1 (TREP 02 Hex)

Элемент данных	Замечания
TimeReal	Дата загрузки
OdometerValueMidnight	Показания счетчика пробега на конец суток, к которым относятся загружаемые данные
VuCardIWData	Информация о циклах ввода/извлечения карточек <ul style="list-style-type: none"> – Если в разделе нет данных, высылается только noOfVuCardIWRecords = 0 – Если внутри периода, охватываемого записью VuCardIWRecord, находится отметка 00:00 часов (карточка введена накануне) или 24:00 часа (карточка извлечена на следующий день), эта запись в полном объеме включается в данные за оба дня
VuActivityDailyData	Состояние считывающего устройства на 00:00 часов и изменения в деятельности водителей, зарегистрированные в течение суток, к которым относятся загружаемые данные
VuPlaceDailyWorkPeriodData	Информация о географических пунктах, зарегистрированная в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылается только noOfPlaceRecords = 0
VuSpecificConditionData	Информация об особых ситуациях, зарегистрированная в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылается только noOfSpecificConditionRecords=0
Подпись	Подпись криптосистемы RSA для всех данных, от TimeReal до последнего байта последней записи об особых ситуациях

Структура данных поколения 2, версия 1 (TREP 22 Hex)

Элемент данных	Замечания
DateOfDayDownloadedRecordArray	Дата загрузки
OdometerValueMidnightRecordArray	Показания счетчика пробега на конец суток, к которым относятся загружаемые данные
VuCardIWRecordArray	Информация о циклах ввода/извлечения карточек. <ul style="list-style-type: none"> – Если в разделе нет данных, высылается только заголовок массива данных noOfRecords = 0 – Если внутри периода, охватываемого записью VuCardIWRecord, находится отметка 00:00 часов (карточка введена накануне) или 24:00 часа (карточка извлечена на следующий день), эта запись в полном объеме включается в данные за оба дня

Элемент данных	Замечания
VuActivityDailyRecordArray	Состояние считывающего устройства на 00:00 часов и изменения в деятельности водителей, зарегистрированные в течение суток, к которым относятся загружаемые данные
VuPlaceDailyWorkPeriodRecordArray	Информация о географических пунктах, зарегистрированная в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылается только заголовок массива данных noOfPlaceRecords = 0
VuGNSSCDRecordArray VuGNSSADRecordArray	Местоположения транспортного средства по ГНСС, в которых непрерывное накопленное время управления водителем транспортным средством достигает значения, кратного трем часам. Если раздел не заполнен, высылается только заголовок массива данных noORecords = 0
VuSpecificConditionRecordArray	Если раздел не заполнен, высылается только noOfPlaceRecords = 0 Информация об особых ситуациях, зарегистрированная в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылается только заголовок массива данных noORecords = 0
SignatureRecordArray	Подпись криптосистемы ЕСС для всех предшествующих данных

Структура данных поколения 2, версия 2 (TREP 32 Hex)

Элемент данных	Замечания
DateOfDayDownloadedRecordArray	Дата суток, за которые загружается массив данных
OdometerValueMidnightRecordArray	Показания счетчика на пробеге конец суток, за которые загружаются данные
VuCardIWRecordArray	Данные о циклах ввода и извлечения карточек <ul style="list-style-type: none"> – Если в разделе данных нет, высылается только заголовок массива данных noORecords = 0 – Если внутри периода, охватываемого записью VuCardIWRecord, находится отметка 00:00 часов (карточка введена накануне) или 24:00 часа (карточка извлечена на следующий день), эта запись в полном объеме включается в данные за оба дня
VuActivityDailyRecordArray	Состояние считывающего устройства на 00:00 часов и изменения в деятельности водителей, зарегистрированные в течение суток, к которым относятся загружаемый массив данные
VuPlaceDailyWorkPeriodRecordArray	Если раздел не заполнен, высылается только заголовок массива данных noORecords = 0.
VuGNSSCDRecordArray VuGNSSADRecordArray	Местоположения транспортного средства по ГНСС, в которых непрерывное накопленное время управления водителем транспортным средством достигает значения, кратного трем часам. Если раздел не заполнен, высылается только заголовок массива данных noORecords = 0
VuSpecificConditionRecordArray	Информация об особых ситуациях, зарегистрированная в течение суток, к которым относятся загружаемые данные. Если в данном разделе данных нет, направляется только заголовок массива данных noOfecords=0

Элемент данных	Замечания
VuBorderCrossingRecordArray	Информация о пересечении границ за сутки, в отношении которых загружены данные. Если раздел не заполнен, направляется только заголовок массива данных noORecords = 0
VuLoadUnloadRecordArray	Информация об операциях загрузки/разгрузки, зарегистрированная в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, направляется только заголовок массива данных noORecords = 0
SignatureRecordArray	Подпись криптосистемы ECC для всех предшествующих данных

2.2.6.43 Положительный ответ на запрос передачи данных о событиях и неисправностях

DDP_031 В поле данных сообщения «Положительный ответ на запрос передачи данных о событиях и неисправностях» включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, в случае SID 76 Hex и TREP 03, 23 или 233 Hex, с соответствующим выделением и нумерацией подсообщений:

Структура данных поколения 1 (TREP 03 Hex)

Элемент данных	Замечания
VuFaultData	Вся сохраненная в БУ и текущая информация о неисправностях. Если в разделе данных нет, высылается только заголовок массива с указанием noOfVuFaults
VuEventData	Вся сохраненная в БУ и текущая информация о событиях (кроме превышений скорости). Если в разделе данных нет, высылается только noOfVuEvents = 0
VuOverSpeedingControlData	Данные, относящиеся к последнему контролю за превышениями скорости (при отсутствии данных — значение по умолчанию)
VuOverSpeedingEventData	Вся сохраненная в БУ и текущая информация о превышениях скорости. Если в разделе данных нет, высылается только noOfVuOverSpeedingEvents = 0
VuTimeAdjustmentData	Вся сохраненная в БУ информация о корректировках времени (кроме производимых в процессе общей калибровки) Если раздел не заполнен, высылается только noOfVuTimeAdjRecords = 0
Signature	Подпись криптосистемы RSA для всех данных, от noOfVuFaults до последнего байта последней записи о корректировках времени

Структура данных поколения 2, версия 1 (TREP 23 Hex)

Элемент данных	Замечания
VuFaultRecordArray	Вся сохраненная в БУ и текущая информация о неисправностях. Если раздел не заполнен, высылается только заголовок массива с указанием noOfVuFaults = 0
VuEventRecordArray	Все события (кроме превышения скорости), сохраненные или текущие в БУ Если раздел не заполнен, высылается только заголовок массива с указанием noOfRecords = 0

Элемент данных	Замечания
VuOverSpeedingControlDataRecordArray	Данные, относящиеся к последнему контролю за превышениями скорости (при отсутствии данных — значение по умолчанию)
VuOverSpeedingEventRecordArray	Вся сохраненная в БУ и текущая информация о превышениях скорости. Если раздел не заполнен, высылается только заголовок с указанием noOfRecords = 0
VuTimeAdjustmentRecordArray	Вся сохраненная в БУ информация о корректировках времени (кроме производимых в процессе общей калибровки) Если раздел не заполнен, то высылается только заголовок с указанием noOfRecords = 0
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Подпись криптосистемы ECC для всех предшествующих данных

Структура данных поколения 2, версия (TREP 33 Hex)

Элемент данных	Замечания
VuFaultRecordArray	Все неисправности, сохраненные или текущие в БУ Если раздел не заполнен, высылается только заголовок массива с указанием noOfRecords = 0
VuEventRecordArray	Все события (кроме превышения скорости), сохраненные или текущие в БУ Если раздел не заполнен, высылается только заголовок массива с указанием noOfRecords = 0
VuOverSpeedingControlDataRecordArray	Данные, относящиеся к последнему контролю за превышениями скорости (при отсутствии данных — значение по умолчанию)
VuOverSpeedingEventRecordArray	Вся сохраненная в БУ информация о превышениях скорости. Если раздел не заполнен, высылается только заголовок массива с указанием noOfRecords = 0
VuTimeAdjustmentRecordArray	Вся сохраненная в БУ информация о корректировках времени (кроме производимых в процессе общей калибровки). Если раздел не заполнен, высылается только заголовок с указанием noOfRecords = 0
SignatureRecordArray	Подпись криптосистемы для всех предшествующих данных

2.2.6.54 Положительный ответ на запрос передачи подробных данных о скоростном режиме

DDP_032 В поле данных сообщения «Положительный ответ на запрос передачи подробных данных о скоростном режиме» включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, в условиях SID 76 Hex, TREP 04 или 24 Hex, с соответствующим выделением и нумерацией подсообщений:

Структура данных поколения 1 (TREP 04 Hex)

Элемент данных	Замечания
VuDetailedSpeedData	Вся сохраненная в БУ подробная информация о скоростном режиме (один блок данных о скорости за каждую минуту движения транспортного средства) 60 значений скорости в минуту (по одному в секунду)

Элемент данных	Замечания
Signature	Подпись криптосистемы RSA для всех данных, от noOfSpeedBlocks до последнего байта последнего блока данных о скорости

Структура данных поколения 2 (TREP 24 Hex)

Элемент данных	Замечания
VuDetailedSpeedBlockRecordArray Data VuDetailedSpeedBlockRecord Array	Вся сохраненная в БУ подробная информация о скоростном режиме (один блок данных о скорости за каждую минуту движения транспортного средства) 60 значений скорости в минуту (по одному в секунду)
SignatureRecordArray	Подпись криптосистемы RSA ECC для всех предшествующих данных от noOfSpeedBlocks до последнего байта последнего блока данных о скорости

2.2.6.65 Положительный ответ на запрос передачи технических данных

DDP_033 В поле данных сообщения «Положительный ответ на запрос передачи технических данных» включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному в части SID 76 Hex, TREP 05, 25 или 235 Hex, с соответствующим выделением и нумерацией подсообщений:

Структура данных поколения 1 (TREP 05 Hex)

Элемент данных	Замечания
VuIdentification	
SensorPaired	
VuCalibrationData	Все сохраненные в БУ калибровочные записи
Подпись	Подпись криптосистемы RSA для всех данных, от vuManufacturerName до последнего байта последней записи VuCalibrationRecord

Структура данных поколения 2, версия 1 (TREP 25 Hex)

Элемент данных	Замечания
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Все данные о сопряжениях MS хранятся в БУ
VuSensorExternalGNSSCoupledRecordArray	Все данные о сопряжениях внешних устройств ГНСС хранятся в БУ
VuCalibrationRecordArray	Все калибровочные записи хранятся в БУ
VuCardRecordArray	Все данные о вводе карточек хранятся в БУ
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Информация о подписи криптосистемы ECC всех предшествующих данных.

Структура данных поколения 2, версия 2 (TREP 35 Hex)

Элемент данных	Замечания
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Все данные о сопряжениях MS хранятся в БУ
VuSensorExternalGNSSCoupledRecordArray	Все данные о сопряжениях внешних устройств ГНСС хранятся БУ
VuCalibrationRecordArray	Все калибровочные записи хранятся в БУ
VuCardRecordArray	Все данные о вводе карточек хранятся в БУ
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Информация о подписи криптосистемы ECC всех предшествующих данных

2.3 Сохранение файлов на ВН

DDP_034 В случаях, когда сеанс загрузки данных включает передачу данных с БУ, СПА сохраняет в виде одного физического файла все данные, полученные от БУ в ходе сеанса загрузки в сообщениях типа «Положительный ответ на запрос передачи данных». Сохраняемые данные не включают заголовки сообщений, счетчики подсообщений, пустые подсообщения и контрольные суммы, но включают SID и TREP (при наличии нескольких подсообщений — только для первого подсообщения).

3. Протокол загрузки данных с карточек тахографа

3.1 Сфера применения

В настоящем пункте изложен порядок прямой загрузки данных с карточки тахографа на СПА. СПА не является частью защищенной среды; поэтому процедура аутентификации между карточкой и СПА не предусмотрена.

3.2 Определения

Сеанс загрузки данных: Каждая загрузка данных с ИСС. Сеанс включает в себя всю процедуру, от перезапуска карточки считывающим устройством до деактивации ИСС (т. е. извлечения или новой перезагрузки карточки).

Подписанный файл данных: Файл из ИСС: файл передается на IFD в текстовой форме. В ИСС происходит хеширование и подпись файла, которая передается в IFD.

3.3 Загрузка с карточки

DDP_035 Процесс загрузки данных с карточки тахографа включает следующие этапы:

- Загрузка обычной информации, записанной на карточке в элементарных файлах ИСС и IC. Эта информация не является обязательной и не защищена цифровой подписью.

- (Для карточек тахографа первого и второго поколений)
 - **Загрузка файлов EF в Tachograph DF:**
 - элементарных файлов (EF) Card_Certificate ~~(or CardSignCertificate)~~ и CA_Certificate. Эта информация не защищена цифровой подписью.

Вышеуказанные файлы загружаются в обязательном порядке при каждом сеансе загрузки.

 - Загрузка данных элементарных файлов (EF) других приложений (в Tachograph DF и ~~Tachograph_C2 DF, если уместно~~), за исключением EF Card_Download. Эта информация защищена цифровой подписью **в соответствии с подразделом 11 «Общие механизмы безопасности, часть А».**

Кроме того, в обязательном порядке загружаются **в случае каждого сеанса загрузки**, как минимум, элементарные файлы (EF) Application_Identification и **Identification**.

 - При загрузке данных с карточки водителя в обязательном порядке загружаются также следующие элементарные файлы:

Events_Data,
 Faults_Data,
 Driver_Activity_Data,
 Vehicles_Used,
 Places,
 Control_Activity_Data,
 Specific_Conditions.
- (Для карточек тахографа только второго поколения)
 - За исключением случаев, когда загрузка данных с карточки водителя, введенной в БУ, производится в процессе проверки контрольным органом, не уполномоченным ЕС, с использованием контрольной карточки первого поколения при загрузке элементарных файлов (EF) в файл Tachograph_G2 DF:
 - Загрузка элементарных файлов CardSignCertificate, CA_Certificate и Link_Certificate ~~(в случае наличия)~~. Эта информация цифровой подписью не защищена.

Эти файлы необходимо загружать в обязательном порядке в случае каждого сеанса загрузки.

 - Загрузка данных EF других приложений (в случае Tachograph_G2 DF), за исключением EF Card_Download. Эта информация защищена цифровой подписью на основе подраздела 11 «Общие механизмы безопасности, часть В».

В случае каждого сеанса загрузки необходимо в обязательном порядке загрузить, как минимум, файлы (EF) Application_Identification, EF Application_Identification_V2 (в случае наличия) и Identification.

 - При загрузке данных с карточки водителя в обязательном порядке загружаются следующие элементарные файлы:

Events_Data,
 Faults_Data,

Driver_Activity_Data,
 Vehicles_Used,
 Places,
Control_Activity_Data,
Specific_Conditions,
VehicleUnits_Used,
 GNSS_Places (в случае наличия),
Places_Authentication, в случае наличия,
GNSS_Places_Authentication, в случае наличия,
Border_Crossings, в случае наличия,
Load_Unload_Operations, в случае наличия,

- **Load_Type_Entries, в случае наличия.** При загрузке данных с карточки тахографа следует обновить дату LastCardDownload в элементарном файле (EF) Card_Download, **Tachograph и, в случае применимости, в DFs Tachograph_G2.**
- При загрузке данных с карточки мастерской сбрасывается счетчик калибровки в элементарном файле Card_Download **в файлах данных Tachograph и, в случае применимости, в DFs Tachograph_G2.**
- При загрузке данных с карточки мастерской элементарные файлы Sensor_Installation_Data в файлах **Tachograph и, в случае применимости, Tachograph_G2** не загружаются.

3.3.1 Процедура инициализации

DDP_036 IDE инициирует следующую последовательность:

Карточка	Направление	IDE/IFD	Значение/Примечания
	⇐	Перезагрузка аппаратного обеспечения	
ATR	⇒		

Для переключения на более высокую скорость передачи данных, если она поддерживается ICC, можно использовать PPS.

3.3.2 Процедура для неподписанных файлов данных

DDP_037 Процедура загрузки файлов EF, ICC, IC, Card_Certificate (или CardSignCertificate) **в случае DF Tachograph_G2), CA_Certificate и Link_Certificate (только для DF Tachograph_G2)** выглядит следующим образом:

Карточка	Направление	IDE/IFD	Значение/Примечания
	⇐	Select File	Выбор файла по идентификаторам
OK	⇒		
	⇐	Read Binary	Если файл содержит больше данных, чем позволяет объем буфера считывающего устройства или карточки, то команду следует повторять до тех пор, пока не будет прочитан весь файл
File Data OK	⇒	Сохранение данных на ВН	в соответствии с 0 и коротким идентификатором EF. 3.4 Формат хранения данных

Примечание 1: Перед выбором элементарного файла Card_Certificate (или CardSignCertificate) необходимо выбрать приложение тахографа (выбор по AID).

Примечание 2: Выбор и чтение файла можно также выполнить в один прием при помощи команды Read Binary с коротким идентификатором EF.

3.3.3 Процедура для подписанных файлов данных

DDP_038 Для каждого из нижеперечисленных файлов, загружаемых вместе с соответствующей подписью, применяется следующая процедура:

Карточка	Направление	IDE/IFD	Значение/Примечания
	⇐	Выбрать файл	
OK	⇒		
	⇐	Произвести хеширование файла	Расчет хеш-функции по данным, содержащимся в выбранном файле, на основе хеш-алгоритма в соответствии с подразделом 11, части А или В . Эта команда не соответствует команде ISO
Расчет и временное хранение хеш-функции файла			
OK	⇒		
	⇐	Считывание двоичных файлов	Если файл содержит больше данных, чем может сохранить буфер считывающего устройства или карточки, команду следует повторять до тех пор, пока не будет прочитан весь файл
Данные файла OK	⇒	Сохранение полученных данных на ВН	в соответствии с 0 с коротким идентификатором EF 3.4 Формат хранения данных
	⇐	PSO: Вычисление цифровой подписи	
На основе временно сохраненной хеш-функции выполнить защитную операцию «генерирование цифровой подписи»			
Подпись OK	⇒	Приобщить данные к данным, сохраненным на ВН ранее	в соответствии с 0 с коротким идентификатором EF 3.4 Формат хранения данных

Примечание: Выбор и чтение файла можно также выполнить в один прием при помощи команды Read Binary с коротким идентификатором EF. В подобных случаях EF можно выбрать и прочитать до применения команды Perform Hash of File.

3.3.4 Процедура обнуления счетчика калибровок

DDP_039 Для обнуления счетчика NoOfCalibrationsSinceDownload в элементарном файле EF Card_Download на карточке мастерской, применяется следующая процедура:

Карточка	Направление	IDE/IFD	Значение/Примечания
	⇐	Выбрать файл EF Card_Download	Выбрать файла по идентификаторам
ОК	⇒		
	⇐	Обновить двоичный файл NoOfCalibrationsSinceDownload = '00 00'	
Обнулить значение загрузок данных карточки			
ОК	⇒		

Примечание: Выбрать и обновить файл можно в один прием командой Update Binary с коротким идентификатором EF.

3.4 Формат хранения данных

3.4.1 Введение

DDP_040 Загружаемые данные хранятся с соблюдением следующих условий:

- Данные хранятся в прозрачном виде. Это означает, что порядок следования байтов, а также порядок следования битов в байте, которые передаются с карточки, в процессе передачи должен сохраняться.
- Все файлы карточки, которые были сгружены с карточки в ходе соответствующего сеанса загрузки, хранятся в одном файле на ВН.

3.4.2 Формат файла

DDP_041 Формат файла представляет собой конкатенацию нескольких объектов TLV.

DDP_042 Меткой EF является FID с добавлением '00'.

DDP_043 Меткой подписи EF является FID файла с добавлением '01'.

DDP_044 Значение длины состоит из двух байтов. Им определяется число байтов в поле значений. Значение 'FF FF' в поле длины резервируется для последующего использования.

DDP_045 Если файл не загружается, никакая информация о нем сохранению не подлежит (т. е. не сохраняется ни метка, ни нулевой параметр длины).

DDP_046 В качестве объекта TLV, следующего непосредственно за объектом TLV с данными файла, сохраняется подпись.

Определение	Значение	Длина
FID (2 байта) '00'	Метка EF (FID) в Tachograph DF или общей информации о карточке	3 байта
FID (2 байта) '01'	Метка подписи EF (FID) в Tachograph DF	3 байта

Определение	Значение	Длина
FID (2 байта) '02'	Метка EF (FID) в Tachograph_G2 DF	3 байта
FID (2 байта) '03'	Метка подписи EF (FID) в Tachograph_G2 DF	3 байта
xx xx	Поле длины значения	2 байта

Пример данных в файле, загруженном на ВН:

Метка	Длина	Значение
00 02 00	00 14	Данные, касающиеся EF ICC
C1 00 00	00 C2	Данные, касающиеся EF Card_Certificate
		...
05 05 00	0A 2E	Данные EF Vehicles_Used (в Tachograph DF)
05 05 01	00 80	Подпись EF Vehicles_Used (в Tachograph DF)
05 05 02	0A 2E	Данные EF Vehicles_Used в Tachograph_G2 DF
05 05 03	xx xx	Подпись EF Vehicles_Used в Tachograph_G2 DF

4. Загрузка данных с карточки тахографа с помощью бортового устройства

DDP_047 БУ должно обеспечивать возможность загрузки данных с введенной в него карточки водителя на подключенную СПА.

DDP_048 Для инициализации данного режима СПА направляет БУ сообщение «Transfer Data Request Card Download» (Запрос на передачу данных, загружаемых с карточки) (см. 002.2.2.9).

DDP_049 Карточки водителя первого поколения: данные загружаются в соответствии с протоколом загрузки данных первого поколения, притом что загруженные данные будут иметь тот же формат, что и данные, загруженные с бортового устройства первого поколения.

Карточки водителя второго поколения: Затем БУ загружает всю карточку файл за файлом в соответствии с протоколом загрузки карточки, определенным в пункте 0, и посылает все данные, полученные с карточки, в СПА в соответствующем формате файла TLV (см. -) и включенные в сообщение «Positive Response Transfer Data» (положительный ответ на запрос передачи данных).

DDP_050 СПА извлекает данные карточки из сообщения «Положительный ответ на запрос передачи данных» (снимая все заголовки, SIDы, TREPы, показания счетчиков подсообщений и контрольных сумм) и сохраняет их в одном физическом файле, как указано в **пункте 00**.

DDP_051 Затем БУ, в случае применимости, обновляет содержание файла Control_Activity_Data или Card_Download на карточке водителя.

Подраздел 8

Протокол калибровки

Содержание

	<i>Стр.</i>
1. Введение	384
2. Термины, определения и справочные материалы	387
3. Обзор функций	387
3.1 Поддерживаемые функции	387
3.2 Коды ответов	388
4. Функции обмена данными	388
4.1 Функция StartCommunication	389
4.2 Функция StopCommunication	391
4.2.1 Описание сообщения	391
4.2.2 Формат сообщения	391
4.2.3 Определение параметров	392
4.3 Функция TesterPresent	392
4.3.1 Описание сообщения	392
4.3.2 Формат сообщения	392
5. Функции управления	393
5.1 Функция StartDiagnosticSession	394
5.1.1 Описание сообщения	394
5.1.2 Формат сообщения	394
5.1.3 Определение параметров	395
5.2 Функция SecurityAccess	396
5.2.1 Описание сообщения	396
5.2.2 Формат сообщения — SecurityAccess — requestSeed	397
5.2.3 Формат сообщения — SecurityAccess — sendKey	398
6. Функции передачи данных	399
6.1 Функция ReadDataByIdentifier	400
6.1.1 Описание сообщения	400
6.1.2 Формат сообщения	400
6.1.3 Определение параметров	401
6.2 Функция WriteDataByIdentifier	402
6.2.1 Описание сообщения	402
6.2.2 Формат сообщения	402
6.2.3 Определение параметров	404

7.	Настройка проверочных импульсов — контрольный функциональный блок регулировки входного/выходного сигнала	404
7.1	Функция InputOutputControlByIdentifier	404
7.1.1	Описание сообщения	404
7.1.2	Формат сообщения	405
7.1.3	Определение параметров	406
8.	Функция RoutineControl (корректировка времени)	407
8.1	Описание сообщения	407
8.2	Формат сообщения	407
9.	Форматы записей данных	410
9.1	Диапазоны передаваемых параметров	410
9.2	Форматы dataRecords	411

1. Введение

В настоящем **подразделе** описан порядок обмена данными между бортовым устройством и тестером по К-линии, являющейся частью интерфейса калибровки в соответствии с приложением 6. В ней также описывается система управления сигнальной линией ввода/вывода соединителя калибровки.

Порядок организации обмена данными по К-линии изложен в разделе 4 «**Функция обмена данными**».

Для определения задач управления обменом данными по К-линии в различных условиях в данном **подразделе** приложения используется понятие диагностических сеансов. Под этим сеансом понимается по умолчанию сеанс StandardDiagnosticSession, который позволяет считывать с бортового устройства все имеющиеся данные, однако записывать данные в бортовое устройство не позволяет.

Выбор вида диагностического сеанса рассмотрен в разделе 5.

Настоящий **подраздел** добавления следует рассматривать как относящийся к обоим поколениям БУ и карточек мастерской в соответствии с требованиями к эксплуатационной совместимости, изложенными в настоящих правилах.

CPR_001 Сеанс «ECUProgrammingSession» позволяет вводить данные в бортовое устройство. При этом для ввода калибровочных данных бортовое устройство должно быть переведено в режим CALIBRATION.

Передача данных по К-линии описана в разделе 0

«6. “Функции передачи данных. Форматы передаваемых данных подробно описаны в разделе 0”

8. Функция RoutineControl (корректировка времени)

8.1 Описание сообщения

CPR_065a Функция RoutineControlService (TimeAdjustment) дает возможность инициировать установку часов БУ по времени, выдаваемому приемником GNSS.

Для выполнения функции RoutineControlService (TimeAdjustment) БУ должно находиться в режиме КАЛИБРОВКИ.

Предварительное условие: необходимо убедиться в том, что БУ может принимать аутентифицированные сообщения о местоположении, выдаваемые приемником ГНСС.

Пока идет корректировка времени, БУ должно реагировать на запрос RoutineControl (штатный контроль) — подфункцию requestRoutineResults с использованием параметра routineInfo = 0x78.

Примечание: Корректировка времени может занять некоторое время. Диагностический тестер запрашивает статус корректировки времени с помощью подфункции requestRoutineResults.

8.2 Формат сообщения

CPR_065b Форматы сообщений в случае функции RoutineControlService (TimeAdjustment) и его примитивов подробно описаны в следующих таблицах.

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#4	Дополнительный байт длины	xx	LEN
#5	Идентификатор функции запроса RoutineControl	31	RC
#6	routineControlType = [startRoutine]	01	RCTP_STR
#7 и #8	routineIdentifier = [TimeAdjustment]	0100	RI_TA
#9	Контрольная сумма	00-FF	CS

Таблица 37а — RoutineControl, штатная подпрограмма (корректировка времени), сообщение с запросом на штатную подфункцию startRoutine

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	xx	LEN
#5	Идентификатор функции положительного ответа на запрос RoutineControl:	71	RCPR
#6	routineControlType = [startRoutine]	01	RCTP_STR
#7 и #8	routineIdentifier = [TimeAdjustment]	0100	RI_TA
#9	Контрольная сумма	00-FF	CS

Таблица 37б — RoutineControl, штатная подпрограмма (корректировка времени), подфункция startRoutine, сообщение с положительным ответом

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	xx	LEN
#5	Идентификатор функции запроса RoutineControl	31	RC
#6	routineControlType = [startRoutine]	03	RCTP_RRR
#7 и #8	routineIdentifier = [TimeAdjustment]	0100	RI_TA
#9	Контрольная сумма	00-FF	CS

Таблица 37с — RoutineControl, штатная подпрограмма (корректировка времени), сообщение с запросом на подфункцию requestRoutineResults

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	xx	LEN
#5	Идентификатор функции положительного ответа на запрос RoutineControl:	71	RCPR
#6	routineControlType = [requestRoutineResults]	03	RCTP_RRR
#7 и #8	routineIdentifier = [TimeAdjustment]	0100	RI_TA
#9	routineInfo (см. таблицу 37f)	XX	RINF_TA

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#10	routineStatusRecord[] = routineStatus#1 (см. таблицу 37g)	XX	RS_TA
#11	Контрольная сумма	00-FF	CS

Таблица 37d — RoutineControl, штатная подпрограмма (корректировка времени), подфункция requestRoutineresults, сообщение с положительным ответом

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции negativeResponse	7F	NR
#6	Идентификатор запроса inputOutputControlByIdentifier	31	RC
#7	responseCode=[подфункция не поддерживается неправильная длина сообщения или недействительный формат неправильные условия {00}]	12 13 22 31	SFNS IMLOIF CNC ROOR
#8	Контрольная сумма	00-FF	CS

Таблица 37e — RoutineControl, штатная подпрограмма (корректировка времени), сообщение с отрицательным ответом

routineInfo	Шестнадцатеричное значение	Описание
NormalExitWithResultAvailable	61	Штатная процедура была выполнена полностью; доступны дополнительные результаты штатной процедуры
RoutineExecutionOngoing	78	Запрошенная штатная процедура еще выполняется

Таблица 37f — RoutineControl, штатная подпрограмма (корректировка времени), обычная информация

Шестнадцатеричное значение	Результат теста	Описание
01	положительный	Корректировка времени успешно завершена
02..0F		RFU
10	отрицательный	Нет приема сигнала GNSS
11..7F		RFU
80..FF		Проблема на уровне изготовителя

Таблица 37g — RoutineControl, штатная подпрограмма (корректировка времени), обычная информация

9. форматы записей “dataRecords”.

CPR_002 Сеанс «ECUAdjustmentSession» позволяет выбрать режим ввода/вывода сигнальной линии калибровочного ввода/вывода через интерфейс К-линии. Управление сигнальной линией калибровочного входа/выхода

описано в разделе 7 «Настройка проверочных импульсов — контрольный функциональный блок регулировки входного/выходного сигнала».

CPR_003 Адрес тестера везде в настоящем документе обозначен как 'tt'. Хотя для тестеров могут существовать общепринятые адреса, БУ должно быть способно правильно поддерживать связь с тестером по любому адресу. Физический адрес БУ — 0xEE.

2. Термины, определения и справочные материалы

Протоколы, сообщения и коды ошибок в основном соответствуют нынешней версии проекта стандарта ISO 14229-1 (Транспорт дорожный. Системы диагностического контроля. Часть 1. Диагностические функции. Версия 6 от 22 февраля 2001 года).

Для идентификаторов функций, запросов функций и ответов на них, а также для стандартных параметров используются шестнадцатеричные величины и байтовое кодирование.

Под термином «тестер» понимается аппаратура, используемая для ввода программных/калибровочных данных в БУ.

Под терминами «клиент» и «сервер» понимаются, соответственно, тестер и БУ.

Под термином «ECU», означающим «электронный контрольный блок», понимается БУ.

Справочные материалы:

ISO 14230-2: Транспортные средства дорожные. Диагностические системы. Ключевой протокол 2000. Часть 2: уровень канала передачи данных. 1-е издание: 1999 год.

~~Транспортные средства. Диагностика.~~

3. Обзор функций

3.1 Поддерживаемые функции

В таблице ниже представлен обзорный перечень функций, которые должны быть предусмотрены в тахографе и определения которых приводятся в настоящем документе.

CPR_004 В таблице показаны функции, доступные после начала диагностического сеанса.

- В **1-м столбце** приведен перечень имеющихся функций.
- Во **2-м столбце** перечислены номера пунктов данного **подраздела**, содержащих развернутые определения соответствующих функций.
- В **3-м столбце** указаны значения идентификаторов соответствующих функций, используемые в запросах.
- В **4-м столбце** указаны функции сеанса «**StandardDiagnosticSession**» (**SD**), которые должны быть реализованы в каждом БУ.
- В **5-м столбце** указаны функции сеанса «**ECUAdjustmentSession**» (**ECUAS**), которые должны быть реализованы для обеспечения возможности управления каналом ввода-вывода калибровочного разъема на передней панели БУ.
- В **6-м столбце** указаны функции сеанса «**ECUProgrammingSession**» (**ECUPS**), которые должны быть реализованы в БУ для программирования параметров.

Название диагностической функции	Раздел №	Идент. функции д/запроса	Диагностические сеансы		
			SD	ECUAS	ECUPS
StartCommunication	0	81	■	■	■
StopCommunication	0	82	■		
TesterPresent	0	3E	■	■	■
StartDiagnosticSession	0	10	■	■	■
SecurityAccess	8	27	■	■	■
ReadDataByIdentifier	0	22	■	■	■
WriteDataByIdentifier	0	2E			■
InputOutputControlByIdentifier	0	2F		■	
RoutineControl	8	31		■	■

Таблица 1 — Сводная таблица значений идентификаторов функций

■ Символ, означающий обязательность функции для данного диагностического сеанса.

Отсутствие символа означает, что в процессе данного диагностического сеанса указанная функция невозможна.

3.2 Коды ответов

Для каждой функции предусмотрены определенные коды ответов.

4. Функции обмена данными

В ряде случаев для установления и поддержания канала обмена данными необходимы соответствующие функции. На уровне приложений они не отображаются. Описание имеющихся функций приведено в таблице ниже:

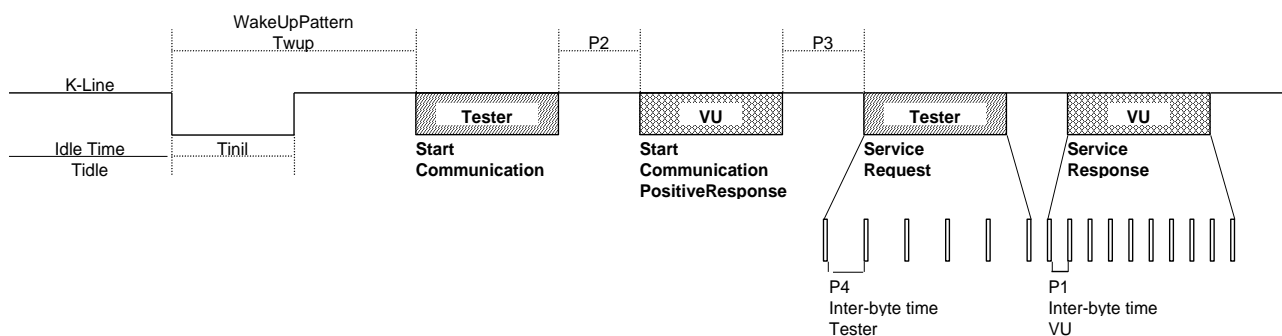
Название функции	Описание
StartCommunication	Запрос клиента на инициализацию сеанса обмена данными с сервером(ами)
StopCommunication	Запрос клиента на прекращение текущего сеанса обмена данными
TesterPresent	Сообщение клиента серверу о продолжении своего присутствия на линии

Таблица 2 — Функции обмена данными

CPR_005 Функция StartCommunication используется для инициализации обмена данными. Для выполнения любой функции необходимо начать обмен данными и обеспечить, чтобы его параметры соответствовали нужному режиму.

4.1 Функция StartCommunication

- CPR_006 По получении примитива индикации StartCommunication БУ проверяет возможность инициализации запрошенного канала обмена данными при существующих условиях. Описание условий, необходимых для инициализации канала обмена данными, приведено в документе ISO 14230-2.
- CPR_007 После этого БУ выполняет все действия, необходимые для инициализации канала обмена данными, и возвращает примитив ответа StartCommunication с выбранными параметрами положительного ответа.
- CPR_008 Если на БУ, которое уже инициализовано (и уже находится в процессе того или иного диагностического сеанса), поступает новый запрос StartCommunication (например, при восстановлении работы тестера после сбоя), то этот запрос принимается и производится повторная инициализация БУ.
- CPR_009 Если по каким-либо причинам инициализация канала обмена данными невозможна, то БУ продолжает функционировать в том же режиме, в котором оно находилось непосредственно перед попыткой инициализации канала обмена данными.
- CPR_010 Сообщение с запросом StartCommunication должно иметь физическую адресацию.
- CPR_011 **Инициализация БУ для выполнения соответствующих функций производится методом «ускоренной инициализации»:**
- любой операции предшествует определенный период бездействия шины;
 - затем тестер высылает шаблон инициализации;
 - ответ БУ содержит всю информацию, необходимую для установления канала обмена данными.
- CPR_012 По завершении инициализации:
- значения всех параметров обмена данными задаются такими, как определено в таблице 4 в соответствии с байтами ключей;
 - БУ ожидает первый запрос от тестера;
 - БУ находится в режиме диагностики, выбираемом по умолчанию, т. е. в режиме StandardDiagnosticSession;
 - канал ввода-вывода калибровочных данных находится в состоянии, выбираемом по умолчанию, т. е. не активирован.
- CPR_014 Скорость передачи данных по К-линии составляет 10 400 бод.
- CPR_016 Для вызова ускоренной инициализации тестер передает по К-линии шаблон запуска (Wup). Этот шаблон начинает действовать после периода бездействия на К-линии, с периода низкого уровня тактового сигнала, равного T_{inil} . Тестер высылает первый бит сообщения StartCommunicationService по истечении периода T_{wup} с момента первого спада тактового сигнала.



CPR_017 Значения временных параметров ускоренной инициализации и обмена данными в целом приведены в нижеследующих таблицах. Время бездействия может быть различным:

- от включения питания до первой передачи данных: $T_{idle} = 300$ мс;
- после завершения функции StopCommunication: $T_{idle} = P3$ мин;
- после прекращения обмена данными из-за превышения времени ожидания $P3$ max: $T_{idle} = 0$.

Параметр	Минимальное значение	Максимальное значение
T_{inil}	25 1 мс	24 мс
T_{wup}	50 1 мс	49 мс

Таблица 3 — Временные параметры ускоренной инициализации

Временные параметры	Нижние предельные значения [мс]	Верхние предельные значения [мс]	
Параметр	Определение параметров	мин.	макс.
P1	Межбайтовый интервал для ответа БУ	0	20
P2	Интервал между запросом тестера и ответом БУ или между двумя ответами БУ	25	250
P3	Интервал между окончанием ответов БУ и началом нового запроса тестера	55	5 000
P4	Межбайтовый интервал для запроса тестера	5	20

Таблица 4 — Временные параметры обмена данными

CPR_018 Формат сообщений для ускоренной инициализации подробно указан в нижеследующих таблицах (ПРИМЕЧАНИЕ: Hex — шестнадцатеричный).

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	81	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Идентификатор функции запроса StartCommunication	81	SCR
#5	Контрольная сумма	00-FF	CS

Таблица 5 — Сообщение запроса StartCommunication

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции положительного ответа на запрос StartCommunication	€1	SCRPR
#6	Ключевой байт 1	EA	KB1
#7	Ключевой байт 2	8F	KB2
#8	Контрольная сумма	00-FF	CS

Таблица 6 — Сообщение положительного ответа на запрос StartCommunication

CPR_019 На сообщение запроса StartCommunication отрицательного ответа нет; если нет положительного ответного сообщения, БУ не инициализируется, ничего не передается, и БУ остается в режиме нормальной эксплуатации.

4.2 Функция StopCommunication

4.2.1 Описание сообщения

Эта функция на уровне обмена данными предназначена для прекращения сеанса обмена.

CPR_020 По получении примитива индикации StartCommunication БУ проверяет возможность инициализации запрошенного канала обмена данными с учетом существующих условий. Если это возможно, БУ выполняет все действия, необходимые для прекращения сеанса обмена данными.

CPR_021 Если обмен данными может быть прекращен, то перед прекращением обмена данными БУ возвращает примитив ответа StopCommunication с выбранными параметрами положительного ответа.

CPR_022 Если по каким-либо причинам прекращение обмена данными невозможно, то БУ возвращает примитив ответа StopCommunication с выбранными параметрами отрицательного ответа.

CPR_023 Если БУ фиксирует истечение периода ожидания $P3max$, то обмен данными прекращается без направления какого-либо примитива ответа.

4.2.2 Формат сообщения

CPR_024 Форматы сообщений для примитивов StopCommunication подробно указаны в нижеследующих таблицах.

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	01	LEN
#5	Идентификатор функции запроса Stop Communication	82	SPR
#6	Контрольная сумма	00-FF	CS

Таблица 7 — Сообщение запроса StopCommunication

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	01	LEN
#5	Идентификатор функции положительного ответа на запрос StopCommunication	C2	SPRPR
#6	Контрольная сумма	00-FF	CS

Таблица 8 — Сообщение положительного ответа на запрос StopCommunication

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса Stop Communication	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Контрольная сумма	00-FF	CS

Таблица 9 — Сообщение отрицательного ответа на запрос StopCommunication

4.2.3 Определение параметров

Данная функция не требует определения каких-либо параметров.

4.3 Функция TesterPresent

4.3.1 Описание сообщения

Функция TesterPresent используется тестером для оповещения сервера о продолжении присутствия на линии с целью предотвратить автоматическое возвращение сервера в обычный режим работы и возможный обрыв связи. Периодически выслаемый запрос данной функции позволяет поддерживать непрерывный сеанс диагностики/обмена данными, так как счетчик времени P3 обнуляется при каждом очередном поступлении этого запроса.

4.3.2 Формат сообщения

CPR_079 Форматы сообщений для примитивов TesterPresent подробно указаны в нижеследующих таблицах.

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	02	LEN

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#5	Ид функции запроса TesterPresent	3E	TP
#6	Подфункция = responseRequired = [да нет]	01 RESPREQ_Y 02 RESPREQ_NO	
#7	Контрольная сумма	00-FF	CS

Таблица 10 — Сообщение запроса TesterPresent

CPR_80 Если параметр responseRequired установлен на ответ «да», то сервер возвращает положительный ответ, показанный ниже. Если параметр установлен на ответ «нет», то на данный запрос сервер не отвечает.

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	01	LEN
#5	Идентификатор функции положительного ответа на запрос TesterPresent	7E	TPPR
#6	Контрольная сумма	00-FF	CS

Таблица 11 — Сообщение положительного ответа на запрос TesterPresent

CPR_81 В данной функции предусмотрены следующие коды отрицательного ответа:

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса TesterPresent	3E	TP
#7	ResponseCode = [SubFunctionNotSupported-InvalidFormatincorrectMessageLength] (подфункция не поддерживается — неправильный формат — неверная длина сообщения)	12 RC_SFNS_IF 13 RC_IML	
#8	Контрольная сумма	00-FF	CS

Таблица 12 — Сообщение отрицательного ответа на запрос TesterPresent

5. Функции управления

Описание имеющихся функций приведено в таблице ниже:

Название функции	Описание
StartDiagnosticSession	Запрос клиента на инициализацию сеанса диагностики БУ
SecurityAccess	Клиент запрашивает доступ к функциям, предназначенным для уполномоченных пользователей

Таблица 13 — Функции управления

5.1 Функция StartDiagnosticSession

5.1.1 Описание сообщения

CPR_025 Функция StartDiagnosticSession используется для инициализации различных диагностических сеансов на сервере. В ходе диагностического сеанса предоставляется доступ к конкретному набору функций, указанному в **таблице 17**. Некоторые функции, возможные в ходе таких сеансов, специфичны для транспортных средств конкретных изготовителей и в настоящем документе не рассматриваются. Правила технической реализации соответствующих систем должны отвечать следующим требованиям:

- БУ постоянно поддерживает только один текущий диагностический сеанс.
- При подаче питания БУ во всех случаях начинает стандартный сеанс диагностики (StandardDiagnosticSession). Если после этого не будет начат другой диагностический сеанс, то StandardDiagnosticSession продолжается до тех пор, пока питание БУ не будет отключено.
- Если тестером запрашивается уже запущенный диагностический сеанс, БУ возвращает положительный ответ.
- Если тестером запрашивается новый диагностический сеанс, то БУ сначала высылает положительный ответ на запрос StartDiagnosticSession, а затем запускает новый сеанс. Если БУ не может начать новый диагностический сеанс в соответствии с запросом, то оно возвращает отрицательный ответ на запрос StartDiagnosticSession, а текущий сеанс продолжается.

CPR_026 Диагностический сеанс может быть начат только в том случае, если между клиентом и БУ установлен канал обмена данными.

CPR_027 Временные параметры, определенные в **таблице 4**, начинают применяться после успешного выполнения запроса StartDiagnosticSession, в котором параметр diagnosticSession был установлен на «StandardDiagnosticSession», если до этого выполнялся другой диагностический сеанс.

5.1.2 Формат сообщения

CPR_028 Формат сообщений для примитивов StartDiagnosticSession подробно указан в нижеследующих таблицах.

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	02	LEN
#5	Идентификатор функции запроса StartDiagnosticSession	10	STDS
#6	diagnosticSession (диагностический сеанс) = [одно значение из таблицы 17]	xx	DS_...
#7	Контрольная сумма	00-FF	CS

Таблица 14 — Сообщение запроса StartDiagnosticSession

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	02	LEN
#5	Идентификатор функции положительного ответа на запрос StartDiagnosticSession	50	STDSPR
#6	diagnosticSession = [то же значение, что и в байте #6 таблицы 14].	xx	DS_...
#7	Контрольная сумма	00-FF	CS

Таблица 15 — Сообщение положительного ответа на запрос StartDiagnosticSession

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса StartDiagnosticSession	10	STDS
#7	ResponseCode= [subFunctionNotSupported ^a (подфункция не поддерживается)	12	RC_SFNS
	incorrectMessageLength ^b (неверная длина сообщения)	13	RC_CNC
	conditionsNotCorrect ^c (недопустимые условия)	22	
#8	Контрольная сумма	00-FF	CS

Таблица 16 — Сообщение отрицательного ответа на запрос StartDiagnosticSession

^a Значение, заданное в байте #6 запроса, не поддерживается и поэтому в таблице 17 указано.

^b Длина сообщения не соответствует ожидаемой.

^c Не соблюдены критерии выполнения запроса StartDiagnosticSession.

5.1.3 Определение параметров

CPR_029 Параметр *diagnosticSession* (*DS_*) используется функцией StartDiagnosticSession для выбора того или иного режима работы сервера(ов). В настоящем документе указаны его значения для следующих видов диагностических сеансов:

Шестнадцатеричное значение	Описание	Мнемокод
81	StandardDiagnosticSession В ходе данного диагностического сеанса могут использоваться все функции, указанные в столбце 4 («SD») таблицы 1 . Эти функции позволяют считывать данные, хранящиеся на сервере (БУ). Данный диагностический сеанс активируется после успешного завершения инициализации канала связи между клиентом (тестер) and сервером (БУ). Этот сеанс может быть впоследствии заменен другими диагностическими сеансами, о которых говорится в настоящем разделе.	SD

Шестнадцатеричное значение	Описание	Мнемокод
85	ECUProgrammingSession (сеанс программирования контрольной аппаратуры) В ходе данного диагностического сеанса могут использоваться все функции, указанные в столбце 6 («ECUPS») таблицы 1. Эти функции обеспечивают программирование памяти сервера (БУ). Данный диагностический сеанс может быть впоследствии заменен другими диагностическими сеансами, о которых говорится в настоящем разделе.	ECUPS
87	ECUAdjustmentSession (сеанс настройки контрольной аппаратуры) В ходе данного диагностического сеанса могут использоваться все функции, указанные в столбце 5 («ECUAS») таблицы 1. Эти функции обеспечивают регулировку параметров входного/выходного сигнала сервера (БУ). Данный диагностический сеанс может быть впоследствии заменен другими диагностическими сеансами, о которых говорится в настоящем разделе.	ECUAS

Таблица 17 — Определение значений параметра `diagnosticSession`

5.2 Функция SecurityAccess

Запись калибровочных данных возможна лишь при условии, что БУ находится в режиме CALIBRATION. Для получения доступа к режиму CALIBRATION необходимо, помимо ввода в БУ действительной карточки мастерской, ввести в бортовое устройство соответствующий ПИН-код.

Когда БУ находится в режиме CALIBRATION или CONTROL, также возможен и доступ к линии ввода/вывода калибровки.

Функция SecurityAccess позволяет ввести ПИН-код и запросить у тестера информацию о том, находится ли БУ в режиме CALIBRATION.

Допустимы и другие альтернативные методы введения ПИН-кода.

5.2.1 Описание сообщения

Функция SecurityAccess предусматривает направление сообщения SecurityAccess «requestSeed» и, в случае необходимости, запрос «sendKey» (передача ключа). Функция SecurityAccess выполняется в обязательном порядке после функции StartDiagnosticSession.

CPR_033 Сообщение SecurityAccess «requestSeed» используется тестером для проверки готовности бортового устройства к приему PIN-кода.

CPR_034 Если бортовое устройство уже находится в режиме CALIBRATION, то в ответ на этот запрос оно возвращает — с использованием функции положительного ответа SecurityAccess — стартовое значение 0x0000.

CPR_035 Если бортовое устройство готово принять PIN-код для проверки с помощью карточки мастерской, то оно возвращает — с использованием функции положительного ответа SecurityAccess — стартовое значение, превышающее 0x0000.

CPR_036 Если бортовое устройство не готово принять от тестера ПИН-код, поскольку введенная карточка мастерской недействительна или не была введена в считывающее устройство, либо по той причине, что бортовое устройство ожидает введения ПИН-кода другим способом, оно выдает отрицательный ответ с кодом `conditionsNotCorrectOrRequestSequenceError` (недопустимые условия или неверная последовательность запросов).

CPR_037 В таких случаях тестер передает PIN-код на бортовое устройство с помощью сообщения SecurityAccess «sendKey». Для обеспечения

достаточного времени, необходимого для завершения процесса аутентификации карточки, БУ использует код отрицательного ответа requestCorrectlyReceived-ResponsePending, позволяющий продлить период ожидания ответа. Этот период, однако, не может превышать 5 минут. Как только выполнение запрошенной функции завершается, БУ высылает положительный или отрицательный ответ с кодом, отличным от данного. Код отрицательного ответа requestCorrectlyReceived-ResponsePending может высылаться бортовым устройством неоднократно, вплоть до завершения запрошенной функции и направления заключительного ответного сообщения.

CPR_038 Бортовое устройство реагирует на данный запрос с помощью функции положительного ответа SecurityAccess лишь в том случае, если оно находится в режиме CALIBRATION.

CPR_039 Ниже перечисляются случаи, когда бортовое устройство возвращает на данный запрос отрицательный ответ, и соответствующий код ответа:

- subFunctionNot supported: неправильный формат параметра подфункции (accessType);
- conditionsNotCorrectOrRequestSequenceError: бортовое устройство не готово к введению ПИН-кода;
- invalidKey: неверный ПИН-код; допустимое количество попыток подтверждения ПИН-кода не превышено;
- exceededNumberOfAttempts: неверный PIN-код; допустимое количество попыток подтверждения PIN-кода превышено;
- generalReject: общий отказ: ПИН-код верен, но взаимную аутентификацию устройства и карточки мастерской произвести не удалось.

5.2.2 Формат сообщения — SecurityAccess — requestSeed

CPR_040 Форматы сообщений для примитивов SecurityAccess «requestSeed» подробно указаны в нижеследующих таблицах.

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	02	LEN
#5	Идентификатор функции запроса SecurityAccess	27	SA
#6	accessType — requestSeed	7D	AT_RSD
#7	Контрольная сумма	00-FF	CS

Таблица 18 — Запрос SecurityAccess — requestSeed

Байт #	Имя параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	04	LEN
#5	Идентификатор функции положительного ответа на запрос SecurityAccess	67	SAPR
#6	accessType — requestSeed	7D	AT_RSD

Байт #	Имя параметра	Шестнадцатеричное значение	Мнемокод
#7	Стартовое значение — верхний байт	00-FF	SEEDH
#8	Стартовое значение — нижний байт	00-FF	SEEDL
#9	Контрольная сумма	00-FF	CS

Таблица 19 — Положительный ответ на запрос SecurityAccess — requestSeed

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Формат байта — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса SecurityAccess	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength (неверная длина сообщения)]	22	RC_CNC
		13	RC_IML
#8	Контрольная сумма	00-FF	CS

Таблица 20 — Отрицательный ответ на запрос SecurityAccess

5.2.3 Формат сообщения — SecurityAccess - sendKey

CPR_041 Форматы сообщений для примитивов SecurityAccess «requestSeed» подробно указаны в нижеследующих таблицах.

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	m+2	LEN
#5	Идентификатор функции запроса SecurityAccess	27	SA
#6	accessType (тип доступа) — sendKey	7E	AT_SK
от #7 до #m+6	Ключ # 1 (верхний)	xx	KEY
	
	Ключ #m (нижний, m должно составлять не менее 4 и не более 8)	xx	
#m+7	Контрольная сумма	00-FF	CS

Таблица 21 –Запрос SecurityAccess — sendKey

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#4	Дополнительный байт длины	02	LEN
#5	Идентификатор функции положительного ответа на запрос SecurityAccess	67	SAPR
#6	accessType — sendKey	7E	AT_SK
#7	Контрольная сумма	00-FF	CS

Таблица 22 — Положительный ответ на запрос SecurityAccess — sendKey

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса SecurityAccess	27	SA
#7	ResponseCode (код ответа) = [generalReject	10	RC_GR
	subFunctionNotSupported	12	RC_SFNS
	(подфункция не поддерживается)		
	incorrectMessageLength	13	RC_IML
	(неверная длина сообщения)		
	conditionsNotCorrectOrRequest	22	RC_CNC
	(недопустимые условия — ошибка в запросе)		
	SequenceError		RC_IK
	(ошибка в последовательности)		
	invalidKey	35	RC_ENA
	(недействительный ключ)		
	exceededNumberOfAttempts	36	RC_RCR_RP
	(превышение числа попыток)		
	requestCorrectlyReceived — ResponsePending	78	
	(запрос получен правильно — ожидается ответ)]		
#8	Контрольная сумма	00-FF	CS

Таблица 23 — Отрицательный ответ на запрос SecurityAccess

6. Функции передачи данных

Описание имеющихся функций приведено в таблице ниже:

Название функции	Описание
ReadDataByIdentifier	Клиент запрашивает передачу текущего значения записи с доступом по идентификатору recordDataIdentifier
Функция WriteDataByIdentifier	Клиент запрашивает возможность сохранения записи, доступ к которой был получен по идентификатору recordDataIdentifier

Таблица 24 — Функции передачи данных

6.1 Функция ReadDataByIdentifier

6.1.1 Описание сообщения

CPR_050 Функция ReadDataByIdentifier используется клиентом с целью запроса у сервера значения записей данных. Данные опознаются по идентификатору recordDataIdentifier. Изготовитель БУ должен обеспечить, чтобы эта функция выполнялась с соблюдением заданных условий работы сервера.

6.1.2 Формат сообщения

CPR_051 Форматы сообщений для примитивов ReadDataByIdentifier подробно указаны в нижеследующих таблицах.

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции запроса ReadDataByIdentifier	22	RDBI
#6 — #7	recordDataIdentifier = [значение из таблицы 28]	xxxx	RDI_...
#8	Контрольная сумма	00-FF	CS

Таблица 25 — Сообщение запроса ReadDataByIdentifier

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	m+3	LEN
#5	Идентификатор функции положительного ответа на запрос ReadDataByIdentifier	62	RDBIPR
#6 и #7	recordDataIdentifier = [то же значение, что и в случае байтов #6 и #7 из таблицы 25]	xxxx	RDI_...
#8 — #m+7	dataRecord[] = [данные#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Контрольная сумма	00-FF	CS

Таблица 26 — Сообщение положительного ответа ReadDataByIdentifier

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	ReadDataByIdentifier Идентификатор функции запроса ReadDataByIdentifier	22	RDBI
#7	ResponseCode (код ответа) = [requestOutOfRange (нештатный запрос) incorrectMessageLength (неверная длина сообщения) conditionsNotCorrect (недопустимые условия)	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Контрольная сумма	00-FF	CS

Таблица 27 — Сообщение отрицательного ответа на запрос ReadDataByIdentifier

6.1.3 Определение параметров

CPR_052 Параметр *recordDataIdentifier (RDI_)* в запросе ReadDataByIdentifier служит для идентификации записи данных.

CPR_053 Значения параметра recordDataIdentifier, определенные в настоящем документе, указаны в таблице ниже.

Таблица RecordDataIdentifier состоит из ~~четырёх~~ **пяти** колонок и нескольких строк.

- В **1-м столбце (Шестн. значение)** приведено шестнадцатеричное значение, закрепленное за идентификатором recordDataIdentifier, который указан в 3-м столбце.
- Во **2-м столбце (Элемент данных)** указывается элемент данных **подраздела 1 приложения добавления**, на котором основан идентификатор записи recordDataIdentifier (иногда требуется перекодировка).
- В **3-м столбце (Описание)** указано наименование соответствующего идентификатора записи recordDataIdentifier.
- В **4-м столбце (Права доступа)** указываются права доступа к данному идентификатору записи (RecordDataIdentifier).
- В **5-м столбце (Мнемокод)** указан мнемокод данного идентификатора записи recordDataIdentifier.

Шестнадцатеричное значение	Элемент данных	Идентификатор recordDataIdentifier (формат см. в разделе 8.2)	Права доступа (чтение/запись)	Мнемокод
F90B	CurrentDateTime (текущая дата и время)	TimeDate	R/W	RDI_TD
F912	HighResOdometer (показания счетчика пробега с высоким разрешением)	HighResolutionTotalVehicleDistance	R/W	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment (постоянная K записывающей аппаратуры)	Kfactor	R/W	RDI_KF
F91C	(окружность шины L)	LfactorTyreCircumference	R/W	RDI_LF
F91D	W-VehicleCharacteristicConstant (характеристическая постоянная W транспортного средства)	WvehicleCharacteristicFactor	R/W	RDI_WVCF
F921	Размер шины	TyreSize	R/W	RDI_TS
F922	Дата следующей калибровки	NextCalibrationDate	R/W	RDI_NCD
F92C	Разрешенная скорость	SpeedAuthorised	R/W	RDI_SA

<i>Шестнадцатеричное значение</i>	<i>Элемент данных</i>	<i>Идентификатор recordDataIdentifier (формат см. в разделе 8.2)</i>	<i>Права доступа (чтение/запись)</i>	<i>Мнемокод</i>
F97D	Страна регистрации транспортного средства	RegisteringMemberState	R/W	RDI_RMS
F97E	Номер регистрации транспортного средства	VehicleRegistrationNumber	R/W	RDI_VRN
F190	Идентификационный номер транспортного средства	VIN	R/W	RDI_VIN
F9D0	Серийный номер датчика	MotionSensorSerialNumber	R	RDI_SSN
F9D1	Серийный номер модуля удаленной связи	RemoteCommunicationFacilitySerialNumber	R	RDI_RCSN
F9D2	Серийный номер датчика HCCr	ExternalGNSSFacilitySerialNumber	R	RDI_GSSN
F9D3	Данные пломбирования БУ	SmartTachographSealsSerialNumber	R/W	RDI_SDV
F9D4	Серийный номер БУ	VuSerialNumber	R	RDI_VSN
F9D5	Тип груза по умолчанию	ByDefaultLoadType	R/W	RDI_BDLT
F9D6	Отмена карточек тахографа первого поколения	TachographCardsGen1Suppression	R/W	RDI_TCG1S
F9D7	Местоположение транспортного средства	VehiclePosition	R	RDI_VP
F9D8	Страна, в которой выполнена последняя калибровка	CalibrationCountry	R	RDI_CC

Таблица 28 — Определение значений recordDataIdentifier

CPR_054 Параметр dataRecord (DREC_) используется в положительном ответе на запрос ReadDataByIdentifier для сообщения клиенту (тестеру) значения записи данных, опознаваемой по идентификатору recordDataIdentifier. Форматы данных указаны в разделе 8. Для удобства пользователя могут быть предусмотрены и другие, не определяемые в настоящем документе виды записей данных, включая специфичные для той или иной модели БУ входные, внутренние и выходные данные.

6.2 Функция WriteDataByIdentifier

6.2.1 Описание сообщения

CPR_056 Функция WriteDataByIdentifier используется клиентом в целях сохранения значений данных на сервере. Данные опознаются по идентификатору recordDataIdentifier. Изготовитель БУ должен обеспечить, чтобы эта функция выполнялась с соблюдением заданных условий работы сервера. Для обновления значений параметров, перечисленных в таблице 28, БУ должно быть переведено в режим CALIBRATION.

6.2.2 Формат сообщения

CPR_057 Форматы сообщений для примитивов ReadDataByIdentifier подробно указаны в нижеследующих таблицах.

<i>Байт #</i>	<i>Название параметра</i>	<i>Шестнадцатеричное значение</i>	<i>Мнемокод</i>
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	m+3	LEN
#5	Идентификатор функции запроса WriteDataByIdentifier	2E	WDBI
#6 — #7	recordDataIdentifier = [значение из таблицы 28]	xxxx	RDI_...
#8 — m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Контрольная сумма	00-FF	CS

Таблица 29 — Сообщение запроса WriteDataByIdentifier

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции положительного ответа WriteDataByIdentifier	6E	WDBIPR
#6 — #7	recordDataIdentifier = [то же значение, что и в случае байтов #6 и #7, таблица 29]	xxxx	RDI_...
#8	Контрольная сумма	00-FF	CS

Таблица 30 — Сообщение положительного ответа на запрос ReadDataByIdentifier

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса WriteDataByIdentifier	2E	WDBI
#7	ResponseCode = [нештатный запрос неверная длина сообщения недопустимые условия]	31 13 22	RC_R0OR RC_IML RC_CNC
#8	Контрольная сумма	00-FF	CS

Таблица 31 — Идентификатор функции отрицательного ответа на запрос WriteDataByIdentifier

6.2.3 Определение параметров

Определение *recordDataIdentifier* (*RDI_*) приводится в таблице 28.

Параметр *dataRecord* (*DREC_*) используется в положительном ответе на запрос *WriteDataByIdentifier* в целях сообщения серверу (БУ) значений записи данных, опознаваемой по идентификатору *recordDataIdentifier*. Форматы данных указаны в разделе 8.

7. Настройка проверочных импульсов — контрольный функциональный блок регулировки входного/выходного сигнала

Описание имеющихся функций приведено в таблице ниже:

Название функции	Описание
<i>InputOutputControlByIdentifier</i>	Клиент запрашивает у сервера управление соответствующим входом/выходом

Таблица 32 — Функциональный блок регулировки входного/выходного сигнала

7.1 Функция *InputOutputControlByIdentifier*

7.1.1 Описание сообщения

Подключение соответствующего тестера к разъему на передней панели позволяет производить настройку или мониторинг проверочных импульсов.

CPR_058 Конфигурация калибровочного канала ввода/вывода может быть изменена с помощью команды, передаваемой по К-линии с использованием функции *InputOutputControlByIdentifier*, позволяющей задавать этому каналу необходимый режим ввода или вывода данных. Предусмотрены следующие режимы:

- отключение;
- режим *speedSignalInput*, при котором по каналу ввода/вывода калибровочных данных вводится тест-сигнал скорости, заменяющий собой сигнал скорости от датчика движения (данная функция недоступна в режиме CONTROL);
- режим *realTimeSpeedSignalOutputSensor*, при котором по каналу ввода/вывода калибровочных данных выводится сигнал скорости, поступающий от датчика движения;
- режим *RTCOutput*, при котором по каналу ввода/вывода калибровочных данных выводится сигнал часов UTC (данная функция недоступна в режиме CONTROL).

CPR_059 CPR_059 Для изменения конфигурации канала на бортовом устройстве должен быть инициирован сеанс настройки, а само устройство должно находиться в режиме CALIBRATION или CONTROL. Если БУ находится в режиме CALIBRATION, можно выбирать из четырех состояний канала (*disabled*, *speedSignalInput*, *realTimeSpeedSignalOutputSensor*, *RTCOutput*). Если БУ находится в режиме CONTROL, можно выбирать только из двух состояний канала (*disabled*, *realTimeSpeedSignalOutputSensor*). При завершении сеанса настройки или при выходе из режима CALIBRATION или CONTROL бортовое устройство должно обеспечивать возвращение канала ввода/вывода калибровочных данных в состояние «disabled» (в котором он находится по умолчанию).

CPR_060 В случае поступления импульсов скорости по входному каналу БУ, предназначенному для приема сигнала скорости в реальном масштабе времени, когда канал ввода-вывода калибровочных данных переключен на ввод, канал ввода-вывода калибровочных данных переключается на вывод или возвращается в отключенное состояние.

CPR_061 Последовательность операций выглядит следующим образом:

- инициализация обмена данными с помощью функции StartCommunication;
- запуск сеанса настройки с помощью функции StartDiagnosticSession и переход в режим CALIBRATION или CONTROL (очередность выполнения этих двух операций значения не имеет);
- изменение состояния канала вывода данных с помощью функции InputOutputControlByIdentifier.

7.1.2 Формат сообщения

CPR_062 Форматы сообщений для примитивов InputOutputControlByIdentifier подробно указаны в нижеследующих таблицах.

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	xx	LEN
#5	Идентификатор функции запроса inputOutputControlBy Identifier	2F	IOCVI
#6 и #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 или #8 — #9	ControlOptionRecord = [inputOutputControlParameter — одно значение из таблицы 36 controlState — одно значение из таблицы 37 (см. примечание ниже)]	xx	COR_... IOCP_... CS_...
#9 или #10	Контрольная сумма	00-FF	CS

Таблица 33 — Сообщение запроса InputOutputControlByIdentifier

Примечание: Параметр controlState присутствует только в некоторых случаях (см. 7.1.3).

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	Tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	Xx	LEN
#5	Идентификатор функции положительного ответа на запрос inputOutputControlByIdentifier	6F	IOCVIPR
#6 и #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 или #8 — #9	controlStatusRecord = [inputOutputControlParameter (то же значение, что и в случае байта #8 в таблице 33) controlState (то же значение, что и в случае байта # 9 в таблице 33)] (если применимо)	xx	CSR_... IOCP_... CS_...
#9 или #10	Контрольная сумма	00-FF	CS

Таблица 34 — Сообщение положительного ответа на запрос InputOutputControl ByIdentifier

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции negativeResponse	7F	NR
#6	Идентификатор функции запроса inputOutputControlByIdentifier	2F	IOСBI
#7	responseCode=[incorrectMessageLength (неверная длина сообщения) conditionsNotCorrect (недопустимые условия) requestOutOfRange (нештатный запрос) deviceControlLimitsExceeded (вне диапазона регулировки устройства)]	13 22 31 7A	RC_IML RC_CNC RC_ROOR RC_DCLE
#8	Контрольная сумма	00-FF	CS

Таблица 35 — Сообщение отрицательного ответа на запрос **InputOutputControlByIdentifier**

7.1.3 Определение параметров

CPR_064 Параметр *inputOutputControlParameter* (IOCP_) определен в следующей таблице.

Шестнадцатеричное значение	Описание	Мнемокод
00	ReturnControlToECU Это значение указывает серверу (БУ), что тестер перестал управлять каналом ввода-вывода калибровочных данных.	RCTECU
01	ResetToDefault Это значение указывает серверу (БУ) о том, что ему следует вернуть канал ввода-вывода калибровочных данных в состояние, выбираемое по умолчанию.	RTD
03	ShortTermAdjustment Это значение указывает серверу (БУ) о том, что ему следует настроить канал ввода-вывода калибровочных данных по значению, указанному в параметре controlState.	STA

Таблица 36 — Определение значений **inputOutputControlParameter**

CPR_065 Параметр *controlState* (управление конфигурацией) присутствует лишь в случаях, когда параметр *inputOutputControlParameter* установлен на *ShortTermAdjustme*, и определен в нижеследующей таблице:

Режим	Шестнадцатеричное значение	Описание
Отключен	00	Канал ввода/вывода отключен (выбирается по умолчанию)
Включен	01	Канал ввода/вывода калибровочных данных работает в режиме speedSignalInput (ввод сигнала скорости)
Включен	02	Канал ввода/вывода калибровочных данных работает в режиме realTimeSpeedSignalOutputSensor (выход сигнала датчика скорости в реальном времени)
Включен	03	Канал ввода/вывода калибровочных данных работает в режиме RTCOutput (выход сигнала синхронизации в формате UTC)

Таблица 37 — Определение значений controlState

8. Функция RoutineControl (корректировка времени)

8.1 Описание сообщения

CPR_065a Функция RoutineControlService (TimeAdjustment) дает возможность произвести установку часов БУ по времени, которое выдается приемником GNSS.

В случае функции RoutineControlService (TimeAdjustment) БУ должно быть переведено в режим CALIBRATION.

Предварительное условие: Необходимо убедиться в том, что БУ может получать аутентифицированные сообщения о местоположении от приемника ГНСС.

В течение всей процедуры корректировки времени БУ отвечает на запрос RoutineControl (подфункция requestRoutineResults), выдавая штатное сообщение «routineInfo = 0x78».

Примечание: Время корректировки времени может занять некоторое время. Диагностический тестер запрашивает статус корректировки времени с помощью подфункции requestRoutineResults.

8.2 Формат сообщений

CPR_065b Форматы сообщений в случае функции RoutineControlService (TimeAdjustment) и ее примитивов подробно изложены в таблицах ниже.

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	xx	LEN
#5	RoutineControl Request Sid (Ид. запроса функции RoutineControl Request)	31	RC
#6	routineControlType = [startRoutine]	01	RCTP_STR

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#7 и #8	routineIdentifier = [TimeAdjustment]	0100	RI_TA
#9	Контрольная сумма	00-FF	CS

Таблица 37а — Функция RoutineControl, штатное сообщение с запросом (корректировка времени) подфункции «startRoutine»

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	xx	LEN
#5	RoutineControl Positive Response Sid (Ид. запроса функции RoutineControl Request)	71	RCPR
#6	routineControlType = [startRoutine]	01	RCTP_STR
#7 и #8	routineIdentifier = [TimeAdjustment]	0100	RI_TA
#9	Контрольная сумма	00-FF	CS

Таблица 37б — Функция RoutineControl, штатное сообщение с положительным ответом на запрос (корректировка времени) подфункции «startRoutine»

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	xx	LEN
#5	RoutineControl Request Sid (Ид. запроса функции RoutineControl Request)	31	RC
#6	routineControlType = [requestRoutineResults]	03	RCTP_RRR
#7 и #8	routineIdentifier = [TimeAdjustment]	0100	RI_TA
#9	Контрольная сумма	00-FF	CS

Таблица 37с — Функция RoutineControl, штатная подфункция requestRoutineResults сообщения на запрос (корректировка времени)

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	xx	LEN
#5	RoutineControl Positive Response Sid (Ид. запроса функции RoutineControl Request)	71	RCPR
#6	routineControlType = [requestRoutineResults]	03	RCTP_RRR
#7 и #8	routineIdentifier = [TimeAdjustment]	0100	RI_TA
#9	routineInfo (см. Таблицу 37f)	XX	RINF_TA

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#10	routineStatusRecord[] = routineStatus#1 (см. Таблицу 37g)	XX	RS_TA
#11	Контрольная сумма	00-FF	CS

Таблица 37d — Функция RoutineControl, штатная подфункция requestRoutine Results положительного ответа сообщения на запрос (корректировка времени)

Байт #	Название параметра	Шестнадцатеричное значение	Мнемокод
#1	Байт формата — физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	negativeResponse Service Id	7F	NR
#6	inputOutputControlByIdentifier Request SID	31	RC
#7	responseCode=[подфункция не поддерживается неверная длина сообщения или неправильный формат недопустимые условия запрос вне диапазона]	12 13 22 31	SFNS IMLOIF CNC ROOR
#8	Контрольная сумма	00-FF	CS

Таблица 37e — Функция RoutineControl, сообщение с отрицательным ответом на штатный запрос (корректировка времени)

routineInfo	Шестнадцатеричное значение	Описание
NormalExitWithResultAvailable	61	Штатная программа выполнена полностью; дополнительные штатные результаты доступны
RoutineExecutionOngoing	78	Задействованная штатная программа все еще продолжается

Таблица 37f — Функция RoutineControl, штатное сообщение routineInfo на запрос (корректировка времени)

Шестнадцатеричное значение	Результат проверки	Описание
01	Положительный	Корректировка времени произведена успешно
02..0F		RFU
10	Отрицательный	Отсутствие сигнала ГНСС
11..7F		RFU
80..FF		Относится конкретно к изготовителю

Таблица 37g — Функция RoutineControl, штатная программа (корректировка времени), обычный статус

9. Форматы записей данных

В настоящем разделе изложены:

- общие правила определения диапазона параметров, передаваемых бортовым устройством на тестер,
- форматы данных, передаваемых посредством функций передачи данных, о которых говорится в части б.

CPR_067 Все указанные здесь параметры должны поддерживаться БУ.

CPR_068 Данные, передаваемые БУ на тестер по соответствующему запросу, по своему типу представляют собой результаты замеров (т. е. текущее значение запрошенного параметра, измеренное или зафиксированное бортовым устройством).

89.1 Диапазоны передаваемых параметров

CPR_069 В **таблице 38** определены диапазоны, по которым определяется допустимость передаваемых значений параметров.

CPR_070 Используя значения диапазона «указатель ошибки», БУ может незамедлительно сообщать о том, что достоверные параметрические данные на текущий момент отсутствуют из-за той или иной ошибки контрольного устройства.

CPR_071 Значения диапазона «данные отсутствуют» могут использоваться бортовым устройством при передаче сообщений, в которых указаны отсутствующие или не поддерживаемые данным модулем параметры. С помощью значений диапазона “данные не запрашиваются” устройство может при передаче команды указать параметры, ответ по которым от устройства-адресата не требуется.

CPR_072 Если из-за отказа того или иного компонента передача достоверных данных о каком-либо параметре невозможна, то вместо этих данных используется указатель ошибки, приведенный в **таблице 38**. Если же данные, полученные в результате расчетов или измерений, являются достоверными, но выходят за пределы заданного диапазона значений запрошенного параметра, то указатель ошибки не используется. В этом случае при передаче данных используется соответствующее минимальное или максимальное значение параметра.

Таблица 38 — Диапазоны dataRecords

Наименование диапазона	1 байт (Шестн. значение)	2 байта (Шестн. значение)	4 байта (Шестн. значение)	ASCII
Допустимый сигнал	00–FA	0000–FAFF	00000000–FAFFFFFF	1–254
Указатель конкретного параметра	FB	FB00–FBFF	FB000000–FBFFFFFF	нет
Диапазон зарезервирован под разряды будущих указателей	FC–FD	FC00–FDFF	FC000000–FDFFFFFF	нет
Указатель ошибки	FE	FE00–FEFF	FE000000–FEFFFFFF	0
Данные отсутствуют или не запрашиваются	FF	FF00–FFFF	FF000000–FFFFFF	FF

CPR_073 Для параметров, представляемых с помощью кода ASCII, символ ASCII «*» резервируется в качестве ограничителя.

89.2 Форматы dataRecords

В **таблицах 39–42** ниже детально описаны форматы, используемые в связи с функциями ReadDataByIdentifier и WriteDataByIdentifier.

CPR_074 В **таблице 39** указывается длина поля данных, разрешение и рабочий диапазон для каждого параметра, определяемого соответствующим идентификатором recordDataIdentifier:

Наименование параметра	Длина поля данных (байт)	Разрешение	Диапазон
TimeDate (время — дата)	8	Подробно см. в таблице 40	
HighResolutionTotalVehicleDistance (общее расстояние пробега)	4	Прибавл.: 5 м/бит, Обратн. смещение: 0 м	От 0 до +21 055 406 км
Kfactor (коэффициент K)	2	Прибавл.: 0,001 имп./м/бит, Обратн. смещение: 0	От 0 до 64 255 имп./м
LfactorTyreCircumference (коэффициент L окружности шины)	2	Прибавл.: 0,125 10 ⁻³ м /бит, Обратн. смещение: 0	От 0 до 8.031 м
WvehicleCharacteristicFactor (характеристический коэффициент W)	2	Прибавл.: 0,001 имп./м/бит, Обратн. смещение: 0	От до 64 255 имп./м
TyreSize (размер шин)	15	ASCII	ASCII
NextCalibrationDate (дата следующей калибровки)	3	Подробно см. в таблице 41	
SpeedAuthorised (разрешенная скорость)	2	Прибавл.: 1/256 км/ч/бит, Обратн. смещение: 0	0–250 996 км/ч
RegisteringMemberState (государство — член регистрации)	3	ASCII	ASCII
VehicleRegistrationNumber (номер регистрации транспортного средства)	14	Подробно см. в таблице 42	
VIN	17	ASCII	ASCII
SealDataVu (данные, касающиеся пломб, в БУ)	55	Подробно см. в таблице 43	
ByDefaultLoadType (тип груза по умолчанию)	1	Подробно см. в таблице 44	
VuSerialNumber (серийный номер БУ)	8	Подробно см. в таблице 45	
SensorSerialNumber (серийный номер датчика)	8	Подробно см. в таблице 45	
SensorGNSSSerialNumber (серийный номер датчика ГНСС)	8	Подробно см. в таблице 45	
RemoteCommunicationModuleSerialNumber (серийный номер модуля удаленной связи)	8	Подробно см. в таблице 45	
TachographCardsGen1Suppression (Отмена карточек тахографа поколения 1)	2	Подробно см. в таблице 46	

Наименование параметра	Длина поля данных (байт)	Разрешение	Диапазон
VehiclePosition (местоположение транспортного средства)	14	Подробно см. в таблице 47	
CalibrationCountry (Страна, в которой проведена калибровка)	3	ASCII	Буквенный код государства, указанный в добавлении 1

Таблица 39 — Формат записей данных

CPR_075 В таблице 40 подробно указаны форматы различных байтов параметра TimeDate:

Байт	Параметр	Разрешение	Диапазон
1	Секунды	Прибавл.: 0,25 с/бит, обратн. смещение: 0 с	От 0 до 59,75 с
2	Минуты	Прибавл.: 1 мин./бит, обратн. смещение: 0 мин	От 0 до 59 мин
3	Часы	Прибавл.: 1 ч/бит, обратн. смещение: 0 ч	От 0 до 23 ч
4	Месяц	Прибавл.: 1 мес./бит, обратн. смещение: 0 мес.	От 1 до 12 месяцев
5	День	Прибавл.: 0,25 сут./бит, обратн. смещение: 0 суток (см. примечание к таблице 41)	От 0,25 до 31,75 суток
6	Год	Прибавл.: 1 год/бит, обратн. смещение: +1985 год (см. примечание к таблице 41)	1985–2235 годы
7	Поправка на местное время (мин)	Прибавл.: 1 мин./бит обратн. смещение: –125 мин	От –59 до +59 мин
8	Поправка на местное время (ч)		От –23 до +23 ч

Таблица 40 — Детальный формат TimeDate (значение recordDataIdentifier # F90B)

CPR_076 В таблице 41 подробно описаны форматы различных байтов параметра NextCalibrationDate:

Байт	Определение параметра	Разрешение	Диапазон
1	Месяц	Прибавл.: 1 мес./бит, обратн. смещение: 0 мес.	От 1 до 12 месяцев
2	День	Прибавл.: 0,25 сут./бит, обратн. смещение: 0 суток (см. примечание ниже)	От 0,25 до 31,75 суток
3	Год	Прибавл.: 1 год/бит, обратн. смещение: +1985 год (см. примечание ниже)	1985–2235 год

Таблица 41 — Детальный формат NextCalibrationDate (значение recordDataIdentifier # F922)

Примечание, касающееся использования параметра «День»:

1. Значение 0 в случае даты неприменимо. Значения 1, 2, 3, и 4 используются для указания первого дня месяца; 5, 6, 7, и 8 — для указания второго дня месяца, и т. д.
2. Данный параметр никак не влияет на параметр «часы» в таблице выше и не изменяет его.

Примечание, касающееся использования параметра «Год»: значение года, равное 0, соответствует 1985 году; значение, равное 1, — 1986 году, и т. д.

CPR_078 В таблице 42 подробно описаны форматы различных байтов параметра VehicleRegistrationNumber:

Байт	Определение параметра	Разрешение	Диапазон
1	Кодовая страница (согласно определению, содержащемуся в добавлении подразделе 1)	ASCII неприменимо	от 01 до 0A Регистрационный номер транспортного средства
2–14	Регистрационный номер транспортного средства (согласно определению, содержащемуся в добавлении подразделе 1)	ASCII неприменимо	ASCII Регистрационный номер транспортного средства

Таблица 42 — Детальный формат параметра VehicleRegistrationNumber (значение recordDataIdentifier # F97E)

CPR_090 В таблице 43 подробно описаны форматы различных байтов параметра SealDataVu (данные, касающиеся пломб в БУ):

Байт	Определение параметра	Разрешение	Рабочий диапазон
1–11	sealRecord1. Формат SealRecord, как он определен в подразделе 1	Неприменимо	SealRecord
12–22	sealRecord2. Формат SealRecord, как он определен в подразделе 1	Неприменимо	SealRecord
23–33	sealRecord3. Формат SealRecord, как он определен в подразделе 1	Неприменимо	SealRecord
34–44	sealRecord4. Формат SealRecord, как он определен в подразделе 1	Неприменимо	SealRecord
45–55	sealRecord5. Формат SealRecord, как он определен в подразделе 1	Неприменимо	SealRecord

Таблица 43 — Детальный формат SealDataVu (recordDataIdentifier value # F9D3)

Примечание: В том случае, если число наложенных пломб менее 5, то значение параметра EquipmentType во всех неиспользованных позициях sealRecords устанавливаются на 15, т. е. неиспользованные.

CPR_091 В таблице 44 подробно описаны форматы различных байтов параметра ByDefaultLoadType (тип груза по умолчанию):

Байт	Определение параметра	Разрешение	Рабочий диапазон
1	loadType Type ‘00’H: не определен ‘01’H: грузы ‘02’H: пассажиры	Неприменимо	‘00’H — ‘02’H

Таблица 44 — Детальный формат параметра ByDefaultLoadType (значение параметра recordDataIdentifier # F9D5)

CPR_092 В таблице 45 детально описаны форматы различных байтов параметров VuSerialNumber, SensorSerialNumber, SensorGNSSSerialNumber и RemoteCommunicationModuleSerialNumber:

Байт	Определение параметра	Разрешение	Рабочий диапазон
1	VuSerialNumber, SensorSerialNumber, SensorGNSSSerialNumber и RemoteCommunicationModuleSerialNumber: формат ExtendedSerialNumber, как он определен в подразделе 1	Неприменимо	ExtendedSerialNumber

Таблица 45 — Детальный формат параметров VuSerialNumber, SensorSerialNumber, SensorGNSSSerialNumber и RemoteCommunicationModuleSerialNumber (значения параметра recordDataIdentifier # F9D4, F9D0, F9D2, F9D1)

CPR_093 В таблице 46 детально описаны форматы различных байтов параметра TachographCardsGen1Suppression:

Байт	Определение параметра	Разрешение	Рабочий диапазон
1–2	TachographCardsGen1Suppression Формат TachographCardsGen1Suppression, как он определен в подразделе 1	Неприменимо	'0000'Н, 'A5E3'Н

Таблица 46 — Детальный формат параметра TachographCardsGen1Suppression (значение параметра recordDataIdentifier # F9D6)

CPR_094 Таблица 47 — Детальный формат различных байтов параметра VehiclePosition:

Байт	Определение параметра	Разрешение	Рабочий диапазон
1–4	Временная метка местоположения транспортного средства была определена	Неприменимо	TimeReal
5	Точность GNSS	Неприменимо	GNSSAccuracy
6–11	Местоположение транспортного средства	Неприменимо	GeoCoordinates
12	Статус аутентификации	Неприменимо	PositionAuthenticationStatus
13	Текущая страна	Неприменимо	NationNumeric
14	Текущий регион	Неприменимо	RegionNumeric

Таблица 47 — Детальный формат параметра VehiclePosition (значение параметра recordDataIdentifier # F9D7)

Примечание: После обновления местоположения транспортного средства обновление текущей страны или текущего региона может происходить с задержкой.

Подраздел 9

Официальное утверждение типа

Перечень минимальных требуемых испытаний

Содержание

	<i>Стр.</i>
1. Введение	416
2. Рабочие испытания бортового устройства	418
3. Рабочие испытания датчика движения	422
4. Функциональные испытания карточек тахографа	425
5. Испытания внешнего устройства ГНСС	433
6. Испытания внешнего устройства удаленной связи	436
7. Функциональные испытания бумаги	437
8. Испытания на эксплуатационную совместимость	439
9. Тесты OSNMA	440

1. Введение

1.1 Официальное утверждение типа

Процедура официального утверждения типа ~~регистрирующей аппаратуры~~ **контрольного устройства** (либо его компонентов) или карточек тахографа состоит из следующих основных частей:

- **сертификация защиты**, проводимая на основе Общих спецификаций, касающихся критериев безопасности, в целях подтверждения соответствия тому или иному из контрольных показателей защиты, которые должны полностью отвечать положениям **подраздела 10 Ж** настоящего ~~приложения~~ **добавления**;
- **сертификация функциональности**, проводимая уполномоченным органом ~~государства-члена Договаривающейся стороны~~ в целях подтверждения того, что испытываемое изделие соответствует требованиям настоящего ~~приложения~~ **добавления** в части выполняемых функций, точности измерений и условий эксплуатации;
- **сертификация эксплуатационной совместимости**, проводимая компетентным органом в целях подтверждения полной эксплуатационной совместимости ~~регистрирующей аппаратуры~~ **контрольного устройства** (или карточки тахографа) с необходимыми моделями карточек тахографа (или ~~регистрирующей аппаратуры~~ **контрольных устройств**) (см. главу 8 настоящего ~~приложения~~ **добавления**).

В данном ~~добавлении~~ **подразделе** содержится перечень минимальных рабочих испытаний, которые должны быть проведены соответствующим уполномоченным это органом ~~государства-члена Договаривающейся стороны~~, а также испытаний на совместимость, которые должен провести соответствующий компетентный орган. Процедуры проведения этих испытаний и их виды дополнительно не конкретизируются.

Аспекты, связанные с сертификацией защиты, в настоящем ~~добавлении~~ **подразделе** не рассматриваются. Если какие-либо из испытаний, необходимых для официального утверждения типа, уже были проведены в процессе аттестации и сертификации систем защиты, то повторное их проведение не требуется. В таких случаях можно ограничиться проверкой результатов этих испытаний. Характеристики, которые должны проверяться в процессе сертификации защиты (или которые тесно связаны с проводимыми при этом испытаниями) в справочных целях помечены в настоящем ~~добавлении~~ **подразделе** знаком «*».

Перечисленные требования относятся к ~~подразделу~~ **добавлению 1С**, в то время как другие требования относятся к другим **подразделам** данного добавления (например, PIC_001 относится к пиктограммам в **подразделе 3** добавления).

Официальное утверждение типа датчика движения, бортового устройства и внешнего устройства ГНСС рассматривается в настоящем ~~приложении~~ **подразделе** добавления отдельно в качестве разных компонентов ~~записывающей аппаратуры~~ **контрольного устройства**. На каждый компонент будет выдаваться свой собственный сертификат официального утверждения типа, в котором будут указываться другие совместимые компоненты. Рабочее испытание датчика движения (или внешнего устройства ГНСС) будет осуществляться вместе с бортовым устройством и наоборот.

Эксплуатационная совместимость каждой модели датчика движения с каждой моделью бортового устройства необязательна; поэтому тип датчика движения может быть утвержден только в сочетании с соответствующим типом бортового устройства, и наоборот.

Национальный орган, ответственный за проведение рабочих испытаний соответствующего бортового устройства или внешнего устройства ГНСС должен в обязательном порядке убедиться в том, что встроенный приемник ГНСС

успешно прошел испытания OSNMA, указанные в настоящем подразделе добавления. Считается, что эти испытания представляют собой один из компонентов рабочих испытаний бортового устройства и внешнего устройства ГНСС.

1.2 Справочные материалы

При подготовке данного ~~добавления~~ **подраздела** использовались следующие источники:

IEC 60068-2-1: Испытания на воздействие внешних факторов. Часть 2-1: Испытания. Испытание А. Холод.

IEC 60068-2-2: Испытания на воздействие внешних факторов. Часть 2: Испытания. Испытание В. Сухое тепло (синусоидальное воздействие).

IEC 60068-2-6: Испытания на воздействие внешних факторов. Часть 2: Испытания — Испытание Fc: Вибрация.

IEC 60068-2-14: Испытания на воздействие внешних факторов; Часть 2-14: Испытания; Испытание N: Изменение температуры.

IEC 60068-2-27: Испытания на воздействие внешних факторов. Часть 2: Испытания. Испытание Ea и руководство: Ударные воздействия.

IEC 60068-2-30: Испытания на воздействие внешних факторов — Часть 2-30: Испытания — Испытание Db: Влажное тепло, циклическое воздействие (цикл: 12 ч + 12 ч).

IEC 60068-2-64: Испытания на воздействие внешних факторов — Часть 2-64: Испытания — Испытание Fh: Вибрация, в широком диапазоне частот и руководство.

IEC 60068-2-78 Испытания на воздействие внешних факторов — Часть 2-78: Испытания — Испытание в испытательной камере: влажное тепло, стационарное состояние.

ISO 16750-3 — Механические нагрузки (2012-12).

ISO 16750-4 — Климатические нагрузки (2010-04).

ISO 20653: Транспорт дорожный — Степень защиты (код IP) — Защита электрооборудования от инородных предметов, воды и доступа.

ISO 10605 :2008 + Техническая поправка :2010 + AMD1 :2014 Транспорт дорожный — Методы испытаний на воздействие электрических помех вследствие электростатического разряда.

ISO 7637-1 :2002 + AMD1 : 2008: Транспорт дорожный — Электрические помехи, вызываемые проводимостью и взаимодействием — Часть 1: Определения и общие положения.

ISO 7637-2 Транспорт дорожный — Электрические помехи, вызываемые проводимостью и взаимодействием — Часть 2: Кондуктивные импульсные помехи в цепях питания.

ISO 7637-3 Транспорт дорожный — Электрические помехи, вызываемые проводимостью и взаимодействием — Часть 3: Распространение помех, вызываемых переходными процессами, обусловленными емкостным или индуктивным соединением в цепях питания.

ISO/IEC 7816-1 Информационные технологии. Карточки идентификационные. Карточки на интегральных микросхемах с контактами. Часть 1. Физические характеристики.

ISO/IEC 7816-2 Информационные технологии. Карточки идентификационные. Карточки на интегральных микросхемах с контактами. Часть 2. Размеры и расположение контактов.

ISO/IEC 7816-3 Информационные технологии. Карточки идентификационные. Карточки на интегральных микросхемах с контактами. Часть 3. Электронные сигналы и протоколы передачи.

ISO/IEC 10373-1 :2006 + AMD1 :2012 Карточки идентификационные. Методы испытаний, Часть 1: Общие характеристики.

ISO/IEC 10373-3 :2010 + Техническая поправка: Карточки идентификационные, 2013 год — Методы испытаний — Часть 3: Карточки на интегральных микросхемах с контактами и соответствующие устройства сопряжения.

ISO 16844-3:2004, Cor 1:2006 Транспорт дорожный — Транспортные системы — Часть 3: Устройства сопряжения датчиков движения (с бортовыми устройствами).

ISO 16844-4 Транспорт дорожный — Тахографические системы — Часть 4: Интерфейс CA

ISO 16844-6 Транспорт дорожный — Тахографические системы — Часть 6: Диагностика

ISO 16844-7 Транспорт дорожный — Тахографические системы — Часть 7: Параметр

ISO 534 Транспорт дорожный — Определение толщины, плотности и удельного объема

UN ECE R10 Единообразные предписания, касающиеся официального утверждения транспортных средств в отношении электромагнитной совместимости (Европейская комиссия Организации Объединенных Наций)

RGODP Технический доклад СИЦ — Руководящие указания по приемникам для обработки данных

2. Рабочие испытания бортового устройства

№	Вид испытания	Описание	Предъявляемые требования
1	Административная проверка		
1.1	Документация	Правильность оформления документации	
1.2	Результаты испытаний, проведенных изготовителем	Результаты испытаний, проводившихся изготовителем при сборке. Проверка технических характеристик по документам.	88, 89,91
2	Визуальный осмотр		
2.1	Соответствие документации		
2.2	Идентификация/маркировка		224–226
2.3	Материалы		219–223
2.4	Наложение пломб		398, 401–405
2.5	Внешние интерфейсы		
3	Рабочие испытания		
3.1	Предусмотренные функции		02 , 03, 04, 05, 07, 382,
3.2	Режимы работы		09–11*, 132 , 133 134 , 135
3.3	Функции и права доступа к данным		12* 13*, 382, 383, 386 to 389
3.4	Контроль за вводом и извлечением карточек		15, 16, 17, 18, 19*, 20*, 132 134
3.5	Измерение скорости, местоположения и пробега		21–374

№	Вид испытания	Описание	Предъявляемые требования
3.6		Отсчет времени (испытание проводится при 20 °C)	38–43
3.7		Контроль за деятельностью водителей	44–53, 132 134
3.8		Контроль за управлением	54, 55, 132 132A
3.9		Ввод данных водителем вручную	56–62c
3.10		Установка блокировки предприятием	63–68
3.11		Мониторинг контрольных операций	69, 70
3.12		Обнаружение событий и/или неисправностей	71–88a, 132 132A
3.13		Идентификационные данные аппаратуры	93*, 94*, 97, 100
3.14		Данные о вводе и извлечении карточек водителя или мастерской	102*–104*
3.15		Данные о деятельности водителей	105*–107*
3.16		Данные о географических пунктах и местоположениях	108*–112*
3.17		Показания счетчика пробега	113*–115*
3.18		Подробные данные о скоростном режиме	116*
3.19		Данные о событиях	117*
3.20		Данные о неисправностях	118*
3.21		Данные калибровки	119*–21*
3.22		Данные о корректировке времени	124*, 125*
3.23		Данные о контрольных операциях	126*, 127*
3.24		Данные о блокировках, установленных предприятием	128*
3.25		Данные об операциях по загрузке данных	129*
3.26		Данные об особых ситуациях	130*, 131*
3.27		Данные о карточках тахографа	132*, 133*
3.28		Пересечение границы	133a*–133d*
3.29		Операция по загрузке/разгрузке	133e*–133i*
3.30		Цифровая карта	133j*–133s*
3.31 ²⁷		Регистрация и сохранение данных на карточках тахографа	134, 135, 136, 137, 138* , 139*, 141*, 142, 143, 144, 145, 146*, 147*, 147a* , 147b* , 148*, 149, 150, 150a
3.32 ²⁸		Индикация данных на дисплее	90, 132 134, 149, 151–166, 168, PIC_001, DIS_001
3.33 ²⁹		Распечатка	90, 132 134, 167, 169–179, 181, PIC_001, PRT_001–PRT_014
3.34 ⁰		Сигналы предупреждения	132, 180 134, 182–189, 191, PIC_001
3.35 ⁴		Сохранение данных на внешнем носителе	90, 132, 190 134, 192–194, 196
3.36 ²		Удаленный обмен данными о целевых проверках на дорогах	195 197–197, 199
3.37 ³		Обмен данными с выводом данных на дополнительных внешних устройствах	198, 199 200, 201
3.38 ⁴		Калибровка	202–206*, 383, 384, 386–391

№	Вид испытания	Описание	Предъявляемые требования
3.395	Проверки калибровки на дорогах		207–209
3.4036	Корректировка времени		210–212*
3.41	Мониторинг пересечения границ		226a–226c
3.42	Обновление программного обеспечения		226d–226f
3.4337	Отсутствие помех при выполнении дополнительных функций		06, 425
3.4438	Интерфейс датчика движения		02, 122
3.4539	Внешнее устройство ГНСС		03, 123
3.460	Проверка с целью убедиться в том, что БУ обнаруживает, регистрирует и хранит данные о событии(ях) и/или неисправности(ях), указанных изготовителем БУ, когда подсоединенный датчик движения реагирует на магнитные поля, вызывающие помехи при обнаружении движения транспортного средства.		217
3.474	Инструкции по шифрованию и стандартизованные параметры домена		CSM_48, CSM_50
4	Испытания на воздействие внешних факторов		
4.1	Температура	<p>Проверка функциональности посредством проведения: испытания в соответствии с ISO 16750-4, глава 5.1.1.2: рабочие испытания при низкой температуре (72 ч при –20 °C)</p> <p>Это испытание строится на основе стандарта IEC 60068-2-1: Испытания на воздействие внешних факторов — Часть 2-1: Испытания — Испытание А: Холод</p> <p>Испытания в соответствии с ISO 16750-4: Глава 5.1.2.2: рабочие испытания при высокой температуре (72 ч при 70 °C). Это испытание строится на основе стандарта IEC 60068-2-2: Базовые процедуры испытания на воздействие внешних факторов; часть 2: испытания; испытания В: сухое тепло</p> <p>Испытания в соответствии с ISO 16750-4: Глава 5.3.2: Быстрая смена температуры с конкретным периодом перепада (–20 °C/70 °C, 20 циклов, время выдерживания 2 ч при каждой температуре)</p> <p>Возможно проведение сокращенной серии испытаний (из числа указанных в разделе 3 настоящей таблицы) при низкой и высокой температурах, а также на протяжении термоциклов</p>	213
4.2	Влажность	Проверка способности бортового устройства выдерживать циклические колебания (температуры во влажной среде (согласно стандарту IEC 60068-2-30, испытание Db: шесть 24-часовых циклов с перепадом температуры от +25 °C до +55 °C в каждом цикле и относительной влажностью воздуха, равной 97 % при + 25 °C и эквивалентной 93 % при +55 °C	214
4.3	Механическая прочность	<p>1. Синусоидальные вибрации</p> <p>Проверка способности бортового устройства выдерживать синусоидальные вибрации по следующей схеме:</p> <p>постоянное смещение в диапазоне от 5 до 11 Гц: пик 10 мм</p> <p>постоянное ускорение в диапазоне 11-300 Гц: 5 g</p> <p>Соответствие данному требованию проверяется согласно стандарту IEC 60068-2-6, испытание Fc</p>	219

№	Вид испытания	Описание	Предъявляемые требования
		<p>минимальной продолжительностью 3 x 12 часов (по 12 часов на каждую ось)</p> <p>ISO 16750-3 не требует испытаний на синусоидальную вибрацию для устройств в транспортном средстве с отдельной кабиной</p> <p>2. Случайная вибрация: Испытания в соответствии с ISO 16750-3: Глава 4.1.2.8: Испытание VIII: Транспортное средство неиндивидуального пользования с отдельной кабиной Испытание на случайные вибрации, 10...2000 Гц, RMS по вертикали 21,3 м/с², RMS в продольном направлении 11,8 м/с², RMS в боковом направлении 13,1 м/с², 3 оси, 32 ч на ось, включая температурный цикл в диапазоне -20...70 °C</p> <p>Это испытание строится на основе стандарта IEC 60068-2-64: Испытание на воздействие внешних факторов — Часть 2-64: Испытания — Испытание Fh: Вибрация широкополосная на произвольной основе и руководство</p> <p>3. Испытание на ударные нагрузки: механический удар с ускорением 3 g и полусинусоидальной схемой согласно стандарту ISO 16750</p> <p>Испытания, описанные выше, проводятся на различных образцах типового оборудования, подвергаемого испытанию</p>	
4.4	Защита от попадания воды и посторонних предметов	Испытания в соответствии с ISO 20653: Транспорт дорожный — Степень защиты (код IP) — Защита электрооборудования от воздействия посторонних предметов, воды и доступа извне (без изменения параметров); минимальное значение — IP 40	220, 221
4.5	Защита от перенапряжения	Проверка с целью убедиться в том, что бортовое устройство может выдерживать скачки напряжения в бортовой сети: Версия на 24 В: 34 В при +40 °C в течение 1 часа Версия на 12 В: 17 В при +40 °C в течение 1 часа (ISO 16750-2)	216
4.6	Защита от несоблюдения полярности	Проверка с целью убедиться в том, что бортовое устройство может выдерживать нарушения полярности своего источника питания (ISO 16750-2)	216
4.7	Защита от короткого замыкания	Проверка с целью убедиться в том, что входные/выходные сигналы предохранены от короткого замыкания цепей электропитания на землю (ISO 16750-2)	216
5	Испытания на электромагнитную совместимость		
5.1	Излучения и электромагнитная защищенность	Соответствие Правилам № 10 ЕЭК	218
5.2	Устойчивость к электростатическому разряду	Соответствие стандарту ISO 10605:2008 + технической поправке: 2010 + AMD1: 2014: +/- 4кВ в случае контакта и +/- 8кВ в случае воздушного разряда	218

№	Вид испытания	Описание	Предъявляемые требования
5.3	Невосприимчивость к быстрым переходным процессам в цепи питания	<p>В вариантах на 24 В — соответствие ISO 7637-2 + Правила ЕЭК № 10, пересмотр 3:</p> <p>импульс 1a: $V_s = -450$ В $R_i = 50$ Ом импульс 2a: $V_s = +37$ В $R_i = 2$ Ом импульс 2b: $V_s = +20$ В $R_i = 0,05$ Ом импульс 3a: $V_s = -150$ В $R_i = 50$ Ом импульс 3b: $V_s = +150$ В $R_i = 50$ Ом импульс 4: $V_s = -16$ В $V_a = -12$ В $t_6 = 100$ мс импульс 5: $V_s = +120$ В $R_i = 2,2$ Ом $t_d = 250$ мс</p> <p>В вариантах на 12 В: соответствие ISO 7637-1 + Правилам ЕЭК № 10, Пересмотр 3:</p> <p>импульс 1: $V_s = -75$ В $R_i = 10$ Ом импульс 2a: $V_s = +37$ В $R_i = 2$ Ом импульс 2b: $V_s = +10$ В $R_i = 0,05$ Ом импульс 3a: $V_s = -112$ В $R_i = 50$ Ом импульс 3b: $V_s = +75$ В $R_i = 50$ Ом импульс 4: $V_s = -6$ В $V_a = -5$ В $t_6 = 15$ мс импульс 5: $V_s = +65$ В $R_i = 3$ Ом $t_d = 100$ мс</p> <p>Импульс 5 проверяется только при испытании бортовых устройств, предназначенных для установки на транспортных средствах, не оборудованных единой внешней защитой от сброса нагрузки генератора</p> <p>В связи с предложением по сбросу нагрузки см. ISO 16750-2, 4-е издание, глава 4.6.4</p>	218

3. Рабочие испытания датчика движения

№	Вид испытания	Описание	Предъявляемые требования
1.	Административная проверка		
1.1	Документация	Правильность оформления документации	
2.	Визуальный осмотр		
2.1.	Соответствие документации		
2.2.	Идентификация/маркировка		225, 226,
2.3	Материалы		219–223
2.4.	Наложение пломб		398, 401–405
3.	Рабочие испытания		
3.1	Идентификационные данные датчика		95–97*
3.2	Датчик движения — подключение к бортовому устройству		122*, 204
3.3	Выявление движения		
	Точность измерения параметров движения		30–35
3.4	Интерфейс бортового устройства		02
3.5	Проверка с целью убедиться в том, что датчик движения не подвержен воздействию постоянного магнитного поля. В качестве варианта проверить, что датчик движения реагирует на постоянные магнитные поля, создающие помехи в выявлении движения транспортного средства, которые позволяют подсоединенному БУ выявлять, регистрировать и хранить данные о сбоях в работе датчика		217

№	Вид испытания	Описание	Предъявляемые требования
4. Испытания на воздействие внешних факторов			
4.1	Рабочая температура	<p>Проверка работоспособности (в соответствии с определением, приведенным в связи с испытанием № 2 3.3) в температурном диапазоне $[-40\text{ °C}; +135\text{ °C}]$ согласно:</p> <p>стандарту IEC 60068-2-1, испытание Ad: продолжительность испытания — 96 часов при нижней предельной температуре T_{min},</p> <p>стандарту IEC 60068-2-2, испытание Bd, продолжительность испытания — 96 часов при верхней предельной температуре T_{max}</p> <p>Испытание согласно стандарту ISO 16750-4: Глава 5.1.1.2: Испытание на работоспособность в условиях низких температур (24 h при -40 °C)</p> <p>Это испытание строится на основе стандарта IEC 60068-2-1: Испытание на воздействие внешних факторов — Часть 2-1: Испытания — Испытание A: IEC 68-2-2 (для низких температур), испытание Bd: продолжительность испытания — 96 часов при нижней предельной температуре -40 °C</p> <p>Испытание согласно стандарту ISO 16750-4: Глава 5.1.2.2: Рабочее испытание в условиях высокой температуры (96 ч при 135 °C)</p> <p>Это испытание строится на основе стандарта IEC 60068-2-2: Базовые процедуры испытания на воздействие внешних факторов; часть 2: испытания; испытания B: сухое тепло</p>	213
4.2	Температурные циклы	<p>Испытание согласно стандарту ISO 16750-4: Глава 5.3.2: Быстрая смена температуры с указанной продолжительностью перехода ($-40\text{ °C}/135\text{ °C}$, 20 циклов, время выдержки 30 мин при каждой температуре)</p> <p>IEC 60068-2-14: Испытания на воздействие внешних факторов; Часть 2-14: Испытания; Испытание N: изменение температуры</p>	213
4.3	Циклы влажности	<p>Проверка работоспособности (как указано в испытании № 3.3) согласно IEC 60068-2-30, испытание Db: шесть 24-часовых циклов с изменением температуры от $+25\text{ °C}$ до $+55\text{ °C}$ в каждом цикле и относительной влажностью воздуха, равной 97 % при $+25\text{ °C}$ и эквивалентной 93 % при $+55\text{ °C}$</p>	214
4.4	Вибрация	<p>ISO 16750-3: Глава 4.1.2.6: Испытание VI: Транспортное средство индивидуального пользования, двигатель, коробка передач</p> <p>Испытания на вибрацию в смешанном режиме, включая</p> <p>испытания на синусоидальную вибрацию, 20...520 Гц, $11,4 \dots 120\text{ м/с}^2$, $\leq 0,5$ окт./мин</p> <p>Испытания на случайные колебания, 10...2000 Гц, $\text{RMS } 177\text{ м/с}^2$</p> <p>а) 94 ч на каждую ось, включая температурный цикл — 20...70 °C)</p> <p>б) Данные испытания строятся на основе стандарта IEC 60068-2-80: Экологические испытания. Часть 2-80: Испытания. Испытание Fi: вибрация, смешанный режим</p>	219

№	Вид испытания	Описание	Предъявляемые требования
4.5	Механический удар	ISO 16750-3: Глава 4.2.3: Испытание VI: Испытания устройств в коробке передач или на ней полусинусоидальный удар, ускорение, подлежащее согласованию в пределах 3000...15000 м/с ² , продолжительность импульса, подлежащая согласованию, но <1 мс, число ударов: подлежит согласованию Данные испытания строятся на стандарте IEC 60068-2-27: Испытания на воздействие внешних факторов. Часть 2: Испытания. Испытание Ea и руководство: удар	219
4.6	Защита от попадания воды и посторонних предметов	Испытания в соответствии с ISO 20653: Транспортные средства, дорожные. Степень защиты (код IP). Защита электрооборудования от инородных тел, воды и доступа (целевое значение IP 64)	220, 221
4.7	Защита от несоблюдения полярности	Проверка способности датчика движения выдерживать подключение к источнику питания противоположной полярности	216
4.8	Защита от короткого замыкания	Проверка защищенности сигналов ввода/вывода от короткого замыкания на источник питания и на массу	216
5.	ЭМС		
5.1	Излучения и электромагнитная защищенность	Проверка соответствия Правилам ЕЭК № 10	218
5.2	Электростатический разряд	Соответствие ISO 10605 :2008 + Техническая поправка: 2010 + AMD1: 2014: +/-4 кВ для контакта и +/-8 кВ для расхода воздуха	218
5.3	Подверженность кондуктивным помехам в каналах передачи данных	Варианты на 24 В: соответствие с ISO 7637-2 + Правила ЕЭК № 10, Пересмотр 3: импульс 1a: $V_s = -450$ В $R_i = 50$ Ом импульс 2a: $V_s = +37$ В $R_i = 2$ Ом импульс 2b: $V_s = +20$ В $R_i = 0,05$ Ом импульс 3a: $V_s = -150$ В $R_i = 50$ Ом импульс 3b: $V_s = +150$ В $R_i = 50$ Ом импульс 4: $V_s = -16$ В $V_a = -12$ В $t_6 = 100$ мс импульс 5: $V_s = +120$ В $R_i = 2,2$ Ом $t_d = 250$ мс Варианты на 12 В: соответствие с ISO 7637-1 + Правила ЕЭК № 10, Пересмотр Rev. 3: импульс 1: $V_s = -75$ В $R_i = 10$ Ом импульс 2a: $V_s = +37$ В $R_i = 2$ Ом импульс 2b: $V_s = +10$ В $R_i = 0,05$ Ом импульс 3a: $V_s = -112$ В $R_i = 50$ Ом импульс 3b: $V_s = +75$ В $R_i = 50$ Ом импульс 4: $V_s = -6$ В $V_a = -5$ В $t_6 = 15$ мс импульс 5: $V_s = +65$ В $R_i = 3$ Ом $t_d = 100$ мс Импульс 5 используется только при испытании бортовых устройств для установки на транспортных средствах, не оборудованных единой внешней защитой от сброса нагрузки генератора По поводу предложения о сбросе нагрузки генератора см. ISO 16750-2, 4-е издание, глава 4.6.4	218

4. Функциональные испытания карточек тахографа

Испытания в соответствии с данным разделом 4,

№ 5 «Протокольные испытания»;

№ 6 «Структура карточки»; и

№ 7 «Рабочие испытания»

может проводить специалист по оценке или сертификации в рамках процедуры сертификации системы защиты на основании общих критериев применительно к модулю микросхемы.

Испытания № 2.3 и № 4.2 одинаковы. Это — механические испытания всей системы в составе основы карточки и модуля микросхемы. Такие испытания необходимы в том случае, если меняется один из этих компонентов (основа карточки или модуль микросхемы).

№	Испытание	Описание	Соответствующие требования
1	Административная проверка		
1.1	Документация	Правильность документации	
2	Основа карточки		
2.1	Дизайн печати	<p>Убедиться в том, что все элементы защиты и визуальной информации нанесены правильно и соответствуют установленным требованиям</p> <p>[Указатель] Приложение Добавление 1С, глава 4.1 «Визуальная информация», 227) На первой странице указываются: слова «Карточка водителя», или «Карточка контролера», или «Карточка мастерской» или «Карточка предприятия», напечатанные заглавными буквами на официальном языке или языках государства-члена, выдавшего Договаривающейся стороны, выдавшей карточку, в соответствии с типом карточки.</p> <p>[название государства-члена Договаривающейся стороны] Приложение Добавление 1С, глава 4.1 «Визуальная информация», 228) На первой странице указывается: название государства-члена, выдавшего Договаривающейся стороны, выдавшей карточку (факультативно).</p> <p>[Знак] Приложение Добавление 1С, глава 4.1 «Визуальная информация», 229) На первой странице указывается: отличительный знак государства-члена, выдавшего Договаривающейся стороны, выдавшей карточку, напечатанный в виде негатива в синем прямоугольнике в окружении 12 желтых звезд.</p>	227–229, 232, 234–236

		<p>[Перечисление] Приложение Добавление 1С, глава 4.1 «Визуальная информация», 232) На обратной стороне указывается: разъяснение пронумерованных позиций, содержащихся на лицевой стороне карточки.</p> <p>[Цвет] Приложение Добавление 1С, глава 4.1 «Визуальная информация», 234) Текст карточек тахографа печатается на фоне следующих основных цветов: – карточка водителя: белый, – карточка мастерской: красный, – карточка контролера: синий, – карточка предприятия: желтый.</p> <p>[Защита] Приложение Добавление 1С, глава 4.1 «Визуальная информация», 235) Карточки тахографа должны содержать как минимум следующие элементы защиты основы карточки от подделки и фальсификации: — защитный фоновый рисунок тонкой сетки блокперфект и печатная расцветка цветами радуги, – по крайней мере одна двухцветная линия — микропринт.</p> <p>[Маркировка] Приложение Добавление, глава 4.1 «Визуальная информация», 236) Государства-члены Договаривающиеся стороны могут включать цвета или маркировку, например, национальные символы и элементы защиты.</p> <p>[Знак официального утверждения] Карточки тахографа содержат знак официального утверждения. Знак официального утверждения состоит из: – прямоугольника, в котором проставлена буква «е», за которой следует указанный ниже общепринятый отличительный номер или буквенный код страны, предоставившей официальное утверждение, – номера официального утверждения, соответствующего номеру сертификата официального утверждения карточки тахографа в любой точке в непосредственной близости от этого прямоугольника.</p>	
2.2	Механические испытания	<p>[Размер карточки] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Карточки идентификационные — физические характеристики, [5] Габариты карточки, [5.1] Размер карточки, [5.1.1] Габариты и допуски карточки, тип карточки ID-1 Неиспользованная карточка</p>	240, 243 ISO/IES 7810

		<p>[Края карточки] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Карточки идентификационные — физические характеристики, [5] Габариты карточки, [5.1] Размер карточки, [5.1.2] Края карточки</p> <p>[Конструкция карточки] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Идентификационные карточки — физические характеристики, [6] Конструкция карточки</p> <p>[Материалы карточки] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Карточки идентификационные — физические характеристики, [7] Материалы карточки</p> <p>[Жесткость при сгибании] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Карточки идентификационные — физические характеристики, [8] Характеристики карточки, [8.1] Жесткость при сгибании</p> <p>[Токсичность] Карточки тахографа должны соответствовать стандарту ISO/IEC 781 Карточки идентификационные — физические характеристики, [8] Характеристики карточки, [8.3] Токсичность</p> <p>[Стойкость к химическим веществам] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Карточки идентификационные — физические характеристики, [8] Характеристики карточки, [8.4] Стойкость к химическим веществам</p> <p>[Стабильность карточки] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Карточки идентификационные — физические характеристики, [8] Характеристики карточки, [8.5] Стабильность габаритов карточки и коробление при воздействии температуры и влажности</p>	
--	--	---	--

		<p>[Освещение] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Карточки идентификационные — физические характеристики, [8] Характеристики карточки, [8.6] Освещение</p> <p>[Долговечность] Приложение Добавление 1С, глава 4.4 «Экологические и электрические спецификации», 241) Карточки тахографа способны надлежащим образом работать в течение пяти лет, если они используются с соблюдением указанных спецификаций по условиям окружающей среды и электромагнитной совместимости.</p> <p>[Прочность на отслаивание] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Карточки идентификационные — физические характеристики, [8] Характеристики карточки, [8.8] Прочность на отслаивание</p> <p>[Сцепление или блокирование] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Карточки идентификационные — физические характеристики, [8] Характеристики карточки, [8.9] Сцепление или блокирование</p> <p>[Коробление] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Карточки идентификационные — физические характеристики, [8] Характеристики карточки, [8.11] Общее коробление карточки</p> <p>[Теплостойкость] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Карточки идентификационные — физические характеристики, [8] Характеристики карточки, [8.12] Теплостойкость</p> <p>[Искажения поверхности] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Карточки идентификационные — физические характеристики, [8] Характеристики карточки, [8.13] Искажения поверхности</p>	
--	--	--	--

		<p>[Загрязнение]</p> <p>Карточки тахографа должны соответствовать стандарту ISO/IEC 7810</p> <p>Карточки идентификационные — физические характеристики,</p> <p>[8] Характеристики карточки,</p> <p>[8.14] Загрязнение и взаимодействие компонентов карточки</p>	
2.3	Механические испытания встроенного модуля микросхемы	<p>[Сгибание]</p> <p>Карточки тахографа должны соответствовать стандарту ISO/IEC 7810:2003/Amd. 1:2009, Карточки идентификационные — физические характеристики, поправка 1: Критерии для карточек на интегральных микросхемах</p> <p>[9.2] Динамическое напряжение при сгибании</p> <p>Общее число циклов сгибания: 4000.</p> <p>[Скручивание]</p> <p>Карточки тахографа должны соответствовать стандарту ISO/IEC 7810:2003/Amd. 1:2009, Карточки идентификационные — физические характеристики, поправка 1: Критерии для карточек на интегральных микросхемах</p> <p>[9.2] Динамическое напряжение при скручивании</p> <p>Общее число циклов скручивания: 4000.</p>	ISO/IEC 7810
3	Модуль		
3.1	Модуль	<p>Модуль — это изоляция микросхемы и контактная пластинка.</p> <p>[Контур поверхности]</p> <p>Карточки тахографа должны соответствовать стандарту ISO/IEC 7816-1:2011 Карточки идентификационные — карточки на интегральных микросхемах. Часть 1: карточки с контактами — физические характеристики</p> <p>[4.2] Контур поверхности контактов</p> <p>[Механическая прочность]</p> <p>Карточки тахографа должны соответствовать стандарту ISO/IEC 7816-1:2011 Карточки идентификационные — карточки на интегральных микросхемах. Часть 1: карточки с контактами — физические характеристики</p> <p>[4.3] Механическая прочность (карточки и контактов)</p> <p>[Электрическое сопротивление]</p> <p>Карточки тахографа должны соответствовать стандарту ISO/IEC 7816-1:2011 Карточки идентификационные — карточки на интегральных микросхемах. Часть 1: карточки с контактами — физические характеристики</p> <p>[4.4] Электрическое сопротивление (контактов)</p>	ISO/IEC 7816

		<p>[Размеры]</p> <p>Карточки тахографа должны соответствовать стандарту ISO/IEC 7816-1:2011 Карточки идентификационные — карточки на интегральных микросхемах. Часть 2: карточки с контактами — габариты и расположение контактов</p> <p>[3] Размеры контактов</p>	
		<p>[Расположение]</p> <p>Карточки тахографа должны соответствовать стандарту ISO/IEC 7816-1:2007 Карточки идентификационные — карточки на интегральных микросхемах. Часть 2: карточки с контактами — Размеры и расположение контактов</p> <p>[4] Число и расположение контактов</p> <p>В случае модулей с шестью контактами настоящее требование к испытаниям не относится к контактам 'C4' и 'C8'.</p>	
4	Микросхема		
4.1	Circuit	<p>[Рабочая температура]</p> <p>Микросхема карточки тахографа работает в диапазоне температур окружающей среды от $-25\text{ }^{\circ}\text{C}$ до $+85\text{ }^{\circ}\text{C}$.</p> <p>[Температура и влажность]</p> <p>Приложение Добавление 1С, глава 4.4 «Экологические и электрические спецификации», 241)</p> <p>Карточки тахографа способны надлежащим образом работать в любых климатических условиях, которые обычно встречаются на территории Сообщества, как минимум в диапазоне температур от $-25\text{ }^{\circ}\text{C}$ до $+70\text{ }^{\circ}\text{C}$ с нерегулярными пиковыми значениями до $+85\text{ }^{\circ}\text{C}$; при этом термин «нерегулярные» означает не более 4 часов каждый раз и не более 100 раз в течение всего срока службы карточки.</p> <p>Карточки тахографа через последовательные этапы на определенный период времени подвергаются воздействию следующих температур и влажности. После каждого такого этапа карточки тахографа проходят испытания на электротехническую пригодность к работе.</p> <ol style="list-style-type: none"> 1. Температура — $20\text{ }^{\circ}\text{C}$ на 2 ч. 2. Температура $+/-0\text{ }^{\circ}\text{C}$ на 2 ч. 3. Температура $+20\text{ }^{\circ}\text{C}$, 50 % RH на 2 ч. 4. Температура $+50\text{ }^{\circ}\text{C}$, 50 % RH на 2 ч. 5. Температура $+70\text{ }^{\circ}\text{C}$, 50 % RH на 2 ч. <p>Температура периодически повышается до $+85\text{ }^{\circ}\text{C}$, 50 % RH, на 60 мин.</p> <ol style="list-style-type: none"> 6. Температура $+70\text{ }^{\circ}\text{C}$, 85 % RH на 2 ч. <p>Температура периодически повышается до $+85\text{ }^{\circ}\text{C}$, 85 % RH, на 30 мин.</p> <p>[Влажность]</p> <p>Приложение Добавление 1С, глава 4.4 «Экологические и электротехнические спецификации», 242)</p> <p>Карточки тахографа полностью работоспособны в диапазоне влажности от 10 % до 90 %.</p>	<p>241–244 ECE R10 ISO/IES 7810 ISO/IES 10373</p>

		<p>[Электромагнитная совместимость (ЭМС)] Приложение Добавление 1С, глава 4.4 «Экологические и электротехнические спецификации» 244) В процессе работы карточки тахографа соответствуют Правилам ЕЭК № 10, касающимся электромагнитной совместимости.</p> <hr/> <p>[Статическое электричество] Приложение Добавление 1С, глава 4.4 «Экологические и электрические спецификации», 244) Во время работы карточки тахографа защищены от электростатических разрядов. Карточки тахографа должны соответствовать стандарту ISO/IEC 7810:2003/Amd. 1:2009, Карточки идентификационные — физические характеристики, поправка 1: Критерии для карточек на интегральных микросхемах [9.4] Статическое электричество [9.4.1] Контактные карточки с ИС Испытательное напряжение: 4000 В</p> <hr/> <p>[Рентгеновское излучение] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810:2003/Amd. 1:2009, Карточки идентификационные — физические характеристики, поправка 1: Критерии для карточек на интегральных микросхемах [9.1] Рентгеновское излучение</p> <hr/> <p>[Ультрафиолетовое излучение] ISO/IEC 10373-1:2006 Карточки идентификационные. Методы испытаний. Часть 1: Общие характеристики [5.11] Ультрафиолетовое излучение</p> <hr/> <p>[3-х роликовое испытание] Карточки тахографа должны соответствовать стандарту ISO/IEC 10373-1:2006/Amd. 1:2012, Карточки идентификационные — Методы испытаний. Часть 1: общие характеристики, поправка 1: [5.22] ICC — механическая прочность: 3-х роликовое испытание для ICC с контактами</p> <hr/> <p>[Перегиб] Карточки тахографа должны соответствовать стандарту MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Испытание на прочность методом перегиба [13.2.1.32] TM-422: Механическая стойкость Испытание на перегиб</p>	
4.2	Механические испытания модуля микросхемы, встроенного в основу карточки -> так же, как в 2.3	<p>[Сгибание] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810:2003/Amd. 1:2009, Идентификационные карточки — физические характеристики, поправка 1: Критерии для карточек на интегральных микросхемах [9.2] Динамическое напряжение при сгибании Общее число циклов сгибания: 4000.</p>	ISO/IEC 7810

		<p>[Скручивание]</p> <p>Карточки тахографа должны соответствовать стандарту ISO/IEC 7810:2003/Amd. 1:2009, Карточки идентификационные — физические характеристики, поправка 1: Критерии для карточек на интегральных микросхемах</p> <p>[9.3] Динамическое напряжение при скручивании</p> <p>Общее число циклов скручивания: 4000.</p>	
5	Протокольные испытания		
5.1	ATR	Проверка соответствия ATR установленным требованиям	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T = 0	Проверка соответствия протокола T = 0	ISO/CEI 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Проверка совместимости команды PTS путем задания протокола T = 1 при исходном T = 0	ISO/CEI 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T = 1	Проверка соответствия протокола T = 1	ISO/CEI 7816-3 TCS_11, TCS_13, TCS_16
6	Структура данных на карточке		
6.1		Подтверждение соответствия файловой структуры на карточке путем проверки наличия обязательных файлов и тестирования условий доступа к ним	TCS_22–TCS_28 TCS_140–TCS_179
7	Функциональные испытания		
7.1	Нормальная обработка	Как минимум, разовая проверка допустимого использования каждой команды (например, проверка исполнения команды UPDATE BINARY при CLA = '00', CLA = '0C' и при разных значениях параметров P1, P2 и Lc). Подтверждение фактического выполнения карточкой соответствующих операций (например, путем считывания файла после исполнения команды на его обработку)	TCS_29–TCS_139
7.2	Сообщение об ошибке	Как минимум, разовое тестирование каждого сообщения об ошибке (из числа указанных в приложении приложении подраздел 2 добавления) при исполнении каждой команды Как минимум, разовое тестирование на общую ошибку каждого вида (кроме ошибок целостности серии '6400', которые проверяются при сертификации систем защиты)	
7.3	Модуль шифрования и стандартизованные параметры домена		CSM_48, CSM_50
8	Персонализация		
8.1	Оптическая персонализация	<p>Приложение Добавление 1C, глава 4.1 «Визуальная информация», 230)</p> <p>На первой странице указывается: конкретная информация, касающаяся выданной карточки.</p>	230, 231, 235

	<p>Приложение Добавление 1С, глава 4.1 «Визуальная информация», 231) На первой странице указываются: даты в формате «дд/мм/гггг» или «дд.мм.гггг» (день, месяц, год).</p> <p>Приложение Добавление 1С, глава 4.1 «Визуальная информация», 235) Карточки тахографа должны содержать как минимум следующие элементы защиты основы карточки от подделки и фальсификации: – на месте фотографии — фоновый защитный рисунок, который перекрывается фотографией.</p>	
--	--	--

5. Испытания внешнего устройства ГНСС

№	Испытание	Описание	Соответствующие требования
1.	Административная проверка		
1.1	Документация	Правильность документации	
2.	Визуальный осмотр внешнего устройства ГНСС		
2.1	Соответствие документации		
2.2	Идентификация/маркировка		224–226
2.3	Материалы		219–223
3.	Функциональные испытания		
3.1	Идентификационные данные датчика		98, 99
3.2	Соединение внешнего модуля ГНСС и бортового устройства		123, 205
3.3	Местоположение ГНСС S		36, 37
3.4	Интерфейс бортового устройства, если приемник ГНСС установлен как внешнее устройство относительно БУ		03
3.5	Модуль шифрования и стандартизованные параметры домена		CSM_48, CSM_50
4.	Испытания на воздействие внешних факторов		
4.1	Температура	Проверка функциональности следующими средствами: Испытание в соответствии с ISO 16750-4, глава 5.1.1.2: рабочие испытания при низкой температуре (72 ч при –20 °С) Данное испытание строится на основе стандарта IEC 60068-2-1: Испытание на воздействие внешних факторов — Часть 2-1: Испытания — Испытание А: холод Испытания в соответствии с ISO 16750-4: Глава 5.1.2.2: рабочие испытания при высокой температуре (72 ч при 70 °С) Данное испытание строится на основе стандарта IEC 60068-2-2: Базовые процедуры испытаний на воздействие внешних факторов. Часть 2: испытания. Часть В: сухое тепло Испытания в соответствии с ISO 16750-4: Глава 5.3.2: быстрая смена температуры с указанной	213

№	Испытание	Описание	Соответствующие требования
		<p>продолжительностью перехода (-20 °C/70 °C, 20 циклов, время выдержки 1 ч при каждой температуре) Возможно проведение сокращенной серии испытаний (из числа указанных в разделе 3 настоящей таблицы) при низкой и высокой температурах, а также на протяжении температурных циклов</p>	
4.2	Влажность	<p>Проверка способности бортового устройства выдерживать циклические колебания температуры во влажной среде согласно стандарту IEC 60068-2-30, испытание Db: шесть 24-часовых циклов с изменением температуры от +25 °C до +55 °C в каждом цикле и относительной влажностью воздуха, равной 97 % при +25 °C и эквивалентной 93 % при +55 °C</p>	214
4.3	Механические испытания	<p>Синусоидальные вибрации</p> <p>Проверка способности бортового устройства выдерживать синусоидальные вибрации со следующими характеристиками:</p> <p> постоянное вытеснение в диапазоне 5–11 Гц: пик — 10 мм;</p> <p> постоянное ускорение в диапазоне 11-300 Гц: 5 g.</p> <p>Соответствие данному требованию проверяется в соответствии со стандартом IEC 60068-2-6, испытание Fc минимальной продолжительностью 3 x 12 часов (по 12 часов на каждую ось)</p> <p>ISO 16750-3 не предусматривает проведение испытаний на синусоидальные вибрации в случае транспортного средства с отдельной кабиной</p> <p>Произвольные колебания</p> <p>Испытания в соответствии с ISO 16750-3: Глава 4.1.2.8: Испытание VIII: транспортное средство индивидуального пользования с отдельной кабиной</p> <p>Испытания на произвольные колебания, 10...2000 Гц, вертикальные RMS 21,3 м/с², продольные RMS 11,8 м/с², поперечные RMS 13,1 м/с², 3 оси, 32 ч на ось, включая температурный цикл -20...70 °C</p> <p>Данные испытания строятся на основе стандарта IEC 60068-2-64: Испытание на воздействие внешних факторов. Часть 2-64: испытания. Испытание Fh: вибрация, широкий диапазон частот и руководство</p> <p>Ударные нагрузки</p> <p>Механический удар по полусинусоиде 3 g в соответствии с ISO 16750</p> <p>Вышеуказанные испытания проводят с использованием разных образцов типа устройства, подвергаемого испытанию</p>	219
4.4	Защита от попадания воды и посторонних предметов	<p>Испытания в соответствии с ISO 20653: Транспортные средства дорожные. Степень защиты (код ИП). Защита электрооборудования от посторонних предметов, воды и доступа (параметры не меняются)</p>	220, 221

№	Испытание	Описание	Соответствующие требования
4.5	Защита от перегрузок по напряжению	Проверка способности бортового устройства выдерживать следующее напряжение в цепи питания: Вариант на 24 В: 34 В при +40 °С 1 час Вариант на 12 В: 17 В при +40 °С 1 час (ISO 16750-2, глава 4.3)	216
4.6	Защита от несоблюдения полярности	Проверка способности бортового устройства выдерживать подключение к источнику питания противоположной полярности: (ISO 16750-2, глава 4.7)	216
4.7	Защита от короткого замыкания	Проверка защищенности сигналов ввода/вывода от короткого замыкания на источник питания и на массу (ISO 16750-2, глава 4.10)	216
5	Испытания на ЭМС		
5.1	Излучения и электромагнитная защищенность	Соответствие Правилам ЕЭК № 10	218
5.2	Электростатический разряд	Соответствие ISO 10605 :2008 + Техническая поправка: 2010 + AMD1 :2014: +/-4 кВ для контакта и +/-8 кВ для расхода воздуха	218
5.3	Подверженность кондуктивным помехам в системе питания	Варианты на 24 В: в соответствии с ISO 7637-2 + Правила ЕЭК № 10, пересмотр 3 : импульс 1a: $V_s = -450 \text{ В}$ $R_i = 50 \text{ Ом}$ импульс 2a: $V_s = +37 \text{ В}$ $R_i = 2 \text{ Ом}$ импульс 2b: $V_s = +20 \text{ В}$ $R_i = 0,05 \text{ Ом}$ импульс 3a: $V_s = -150 \text{ В}$ $R_i = 50 \text{ Ом}$ импульс 3b: $V_s = +150 \text{ В}$ $R_i = 50 \text{ Ом}$ импульс 4: $V_s = -16 \text{ В}$ $V_a = -12 \text{ В}$ $t_6 = 100 \text{ мс}$ импульс 5: $V_s = +120 \text{ В}$ $R_i = 2,2 \text{ Ом}$ $t_d = 250 \text{ мс}$ Варианты на 12В: соответствие с ISO 7637-1 + Правила ЕЭК № 10, пересмотр 3: импульс 1: $V_s = -75 \text{ В}$ $R_i = 10 \text{ Ом}$ импульс 2a: $V_s = +37 \text{ В}$ $R_i = 2 \text{ Ом}$ импульс 2b: $V_s = +10 \text{ В}$ $R_i = 0,05 \text{ Ом}$ импульс 3a: $V_s = -112 \text{ В}$ $R_i = 50 \text{ Ом}$ импульс 3b: $V_s = +75 \text{ В}$ $R_i = 50 \text{ Ом}$ импульс 4: $V_s = -6 \text{ В}$ $V_a = -5 \text{ В}$ $t_6 = 15 \text{ мс}$ импульс 5: $V_s = +65 \text{ В}$ $R_i = 3 \text{ Ом}$ $t_d = 100 \text{ мс}$ Импульс 5 используется только при испытании бортовых устройств для установки на транспортных средствах, не оборудованных единой внешней защитой от сброса нагрузки генератора По поводу предложения о сбросе нагрузки генератора см. ISO 16750-2, 4-й пересмотр, глава 4.6.4	218

6. Испытания внешнего устройства удаленной связи

№	Испытание	Описание	Соответствующие требования
1.	Административная проверка		
1.1	Документация	Правильность документации	
2.	Визуальный осмотр		
2.1	Соответствие документации		
2.2	Идентификация/маркировка		225, 226
2.3	Материалы		219–223
3.	Функциональные испытания		
3.1	Удаленный обмен данными в порядке проведения целевых проверок на дорогах		4, 197–199
3.2	Регистрация и хранения в блоке памяти данных		91
3.3	Обмен данными с бортовым устройством		Подраздел 14, DCS_66–DCS_70, DCS_71–DCS_76
4.	Испытания на воздействие внешних факторов		
4.1	Температура	Проверка функциональности посредством: Испытания в соответствии с ISO 16750-4, глава 5.1.1.2: рабочие испытания при низкой температуре (72 ч при –20 °С) Данные испытания строятся на основе IEC 60068-2-1: Испытания на воздействие внешних факторов. Часть 2-1: испытания. Испытание А: холод Испытания в соответствии со стандартом ISO 16750-4: Глава 5.1.2.2: рабочие испытания при высокой температуре (72 ч при 70 °С) Данные испытания строятся на основе стандарта IEC 60068-2-2: Базовые процедуры испытаний на воздействие внешних факторов. Часть 2: испытания. Часть В: сухое тепло Испытания в соответствии с ISO 16750-4: Глава 5.3.2: быстрая смена температуры с указанной продолжительностью перехода (–20 °С/70 °С, 20 циклов, время выдержки 2 ч при каждой температуре) Возможно проведение сокращенной серии испытаний (из числа указанных в разделе 3 настоящей таблицы) при более низкой и высокой температурах, а также на протяжении предусмотренных температурных циклов	213
4.2	Защита от попадания воды и посторонних предметов	Испытания в соответствии с ISO 20653: Дорожные транспортные средства. Степень защиты (код IP). Защита электрооборудования от посторонних предметов, воды и доступа (целевое значение IP40)	220, 221
5	Испытания на ЭМС		
5.1	Излучения и подверженность	В соответствии с Правилами ЕЭК № 10	218

№	Испытание	Описание	Соответствующие требования
5.2	Электростатический разряд	В соответствии с ISO 10605 :2008 + Техническая поправка: 2010 + AMD1: 2014: +/-4 кВ для контакта и +/-8 кВ для расхода воздуха	218
5.3	Подверженность кондуктивным помехам в системе питания	<p>Варианты на 24 В: в соответствии с ISO 7637-2 + Правила ЕЭК № 10, пересмотр 3:</p> <p>импульс 1a: $V_s = -450$ В $R_i = 50$ Ом импульс 2a: $V_s = +37$ В $R_i = 2$ Ом импульс 2b: $V_s = +20$ В $R_i = 0,05$ Ом импульс 3a: $V_s = -150$ В $R_i = 50$ Ом импульс 3b: $V_s = +150$ В $R_i = 50$ Ом импульс 4: $V_s = -16$ В $V_a = -12$ В $t_6 = 100$ мс импульс 5: $V_s = +120$ В $R_i = 2,2$ Ом $t_d = 250$ мс</p> <p>Варианты на 12 В: в соответствии с ISO 7637-1 + Правила ЕЭК № 10, пересмотр 3:</p> <p>импульс 1: $V_s = -75$ В $R_i = 10$ Ом импульс 2a: $V_s = +37$ В $R_i = 2$ Ом импульс 2b: $V_s = +10$ В $R_i = 0,05$ Ом импульс 3a: $V_s = -112$ В $R_i = 50$ Ом импульс 3b: $V_s = +75$ В $R_i = 50$ Ом импульс 4: $V_s = -6$ В $V_a = -5$ В $t_6 = 15$ мс импульс 5: $V_s = +65$ В $R_i = 3$ Ом $t_d = 100$ мс</p> <p>Импульс 5 используется только при испытании бортовых устройств для установки на транспортных средствах, не оборудованных единой внешней защитой от сброса нагрузки генератора</p> <p>По поводу предложения о сбросе нагрузки генератора см. ISO 16750-2, 4-е издание, глава 4.6.4</p>	218

7. Функциональные испытания бумаги

№	Испытание	Описание	Соответствующие требования
1.	Административная проверка		
1.1	Документация	Правильность документации	
2	Общие испытания		
2.1	Число символов в строке	Визуальный осмотр распечаток	172
2.2	Минимальный размер символов	Визуальный осмотр распечаток и символов	173
2.3	Поддерживаемый набор символов	Принтер поддерживает знаки, указанные в главе 4 «Наборы знаков» приложения в подразделе 1 добавления	174
2.4	Определение распечаток	Проверка утверждения типа тахографа и визуальный осмотр распечаток	174
2.5	Читаемость и идентификационные данные распечаток	Проверка распечаток по отчетам испытаний и тестовым протоколам изготовителя Все номера утверждения тахографов, с которыми может использоваться печатная бумага, указываются на бумаге	175, 177, 178
2.6	Добавление рукописных заметок	Визуальный осмотр: Поле для подписи водителя предусмотрено Поля для других дополнительных рукописных записей предусмотрены	180

№	Испытание	Описание	Соответствующие требования
2.7	Дополнительные сведения о лицевых сторонах бумаги	Лицевая и оборотная стороны бумаги могут характеризоваться различными дополнительными данными и информацией Такие дополнительные сведения и информация не должны влиять на читаемость распечаток Визуальный осмотр	177, 178
3	Испытания на сохранность		
3.1	Сухое тепло	Предварительное кондиционирование: 16 часов при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности Тестовая среда: 72 часа при $+70\text{ °C} \pm 2\text{ °C}$ Восстановление: 16 часов при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности	176, 178 IES 60068-2-2-Bb
2.2	Влажное тепло	Предварительное кондиционирование: 16 часов при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности Тестовая среда: 144 часа при $+55\text{ °C} \pm 2\text{ °C}$ и $93\% \pm 3\%$ относительной влажности Восстановление: 16 часов при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности	176, 178 IES 60068-2-78-Cab
4	Испытания бумаги во время работы		
4.1	Влагостойкий фон (бумага без печати)	Предварительное кондиционирование: 16 часов при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности Тестовая среда: 144 часа при $+55\text{ °C} \pm 2\text{ °C}$ и $93\% \pm 3\%$ относительной влажности Восстановление: 16 часов при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности	176, 178 CEI 60068-2-78-Cab
4.2	Печатные свойства	Предварительное кондиционирование: 24 часа при $+40\text{ °C} \pm 2\text{ °C}/93\% \pm 3\%$ относительной влажности Тестовая среда: распечатка при $+23\text{ °C} \pm 2\text{ °C}$ Восстановление: 16 часов при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности	176, 178
4.3	Теплостойкость	Предварительное кондиционирование: 16 часов при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности Тестовая среда: 2 часа при $+70\text{ °C} \pm 2\text{ °C}$, сухое тепло Восстановление: 16 часов при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности	176, 178 CEI 60068-2-2-Bb
4.4	Стойкость к низким температурам	Предварительное кондиционирование: 16 часов при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности Тестовая среда: 24 часа при $20\text{ °C} \pm 3\text{ °C}$, сухой холод Восстановление: 16 часов при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности	176, 178 ISO 60068-2-1-Ab
4.5	Светостойкость	Предварительное кондиционирование: 16 часов при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности Тестовая среда: 100 часов при освещении 5 000 лк при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности Восстановление: 16 часов при $+23\text{ °C} \pm 2\text{ °C}/55\% \pm 3\%$ относительной влажности	176, 178

Критерии читаемости для испытаний 3.х и 4.х:

Читаемость распечаток обеспечивается, если оптическая плотность соответствует следующим пределам:

печатные символы: мин. 1,0;

фон (бумага без печати): макс. 0,2.

Оптическая плотность получаемых распечаток измеряется в соответствии с DIN EN ISO 534.

Распечатки не меняются в размерах и остаются хорошо читаемыми.

8. Испытания на эксплуатационную совместимость

№	Испытание	Описание
8.1 Испытания на эксплуатационную совместимость		
1	Взаимная аутентификация	Проверка нормального выполнения процедур взаимной аутентификации бортового устройства и карточки тахографа
2	Проверка записи/ считывания данных	Отработка типового сценария работы бортового устройства. Сценарий выбирается с учетом типа тестируемой карточки и включает в себя операции по записи данных в максимально возможном числе элементарных файлов на карточке Загрузка данных с бортового устройства для проверки наличия и правильности всех соответствующих записей данных Загрузка данных с карточки для проверки наличия и правильности всех соответствующих записей данных Проверка по ежедневным распечаткам читаемости всех соответствующих записей данных
8.2 Испытания на эксплуатационную совместимость между бортовыми устройствами и датчиками движения		
1	Сопряжение	Проверка нормальной работы соединения бортового устройства и датчика движения
2	Рабочие испытания	Отработка типового сценария функционирования датчика движения. Сценарий включает в себя нормальную деятельность и создает как можно больше событий или неисправностей Загрузка данных с бортового устройства для проверки наличия и правильности всех соответствующих записей данных Загрузка данных с карточки для проверки наличия и правильности всех соответствующих записей данных Проверка по ежедневным распечаткам читаемости всех соответствующих записей данных
8.3 Испытания на эксплуатационную совместимость между бортовыми устройствами и внешними устройствами ГНСС (если применимо)		
1	Взаимная аутентификация	Проверка нормального выполнения процедур взаимной аутентификации (сопряжения) бортового устройства и внешнего модуля ГНСС.
2	Рабочие испытания	Отработка типового сценария функционирования внешней ГНСС. Сценарий включает в себя нормальную деятельность и создает как можно больше событий или неисправностей Загрузка данных с бортового устройства для проверки наличия и правильности всех соответствующих записей данных Загрузка данных с карточки для проверки наличия и правильности всех соответствующих записей данных Проверка по ежедневным распечаткам читаемости всех соответствующих записей данных

9. Тесты OSNMA

9.1 Введение

В настоящей главе описаны тесты, имеющие целью подтвердить правильную работу функции OSNMA в приемнике ГНСС. Поскольку аутентификация спутникового сигнала осуществляется исключительно приемником ГНСС независимо от любого другого компонента тахографа, испытания, изложенные в настоящей главе, могут проводиться на приемнике ГНСС как на отдельном элементе. В этом случае изготовитель тахографа представляет органам по официальному утверждению типа соответствующий отчет, содержащий детальные данные о разработке и результатах испытаний, ответственность за которые возлагаются на изготовителя приемника ГНСС.

9.2 Применимые условия

- Критерии «прохождения/непрохождения», определенные в испытаниях OSNMA, считаются действительными только в случае установленных условий испытаний.
- Эти критерии могут быть пересмотрены в момент извещения о намерении ввести в действие систему OSNMA и рассмотрении соответствующих обязательств по ее выполнению.

9.3 Определения и сокращения

9.3.1 Определения

Введение в действие ГНСС в холодном/теплом/горячем состоянии: речь идет о начальном состоянии приемника ГНСС с учетом наличия времени (Т), каталога зафиксированных событий (А) и координат небесных ориентиров (Е), а также местоположения (Р):

- Введение в действие ГНСС: нет
- Введение в действие ГНСС в теплом состоянии: Т, А, Р
- Введение в действие ГНСС в горячем состоянии: Т, А, Е, Р

Введение в действие функции OSNMA в холодном/теплом/горячем состоянии: речь идет о начальных условиях введения в действие функции OSNMA с учетом наличия открытого ключа (Р) и информации DSM-KROOT (К) (как это определено в руководстве по приемнику OSNMA, упомянутом в подразделе 12 добавления):

- Введение в действие OSNMA в холодном состоянии: нет
- Введение в действие OSNMA в теплом состоянии: Р
- Введение в действие OSNMA в горячем состоянии: Р, К

9.3.2 Сокращения

АДКД	Данные аутентификации и задержка ключа
DSM-KROOT	Сообщение с цифровой подписью KROOT
ГНСС	Глобальная навигационная спутниковая система
KROOT	Корневой ключ ключевой последовательности ТЕСЛА
MAC	Код аутентификации сообщений
HMAC	Количество блоков MAC и ключей (в расчете на 30 секунд)

OSNMA	Открытая функция аутентификации навигационных сообщений «Галилей»
SLMAC	Низкоскоростной MAC
TECLA	Эффективная аутентификация, устойчивая к потерям потока с привязкой ко времени (протокол, используемый в OCHMA)

9.4 Оборудование для генерации сигналов ГНСС

Генерация сигналов ГНСС, необходимых для работы ГНСС, может осуществляться с помощью сети генераторов сигналов станций управления ГНСС и задаваемых пользователем параметров навигационных сообщений, а также времени начала и продолжительности сценария. В качестве альтернативы можно использовать повторитель радиочастотных сигналов, способный воспроизводить выборки сигналов ГНСС из имеющихся файлов. Типичная глубина в битах и частота дискретизации составляют соответственно 4 бита I/Q и 10 МГц.

Предполагается, что приемник ГНСС оснащен интерфейсами, позволяющими передавать команду на очистку памяти приемника (для самостоятельного стирания открытого ключа, KROOT, информации о часах, информации о местоположении, координат небесных ориентиров и каталога зафиксированных событий), в целях отображения в приемнике местного времени в соответствии с требованием проверки времени OCHMA и загрузки криптографической информации. Эти команды могут быть ограничены в целях тестирования и поэтому могут быть недоступны для номинальной работы приемника.

9.5 Условия испытаний

9.5.1 Состояния ГНСС

Моделируемые или воспроизводимые сигналы ГНСС должны обладать следующими характеристиками:

- сценарий статического пользовательского приемника;
- частота E1/L1;
- не менее 4 передающих спутников OSNMA с углом возвышения более 5°;
- продолжительность в зависимости от требований применительно к каждому испытанию;
- постоянные навигационные координаты небесных ориентиров со спутников во время теста.

9.5.2 Состояния OSNMA

Сообщение OSNMA, передаваемое в радиочастотном сигнале, должно иметь следующие характеристики:

- сообщение HKROOT со статусом OSNMA, передаваемое в режиме «Operational» (работа) или «Test» (тест), и фиксированным ключем DSM-KROOT из 8 блоков для действующей цепочки;
- не менее 4 передающих спутников, OCHMA;
- сообщение MACK с одним блоком MACK (т. е. NMACK=1) и, как минимум, одним ADKD = 0 и одним ADKD = 12 в расчете на спутник и блок MACK;
- размер метки составляет 40 битов;

- минимальная эквивалентная длина метки в соответствии с требованиями Руководства по приемникам OSNMA (в настоящее время 80 битов).

За исключением случаев, когда это указано, внутренняя установка времени приемника должна быть известна с достаточной точностью и правильно согласована с моделируемым временем. Это гарантирует, что требование начальной синхронизации времени OSNMA выполняется для каждого условия испытания, т. е. номинальная синхронизация для всех тестов, кроме теста SLMAC. Более подробную информацию об инициализации времени см. Руководство по приемнику OSNMA.

9.6 Спецификация тестов

№	Тест	Описание	Соответствующие требования
1.	Административная проверка		
1.1	Документация	Правильность документации	
2	Общие тесты		
2.1	Введение в действие OSNMA в горячем состоянии	<p>Цель: убедиться в том, что приемник ГНСС вычисляет местоположение с помощью системы OSNMA после введения ее в действие в горячем состоянии.</p> <p>Процедура: приемник GNSS подключается в горячем состоянии к системе GNSS и OSNMA и принимает сигналы видимых спутников; приемник проверяет аутентичность навигационных данных с помощью OSNMA (ADKD = 0) и выдает местоположение с проверенными данными.</p> <p>Критерии прохождения/непрохождения: приемник рассчитывает аутентифицированную фиксацию положения в течение 160 секунд.</p>	Добавление 12, GNS_3b
2.2	Введение в действие OSNMA в теплом состоянии	<p>Цель: убедиться в том, что приемник ГНСС вычисляет местоположение с помощью OSNMA после введения ее в действие в теплом состоянии.</p> <p>Процедура: перед началом теста координаты небесных ориентиров и данные KROOT должны быть удалены из памяти приемника ГНСС в целях принудительного введения в действие ГНСС и OSNMA в теплом состоянии.</p> <p>Приемник ГНСС начинает работать и принимать сигналы видимых спутников.</p> <p>Сообщение DSM-KROOT получено и проверяется.</p> <p>Приемник проверяет аутентичность навигационных данных с помощью OSNMA (ADKD = 0) и выдает местоположение с подтвержденными данными.</p> <p>Критерии прохождения/непрохождения: приемник рассчитывает аутентифицированную фиксацию местоположения в течение 430 секунд.</p>	Добавление 12, GNS_3b

№	Тест	Описание	Соответствующие требования
2.3	Введение в действие OSNMA с помощью SLMAC	<p>Цель: убедиться в том, что приемник ГНСС вычисляет положение с помощью ОСНМА после введения в действие этой системы в теплом состоянии в течение времени, необходимого для инициализации режима SLMAC, как определено в руководстве по приемнику OSNMA.</p> <p>Процедура: внутренняя конфигурация времени приемника должна быть произведена таким образом, чтобы иметь начальную временную неопределенность в пределах 2–2,5 минуты с целью активировать, как предусмотрено в Руководстве по приемникам ОСНМА, низкоскоростной режим «Slow MAC».</p> <p>Перед началом теста координаты небесных ориентиров и данные KROOT должны быть удалены из памяти приемника ГНСС в целях принудительного введения в действие ГНСС и ОСНМА в теплом состоянии.</p> <p>Приемник ГНСС начинает работать и принимать сигналы видимых спутников.</p> <p>Сообщение DSM-KROOT получено и проверяется.</p> <p>Приемник проверяет аутентичность навигационных данных с помощью только «Slow MAC» ОСНМА (ADKD = 12) и выдает местоположение с аутентифицированными данными.</p> <p>Критерии прохождения/непрохождения: приемник рассчитывает аутентифицированную фиксацию местоположения в течение 730 секунд.</p>	Добавление 12, GNS_3b
2.4	Введение в действие ОСНМА в горячем состоянии методом воспроизведенного сигнала	<p>Цель: убедиться в том, что приемник ГНСС обнаруживает воспроизведенный сигнал.</p> <p>Процедура:</p> <p>приемник ГНСС подключается в горячем состоянии к системе ГНСС и OSNMA и принимает сигналы видимых спутников.</p> <p>приемник проверяет аутентичность навигационных данных с помощью ОСНМА (ADKD = 0) и выдает местоположение с аутентифицированными данными.</p> <p>Как только приемник выдает PVT-решение с аутентифицированными данными, он отключается.</p> <p>Воспроизведенный сигнал моделируется по отношению к предыдущему сигналу с задержкой порядка 40 секунд, после чего включается приемник.</p> <p>Приемник обнаруживает, что системное время, установленное по временному пространственному сигналу, и местное время не соответствуют требованию синхронизации, и прекращает обработку данных ОСНМА, как определено в Руководстве по приемнику ОСНМА.</p> <p>Критерии прохождения/непрохождения: приемник обнаруживает повтор и не вычисляет аутентифицированную действительную позицию с момента начала повтора до окончания теста.</p>	Добавление 12, GNS_3b

№	Тест	Описание	Соответствующие требования
2.5	Введение в действие OSNMA в горячем состоянии с ложными данными	<p>Цель: убедиться в том, что OSNMA обнаруживает ложные данные.</p> <p>Процедура: приемник GNSS запускается в горячем состоянии GNSS и OSNMA.</p> <p>Приемник ГНСС должен быть способен принимать сигнал всех видимых спутников и проверять аутентичность их навигационных сообщений от OSNMA.</p> <p>По крайней мере один бит данных эфемерид, предоставленных каждым спутником, не соответствует оригинальным и аутентифицированным данным, но сообщение I/NAV должно быть когерентным, включая CRC.</p> <p>Критерии прохождения/непрохождения: приемник обнаруживает ложные данные в течение 160 секунд и не вычисляет аутентифицированное действительное местоположение до конца теста.</p>	Добавление 12, GNS_3b

Подраздел 10

Требования в области безопасности

В настоящем ~~приложении~~ **подразделе** изложены требования в области безопасности ИТ применительно к компонентам систем смарт-тахографов (тахографов второго поколения).

SEC_001 Защита нижеперечисленных компонентов систем смарт-тахографов подлежит сертификации в соответствии со схемой общих критериев:

- бортовое устройство;
- карточка тахографа;
- датчик движения;
- внешнее устройство ГНСС.

SEC_002 Минимальные требования в области безопасности ИТ, которым должен соответствовать каждый компонент, подлежащий сертификации в части системы безопасности, определяются в характеристиках защиты того или иного компонента в соответствии со схемой общих критериев.

SEC_003 ~~Европейская комиссия заботится о том, чтобы четыре~~ Следующие нижеперечисленные наборы характеристик защиты, **соответствующие не-настоящему приложению подразделу добавления должны быть** ~~были~~ профинансированы, разработаны и утверждены соответствующими государственными сертификационными органами по безопасности ИТ на уровне Совместной рабочей группы по интерпретации (J1WG), поддерживающей принцип взаимного признания сертификатов на основании Европейского соглашения SOGIS-MRA (соглашение о взаимном признании сертификатов оценки безопасности информационных технологий) и надлежащим образом зарегистрированы:

- Схема защиты бортового устройства;
- Схема защиты карточек тахографа;
- Схема защиты датчика движения;
- Схема защиты внешнего устройства ГНСС.

Схема защиты бортового устройства охватывает случаи, когда БУ должен использоваться вместе с внешним устройством ГНСС или без него. В первом случае требования к безопасности внешнего устройства ГНСС изложены в специальной схеме защиты.

SEC_004 Изготовители компонентов по мере необходимости уточняют и дополняют соответствующие схемы защиты компонентов, не меняя или не исключая установленные спецификации, регламентирующие угрозы, задачи, процедуры и функции обеспечения безопасности, в порядке достижения целевого уровня защиты, которого они будут придерживаться в своей работе, ориентированной на сертификацию данного компонента.

SEC_005 В процессе оценки должно быть подтверждено строгое соответствие такого целевого уровня защиты соответствующему набору характеристик защиты.

SEC_006 Уровень обеспечения соблюдения каждого набора характеристик защиты соответствует норме EAL4, подкрепленной компонентами обеспечения защиты ATE_DPT.2 и AVA_VAN.5.

Подраздел 11

Общие механизмы безопасности

Содержание

Стр.

	Преамбула	449
ЧАСТЬ А	СИСТЕМА ТАХОГРАФОВ ПЕРВОГО ПОКОЛЕНИЯ	449
1.	Введение	449
1.1	Справочные материалы	449
1.2	Условные обозначения и сокращение терминов	450
2.	Криптографические системы и алгоритмы	451
2.1	Криптографические системы	451
2.2	Криптографические алгоритмы	452
2.2.1	Алгоритм RSA	452
2.2.2	Алгоритм хеширования	452
2.2.3	Алгоритм шифрования данных	452
3.	Ключи и сертификаты	452
3.1	Генерирование и рассылка ключей	452
3.1.1	Генерация и рассылка ключей RSA	452
3.1.2	Испытательные ключи RSA	453
3.1.3	Ключи датчика движения	454
3.1.4	Генерация и рассылка сеансовых ключей T-DES	454
3.2	Ключи	454
3.3	Сертификаты	455
3.3.1	Содержание сертификатов	455
3.3.2	Выдаваемые сертификаты	457
3.3.3	Проверка и расшифровка сертификатов	457
4.	Механизм взаимной аутентификации	458
5.	Механизмы обеспечения конфиденциальности, целостности и аутентификации данных в процессе их передачи между БУ и карточками	461
5.1	Защищенный обмен сообщениями	461
5.2	Обработка ошибок при криптозащищенном обмене сообщениями	462
5.3	Алгоритм расчета криптографических контрольных сумм	463
5.4	Алгоритм расчета криптограмм для защиты конфиденциальности Dos	463
6.	Механизмы цифровой подписи при загрузке данных	464
6.1	Генерация подписей	464
6.2	Проверка подписей	464

ЧАСТЬ В	СИТЕМА ТАХОГРАФОВ ПЕРВОГО ПОКОЛЕНИЯ	466
7.	Введение	466
7.1	Справочные материалы	466
7.2	Условные обозначения и сокращения	467
7.3	Определения	468
8.	Криптографические системы и алгоритмы	468
8.1	Криптографические системы	468
8.2	Криптографические алгоритмы	469
8.2.1	Симметричные алгоритмы	469
8.2.2	Асимметричные алгоритмы и стандартизованные параметры домена	469
8.2.3	Алгоритмы хеширования	470
8.2.4	Последовательности шифров	470
9.	Ключи и сертификаты	471
9.1	Асимметричные пары ключей и сертификаты открытых ключей	471
9.1.1	Общие положения	471
9.1.2	Корневой уровень	471
9.1.3	Уровень Договаривающейся стороны	472
9.1.4	Аппаратный уровень: бортовые устройства	473
9.1.5	Аппаратный уровень: карточки тахографа	475
9.1.6	Аппаратный уровень: внешние устройства ГНСС	476
9.1.7	Обзор: замена сертификата	477
9.2	Симметричные ключи	479
9.2.1	Ключи для обеспечения связи между БУ и датчиком движения	479
9.2.2	Ключи для обеспечения безопасности связи DSRC	483
9.3	Сертификаты	487
9.3.1	Общие положения	487
9.3.2	Содержание сертификатов	487
9.3.3	Запрос на сертификаты	489
10.	Взаимная аутентификация и безопасный обмен сообщениями с карточкой БУ	490
10.1	Общие положения	490
10.2	Взаимная проверка последовательности сертификата	491
10.2.1	Проверка последовательности сертификата карточки БУ	491
10.2.2	Проверка последовательности сертификатов в БУ карточкой	493
10.3	Аутентификация БУ	496
10.4	Аутентификация микросхемы и согласование сеансовых ключей	498
10.5	Защищенный обмен сообщениями	500
10.5.1	Общие положения	500
10.5.2	Структура защищенного сообщения	500
10.5.3	Отмена сеанса защищенного обмена сообщениями	503

11.	Соединение, взаимная аутентификация и защищенный обмен сообщениями между БУ и внешним устройством ГНСС	505
11.1	Общие положения	505
11.2	Соединение БУ и внешнего устройства ГНСС	505
11.3	Взаимная проверка последовательности сертификатов	506
11.3.1	Общие положения	506
11.3.2	Во время соединения БУ и EGF	506
11.3.3	Во время нормальной эксплуатации	507
11.4	Аутентификация БУ, аутентификация микросхемы и согласование сеансовых ключей	508
11.5	Защищенный обмен сообщениями	508
12.	Соединение и связь между БУ и датчиком движения	509
12.1	Общие положения	509
12.2	Соединение БУ и датчика движения с использованием различных поколений ключей	509
12.3	Соединение и связь между БУ и датчиком движения с использованием AES	510
12.4	Соединение БУ и датчика движения с использованием различных поколений оборудования	512
13.	Защита удаленной связи по DSRC	512
13.1	Общие положения	512
13.2	Шифрование данных тахографа и генерирование MAC	513
13.3	Проверка и расшифровка данных тахографа	514
14.	Подписание загружаемых данных и проверка подписей	515
14.1	Общие положения	515
14.2	Генерация подписей	515
14.3	Проверка подписей	516

Преамбула

В этом ~~приложении~~ **подразделе** указаны механизмы безопасности, обеспечивающие

- взаимную аутентификацию между различными компонентами системы тахографов;
- конфиденциальность, целостность, подлинность и/или невозможность отказа от данных, передаваемых между различными компонентами системы тахографов или загружаемых на внешние носители.

~~Данное Приложение~~ **Данный подраздел добавления** состоит из двух частей. В части А содержится описание механизмов безопасности для системы тахографов первого поколения (цифрового тахографа). В части В содержится описание механизмов безопасности для системы тахографов второго поколения (смарт-тахографа).

Механизмы, представленные в части А настоящего ~~приложения~~ **подраздела**, применяются в том случае, если хотя бы один из компонентов системы тахографа, задействованный в процессе взаимной аутентификации и/или передаче данных, принадлежит к первому поколению.

Механизмы, представленные в части В настоящего приложения подраздела, применяются в том случае, если хотя бы один из компонентов системы тахографа, задействованный во взаимной аутентификации и/или передаче данных, принадлежит ко второму поколению.

В ~~приложении~~ **подразделе** 15 представлена более подробная информация об использовании компонентов первого поколения в сочетании с компонентами второго поколения.

ЧАСТЬ А СИСТЕМА ТАХОГРАФОВ ПЕРВОГО ПОКОЛЕНИЯ

1. Введение

1.1 Справочные материалы

В данном ~~приложении~~ **подразделе** используются следующие ссылки:

SHA-1	Национальный институт стандартов и технологии (НИСТ). <i>FIPS Publication 180-1: Secure Hash Standard</i> . April 1995. <i>Публикация FIPS 180-1: Стандарт безопасного хеширования</i> . Апрель 1995 года.
PKCS1	Лаборатории RSA. PKCS # 1: стандарт шифрования RSA. Версия 2.0. Октябрь 1998 года.
TDES	Национальный институт стандартов и технологий (НИСТ). <i>Публикация FIPS 46-3: стандарт шифрования данных</i> . Проект 1999 года.
TDES-OP	ANSI X9.52, Рабочие режимы алгоритма тройного шифрования данных. 1998 год.
ISO/IEC 7816-4	Информационные технологии. Карточки идентификационные — карточки на интегральных микросхемах с контактами — Часть 4: межотраслевые команды обмена данными. Первое издание: 1995 + Поправка 1: 1997 год.
ISO/IEC 7816-6	Информационные технологии — Карточки идентификационные — Карточки на интегральных микросхемах с контактами — Часть 6:

	Межотраслевые элементы данных. 1-е издание: 1996 + поправка 1: 1998 год.
ISO/IEC 7816-8	Информационные технологии. Карточки идентификационные — карточки на интегральных микросхемах с контактами — Часть 8: межотраслевые команды, связанные с безопасностью. Первое издание: 1998 год.
ISO/IEC 9796-2	Техника обеспечения безопасности. Схемы цифровой подписи с восстановлением сообщений. Часть 2: механизмы с использованием хэш-функции. Первое издание: 1997 год.
ISO/IEC 9798-3	Информационные технологии — Методы обеспечения безопасности — Механизмы аутентификации сущностей — Часть 3: Аутентификация сущностей с использованием алгоритма открытого ключа. 2-е издание, 1998 год.
ISO 1684 4 3	Транспортные средства дорожные. Системы тахографов. Часть 3: интерфейс датчика движения.

1.2 Условные обозначения и сокращение терминов

В данном ~~приложении~~ **подразделе** используются следующие обозначения и сокращения:

(K _a , K _b , K _c)	набор ключей, используемый в алгоритме тройного шифрования данных
CA	сертификационный орган
CAR	ссылка на сертификационный орган
CC	криптографическая контрольная сумма
CG	криптограмма
CH	заголовок команды
CHA	полномочия держателя сертификата
CPЖД	справочный номер держателя сертификата
D()	расшифровка при помощи DES
DE	элемент данных
DO	объект данных
d	закрытый ключ в криптосистеме RSA, закрытая экспонента
e	открытый ключ в криптосистеме RSA, открытая экспонента
E()	шифрование по системе DES
EQT	оборудование
<i>Hash()</i>	значение хэш-функции, выходные данные <i>хеширования</i>
<i>Хеш</i>	хэш-функция
KID	ключевой идентификатор
Km	ключ TDES. ключ верхнего уровня, определение которого содержится в ISO 16844-3
Km _{VU}	ключ TDES, вводимый в бортовые устройства
Km _{WC}	ключ TDES, вводимый в бортовые карточки
<i>m</i>	репрезентативный параметр сообщения — целое число от 0 до n-1
<i>n</i>	ключ криптосистемы RSA, модуль

PB	байты заполнения
PI	байт индикации заполнения (используется в криптограммах для обеспечения конфиденциальности объектов данных)
PV	простое значение
<i>s</i>	репрезентативный параметр сообщения, целое число от 0 до $n-1$
ЦИО	счетчик исходящих сообщений
SM	защищенный обмен сообщениями
TCBC	режим сцепления криптоблоков при тройном шифровании данных TDEA
TDEA	тройной алгоритм шифрования данных
ПДК	значение длины метки
VU (БУ)	бортовое устройство
X.C	сертификат пользователя X, выданный сертификационным органом
X.CA	сертификационный орган пользователя X
X.CA.PK ◦ X.C	операция по расшифровке сертификата в целях извлечения открытого ключа. Это — инфиксный оператор, левый операнд которого является открытым ключом сертификационного органа, а правый операнд — сертификатом, выданным этим сертификационным органом. Результатом этой операции является открытый ключ пользователя X, сертификатом которого является операнд
X.PK	открытый ключ пользователя X в криптосистеме RSA
X.PK[I]	шифрование информации I по системе RSA с использованием открытого ключа пользователя X
X.SK	открытый ключ пользователя X в криптосистеме RSA
X.SK[I]	шифрование информации I по системе RSA с использованием открытого ключа пользователя X
'xx'	шестнадцатеричное значение
	оператор конкатенации

2. Криптографические системы и алгоритмы

2.1 Криптографические системы

- CSM_001 В бортовых устройствах и карточках тахографа применяется классический вариант криптосистемы RSA с открытым ключом, обеспечивающий следующие механизмы защиты:
- взаимная аутентификация бортовых устройств и карточек;
 - передача между бортовыми устройствами и карточками тахографа сеансовых ключей тройного шифрования по системе DES;
 - цифровая подпись данных, загружаемых с бортовых устройств или карточек тахографа и сохраняемых на внешних носителях.
- CSM_002 В бортовых устройствах и карточках тахографа используется симметричная криптосистема DES с тройным шифрованием информации для ее защиты от искажений при пользовательских операциях обмена данными между бортовыми устройствами и карточками тахографа и для

обеспечения в необходимых случаях конфиденциальности данных, передаваемых между бортовым устройством и карточкой тахографа.

2.2 Криптографические алгоритмы

2.2.1 Алгоритм RSA

CSM_003 Алгоритм RSA полностью определяется следующими соотношениями:

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

Более полное описание функции RSA можно найти в источниках [PKCS1]. Открытая экспонента e для расчетов RSA это — целое число в диапазоне от 3 до $n-1$, удовлетворяющее условию $\gcd(e, \text{lcm}(p-1, q-1))=1$.

2.2.2 Алгоритм хеширования

CSM_004 В схемах цифровой подписи используется алгоритм хеширования SHA-1, описание которого содержится в источниках [SHA-1].

2.2.3 Алгоритм шифрования данных

CSM_005 Алгоритмы на базе DES применяются в режиме сцепления криптоблоков.

3. Ключи и сертификаты

3.1 Генерация и рассылка ключей

3.1.1 Генерация и рассылка ключей RSA

CSM_006 Ключи RSA генерируются на трех функциональных уровнях, которые образуют следующую иерархию:

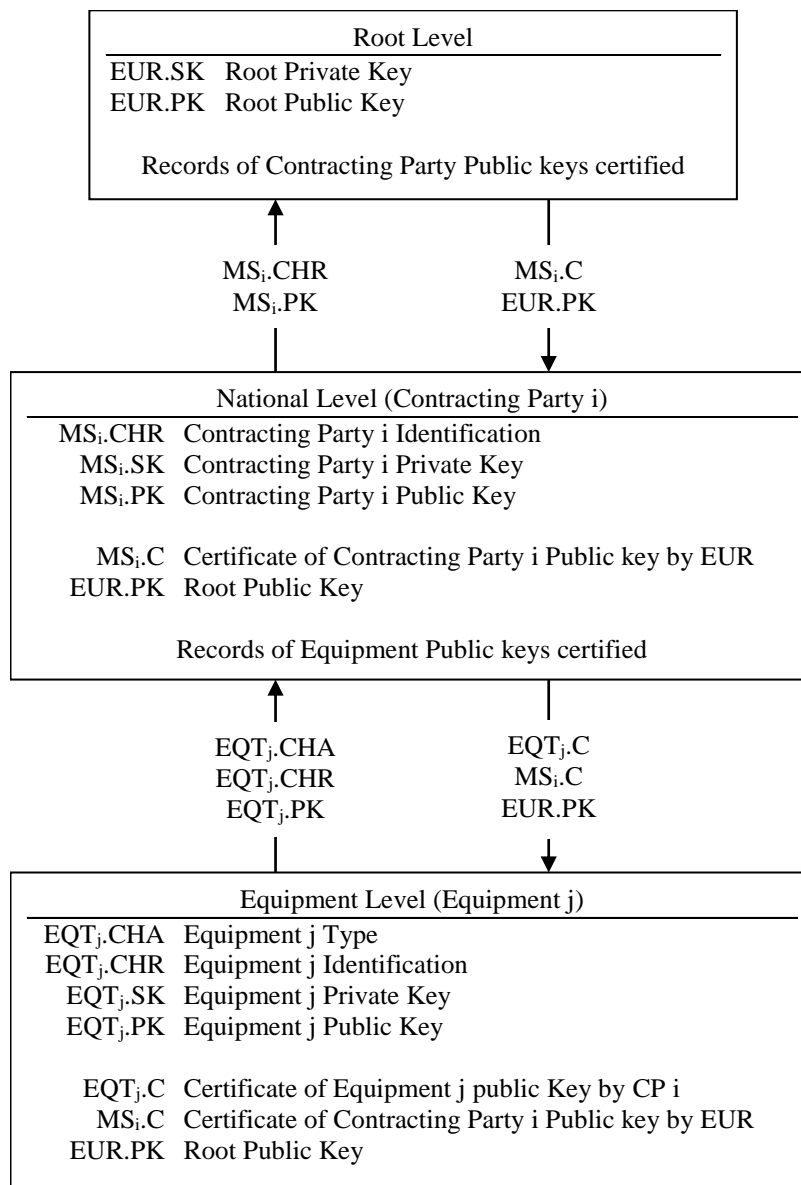
- европейский **корневой** уровень;
- уровень **государства-члена Договаривающейся стороны**;
- аппаратный уровень.

CSM_007 На **европейском корневом** уровне генерируется единая **корневая** пара **общеевропейских** ключей (EUR.SK и EUR.PK). Закрытый **европейский корневой** ключ служит для сертификации открытых ключей **государств-членов Договаривающихся сторон**. Все сертифицируемые ключи подлежат регистрации. Эти задачи выполняет **европейский корневой** сертификационный орган **под руководством и ответственность Европейской комиссии**.

CSM_008 На уровне **государства-члена Договаривающихся сторон** генерируется по паре ключей (MS.SK и MS.PK) для **каждого государства-члена каждой Договаривающейся стороны**. Открытые ключи **государств-членов Договаривающихся сторон** сертифицируются **европейским корневым** сертификационным органом. Закрытый ключ **государства-члена Договаривающейся стороны** используется для сертификации открытых ключей, вводимых в соответствующие аппаратные средства (бортовые устройства или карточки тахографа). Все сертифицируемые открытые ключи подлежат регистрации с указанием аппаратуры, для которой они предназначены. Эти функции выполняет сертификационный орган **государства-члена Договаривающейся стороны**. **Государство-член Договаривающаяся сторона** может регулярно менять свою пару ключей.

- CSM_009 На аппаратном уровне генерируется единая пара ключей (EQT.SK и EQT.PK), вводимых в каждое устройство. Эти функции выполняет сертификационный орган государства-члена Договаривающейся стороны. Открытые ключи аппаратного уровня сертифицируются сертификационным органом ~~государства-члена Договаривающейся стороны~~. Эти функции могут также выполнять изготовители аппаратуры, предприятия, персонализирующие аппаратуру, или соответствующие органы ~~государств-членов Договаривающихся сторон~~. Данная пара ключей служит для аутентификации, создания цифровых подписей и шифрования данных.
- CSM_010 При генерации, транспортировке (если она необходима) и хранении закрытых ключей соблюдается режим конфиденциальности.

Поток данных в ходе этого процесса схематически представлен на рисунке ниже.



3.1.2 Испытательные ключи RSA

- CSM_011 В целях испытания аппаратуры (включая испытания на эксплуатационную совместимость) ~~европейский~~ **корневой** сертификационный орган генерирует отдельную единую пару ~~европейских~~ **корневых** испытательных ключей и не менее двух пар испытательных ключей для ~~государств-членов Договаривающихся~~

сторон, открытые ключи которых сертифицируются закрытым испытательным ключом общеевропейского уровня. В ходе испытаний, проводимых с целью официального утверждения типовых образцов, в испытываемую аппаратуру изготовителями вводятся испытательные ключи, сертифицированные с помощью одного из вышеупомянутых испытательных ключей ~~государств-членов~~ **Договаривающихся сторон**.

3.1.3 Ключи датчика движения

В ходе генерации, транспортировки (если она необходима) и хранения трех ключей TDES, о которых говорится ниже, соблюдается надлежащий режим конфиденциальности.

В целях обеспечения совместимости с компонентами тахографов, соответствующими стандарту ISO 16844, ~~европейский~~ **корневой** сертификационный орган и сертификационные органы ~~государств-членов~~ **Договаривающихся сторон** принимают нижеследующие дополнительные меры:

CSM_036 ~~Европейский~~ **Корневой** сертификационный орган генерирует $K_{m_{VU}}$ и $K_{m_{WC}}$ — два независимых уникальных ключа для тройного шифрования по системе DES — после чего вычисляет K_m по формуле: $K_m = K_{m_{VU}} \text{ XOR } K_{m_{WC}}$. По запросам сертификационных органов ~~государств-членов~~ **Договаривающихся сторон** ~~Европейский~~ **корневой** сертификационный орган высылает им эти ключи с соблюдением надлежащих процедур защиты.

CSM_037 Сертификационные органы ~~государств-членов~~ **Договаривающихся сторон**:

- используют ключ K_m для шифрования показаний датчиков движения в соответствии с указаниями изготовителей этих датчиков (определение данных, подлежащих шифрованию ключом K_m , дается в стандарте ISO 16844-3);
- с соблюдением надлежащих процедур защиты высылают $K_{m_{VU}}$ изготовителям бортовых устройств для его ввода в эти устройства;
- обеспечивают ввод $K_{m_{WC}}$ во все карточки мастерских (запись SensorInstallationSecData в элементарном файле Sensor_Installation_Data) в процессе персонализации карточек.

3.1.4 Генерация и рассылка сеансовых ключей T-DES

CSM_012 Бортовые устройства и карточки тахографа в рамках процесса взаимной аутентификации генерируют необходимые данные и обмениваются ими в целях составления единого сеансового ключа для тройного шифрования по системе DES. Для сохранения конфиденциальности этого обмена данными используется криптографическая защита RSA.

CSM_013 Этот ключ используется при всех последующих операциях криптозащищенного обмена сообщениями. Он перестает действовать по окончании текущего сеанса (извлечение или перезагрузка карточки) и/или после 240-го использования (однократное использование ключа = передача на карточку одного защищенного сообщения-команды и получение соответствующего ответа).

3.2 Ключи

CSM_014 Ключи RSA (независимо от уровня) имеют следующую длину: модуль n 1024 бита, открытая экспонента e — до 64 бит, закрытая экспонента d — 1024 бита.

CSM_015 Ключи DES для тройного шифрования имеют вид (K_a, K_b, K_a) , где K_a и K_b независимые ключи длиной 64 бита. Биты контроля по четности не задаются.

3.3 Сертификаты

CSM_016 Сертификаты открытых ключей RSA должны быть сертификатами «не содержащими самоописания», с возможностью «проверки по карточке» (см. ISO/IEC 7816-8).

3.3.1 Содержание сертификатов

CSM_017 Сертификаты открытых ключей RSA создаются на основе следующих данных в указанной последовательности:

Данные	Формат	Байты	Примечание
CPI	ЦЕЛОЕ ЧИСЛО	1	Идентификатор профиля сертификата (в данной версии — '01')
RAC	ОКТЕТНАЯ СТРОКА	8	Указатель сертификационного органа
ADC	ОКТЕТНАЯ СТРОКА	7	Полномочия держателя сертификата
EOV	Реальное время	4	Дата истечения срока действия сертификата
RDC	ОКТЕТНАЯ СТРОКА	8	Указатель держателя сертификата
<i>n</i>	ОКТЕТНАЯ СТРОКА	128	Открытый ключ (модуль)
<i>e</i>	ОКТЕТНАЯ СТРОКА	8	Открытый ключ (открытая экспонента)

164

Примечания:

1. «Идентификатор профиля сертификата» (CPI) определяет конкретную структуру сертификата, используемого в целях аутентификации. Он может применяться аппаратурой в качестве внутреннего идентификатора для вызова соответствующего списка заголовков, заключающего в себе описание конкатенации элементов данных, из которых состоит сертификат.

Такой список заголовков, отражающий содержание сертификата, выглядит следующим образом:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Расширенная метка списка заголовков	Длина списка заголовков	Метка CPI	Длина CPI	Метка RAC	Длина RAC	Метка ADC	Длина ADC	Метка EOV	Длина EOV	Метка RDC	Длина RDC	Метка открытого ключа (генерируется)	Длина последующих объектов данных	Метка модуля	Длина модуля	Метка открытой экспоненты	Длина открытой экспоненты

2. «Указатель сертификационного органа» (CAR) служит для обозначения сертификационного органа, выдавшего сертификат; таким образом, этот элемент данных может использоваться одновременно с идентификатором ключа сертификационного органа для указания на принадлежащий данному органу

открытый ключ (информацию о соответствующих кодах см. ниже в пункте, посвященном идентификаторам ключей).

3. «Полномочия держателя сертификата» (СНА) — указание на объем прав, предоставляемых сертификатом. Они включают в себя идентификатор приложения тахографа и типа аппаратуры, для которой предназначен сертификат (соответствует элементу данных EquipmentType; для ~~государства-члена Договаривающейся стороны~~ используется значение '00').

4. «Указатель держателя сертификата» (СНР) служит для уникального обозначения держателя сертификата; таким образом, этот элемент данных может использоваться одновременно с идентификатором ключа субъекта для указания на принадлежащий данному держателю сертификата открытый ключ.

5. Идентификаторы ключей позволяют однозначно идентифицировать держателя сертификата или сертификационный орган. Они кодируются следующим образом:

5.1 Аппаратура (БУ или карточка):

Данные	Серийный номер аппаратуры	Дата	Тип	Изготовитель
Длина	4 байта	2 байта	1 байт	1 байт
Значение	Целое число	мм гтгг VCD-код	По усмотрению изготовителем	Код изготовителя

Когда речь идет о БУ, его изготовитель, запрашивая сертификаты, не обязательно должен знать идентификационные данные аппаратуры, в которую будут вводиться соответствующие ключи.

В первом случае изготовитель направляет идентификационные данные оборудования вместе с открытым ключом в сертификационный орган ~~своего государства-члена своей Договаривающейся стороны~~. Выданный в результате сертификат будет содержать идентификационные данные аппаратуры, в связи с чем изготовителю необходимо будет принять меры к тому, чтобы ключи и сертификат вводились именно в ту аппаратуру, для которой они предназначены. Идентификатор ключа имеет вид, показанный выше.

Во втором случае изготовитель должен однозначно идентифицировать каждый запрос на сертификат и направить такие идентификационные данные вместе с открытым ключом на сертификацию в сертификационный орган ~~своего государства-члена своей Договаривающейся стороны~~. В выданном сертификате будет указано индивидуальное обозначение заявки. После ввода ключа в аппаратуру изготовитель должен информировать сертификационный орган ~~своего государства-члена своей Договаривающейся стороны~~ о закреплении этого ключа за соответствующей аппаратурой (т. е. сообщить индивидуальное обозначение заявки на сертификат и идентификационные данные аппаратуры). Идентификатор ключа имеет вид, показанный выше.

Данные	Серийный номер заявки на сертификат	Дата	Тип	Изготовитель
Длина	4 байта	2 байта	1 байт	1 байт
Значение	Целое число	мм гтгг VCD-код	'FF'	Код изготовителя

5.2 Сертификационный орган

Данные	Идентификационные данные органа	Серийный номер ключа	Дополнительная информация	Идентификатор
Длина	4 байта	1 байт	2 байта	1 байт
Значение	1-байтовый числовой код страны 3-байтовый буквенно-цифровой код страны	Целое число	Дополнительный код (определяется сертификационным органом) Если не указан — 'FF FF'	'01'

Серийный номер ключа позволяет отличать друг от друга различные ключи государства-члена Договаривающейся стороны в случае смены своего ключа.

6. Сторона, проверяющая сертификат, по косвенным признакам распознает сертифицируемый открытый ключ как ключ криптосистемы RSA, предназначенный для аутентификации, проверки цифровых подписей и шифрования конфиденциальной информации (сам сертификат не содержит прямо указывающих на это идентификаторов объектов).

3.3.2 Выдаваемые сертификаты

CSM_018 CSM_018 Выдаваемый сертификат представляет собой цифровую подпись с возможностью частичного восстановления содержания сертификата, соответствующую стандарту ISO/IEC 9796-2 (за исключением приложения A4) и сопровождаемую «указателем сертификационного органа».

$$X.C = X.CA.SK['6A' \parallel C_r \parallel Hash(Cc) \parallel 'BC'] \parallel C_n \parallel X.CAR$$

При содержании сертификата = Cc = C_r || C_n

106 байтов 58 байтов

Примечания:

1. Длина данного сертификата составляет 194 байта.
2. К подписи также приобщается скрытый ею CAR, что позволяет использовать для проверки сертификата открытый ключ соответствующего сертификационного органа.
3. Сторона, проверяющая сертификат, по косвенным признакам определяет алгоритм, использованный сертификационным органом для подписания сертификата.
4. Данному сертификату соответствует следующий список заголовков:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Метка сертификата CV (генерируется)	Длина последующих объектов данных	Метка подписи	Длина подписи	Метка остатка	Длина остатка	Метка CAR	Длина CAR

3.3.3 Проверка и расшифровка сертификатов

Процесс проверки и расшифровки сертификатов заключается в проверке подписи согласно стандарту ISO/IEC 9796-2, извлечении содержания сертификата и получении

из него соответствующего открытого ключа: $X.PK = X.CA.PK \circ X.C$ и проверке действительности сертификата.

CSM_019 Этот процесс состоит из следующих этапов:

Проверка подписи и извлечение содержания:

- Из X.C извлекаются Sign., C_n' и CAR: $X.C = \text{Sign} \parallel C_n' \parallel \text{CAR}'$
 128 байтов 58 байтов 8 байтов

из указателя CAR' выбирается открытый ключ соответствующего сертификационного органа (если он не выбран до этого иным способом)

- функция Sign открывается при помощи открытого ключа CA: $Sr' = X.CA.PK$ [подпись],
- проверяется Sr' (начальными символами должны быть '6A', конечными — 'BC');
- вычисляются C_r' и H' по формуле: $Sr' = '6A' \parallel C_r' \parallel H' \parallel 'BC'$
 106 байтов 20 байтов
- извлекается содержание сертификата $C' = C_r' \parallel C_n'$;
- проверяется $\text{Hash}(C') = H'$

Положительный результат проверки указывает на подлинность сертификата, содержание которого соответствует C'.

Подтверждение действительности. Из C':

- Если применимо, проверяется дата истечения срока действия сертификата.

Извлечение из C' и сохранение открытого ключа, идентификатора ключа, полномочий держателя сертификата и даты истечения срока его действия:

- $X.PK = n \parallel e$
- $X.KID = CHR$
- $X.CHA = CHA$
- $X.EOV = EOV$

4. Механизм взаимной аутентификации

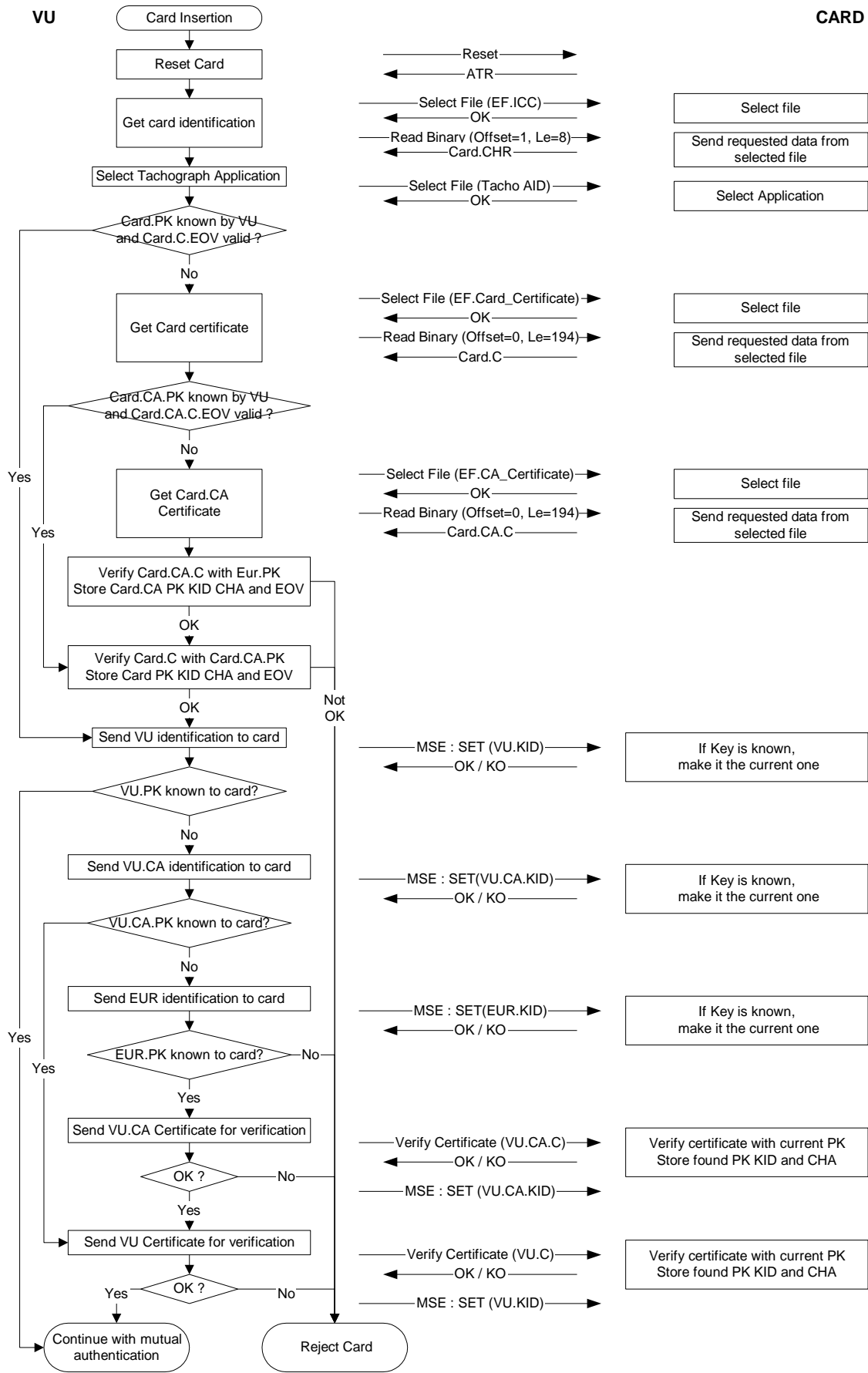
В основу механизма взаимной аутентификации карточек и БУ положен следующий принцип:

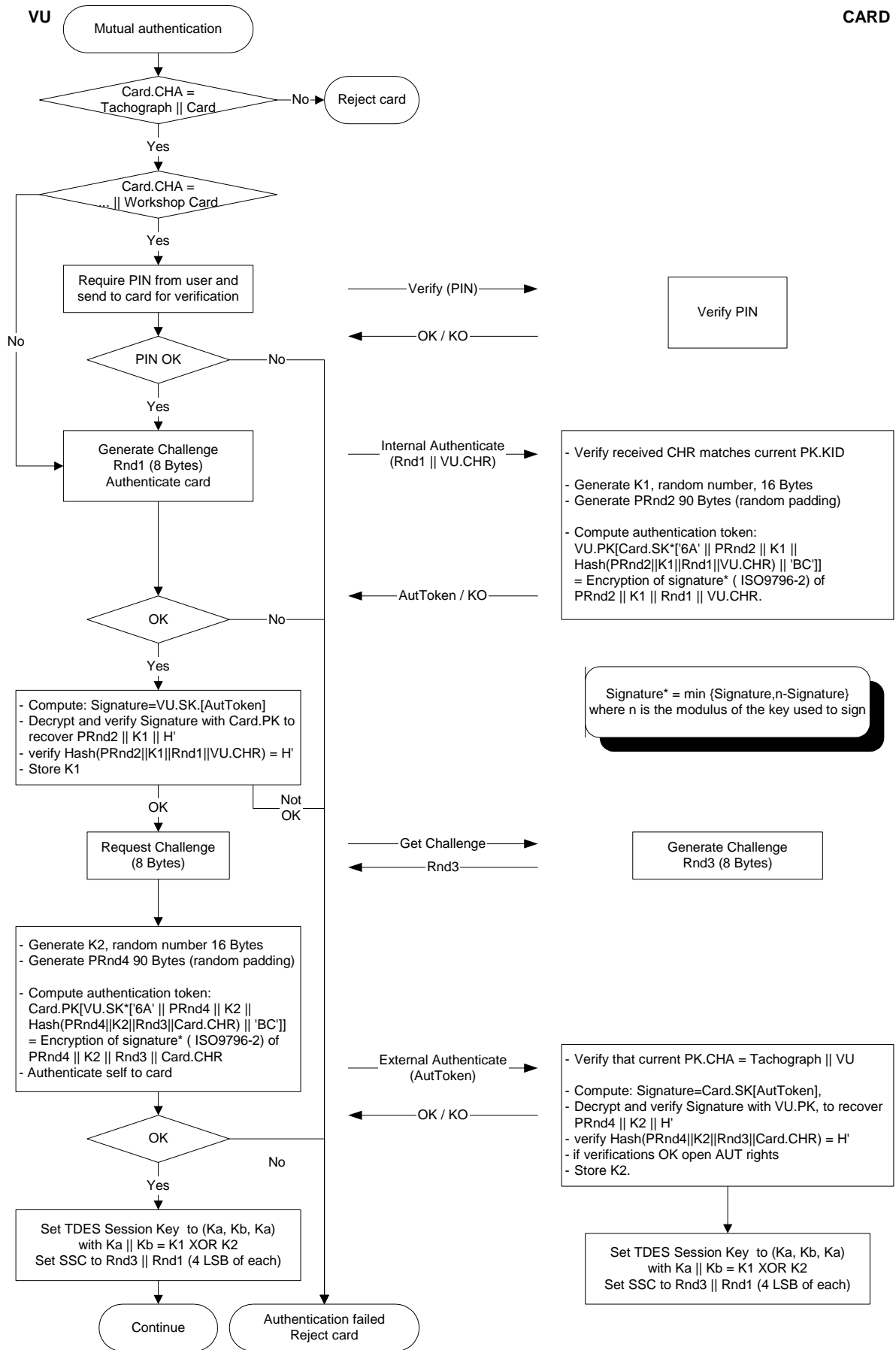
Каждая сторона должна доказать другой наличие у нее действительной пары ключей, открытый ключ которой сертифицирован сертификационным органом ~~государства-члена Договаривающейся стороны~~, имеющим в свою очередь сертификат, выданный ~~европейским~~ **корневым сертификационным органом**.

Доказательством служит подписание закрытым ключом случайной последовательности цифр, полученной от другой стороны, которая при проверке подписи должна восстановить из нее ту же последовательность цифр.

Данный механизм вводится в действие БУ при вводе карточки. Процесс начинается с обмена сертификатами и извлечения открытых ключей и завершается созданием сеансового ключа.

CSM_020 При этом используется протокол, представленный ниже (стрелками показаны команды и передаваемые данные (см. ~~приложение~~ **подраздел 2 добавления**)):





5. Механизмы обеспечения конфиденциальности, целостности и аутентификации данных в процессе их передачи между БУ и карточками

5.1 Защищенный обмен сообщениями

- CSM_021 Целостность данных, передаваемых между БУ и карточками, обеспечивается благодаря криптозащите сообщений в соответствии со следующими ссылками [ISO/IEC 7816-4] и [ISO/IEC 7816-8].
- CSM_022 При передаче данных, которые нуждаются в защите, к посылаемым в виде команды или ответа объектам данных добавляется объект, представляющий собой криптографическую контрольную сумму. Эта криптографическая контрольная сумма проверяется принимающим устройством.
- CSM_023 В криптографической контрольной сумме данных, посылаемых в виде команды, учитываются заголовок команды и все содержащиеся в ней объекты данных (\Rightarrow CLA = '0C', причем все эти объекты данных при их формировании снабжаются метками, в которых b1=1).
- CSM_024 Байты ответа, несущие информацию о состоянии, защищаются с помощью криптографической контрольной суммы в тех случаях, когда ответ не содержит полей данных.
- CSM_025 Криптографические контрольные суммы имеют длину 4 байта.

Таким образом, при защищенном обмене сообщениями команды и ответы имеют структуру, показанную ниже.

Используемые здесь объекты данных представляют собой часть набора DO для криптозащищенного обмена сообщениями, описание которого приводится в ISO/IEC 7816-4:

Метка	Мнемокод	Значение
'81'	T _{VC}	Простое значение: данные без кодировки BER-TLV (защищаются с помощью ККС)
'97'	T _{LE}	Значение Le в незащищенной команде (защищается с помощью ККС)
'99'	T _{ME}	Информация о состоянии (защищается с помощью ККС)
'8E'	T _{CC}	Криптографическая контрольная сумма
'87'	T _{IR CG}	Байт индикации заполнения Криптограмма (Простое значение без кодировки BER-TLV)

Если незащищенная пара «команда — ответ» выглядит следующим образом:

Заголовок команды				Текст команды		
CLA	INS	P1	P2	[Поле L _c]	[Поле данных]	[Поле L _e]
	4 байта			L байт, обозначаемый как байты V ₁ –V _L		

Текст ответа	Концевая метка ответа
[Поле данных]	SW1 SW2
L _r байтов данных	2 байта

то соответствующая ей криптозащищенная пара «команда — ответ» имеет следующий вид:

Криптозащищенная команда:

Заголовок команды (CH)				Текст команды										
CLA	INS	P1	P2	[Новое поле L _c]	[Новое поле данных]						[Новое поле L _e]			
'0C'				Длина [нового поля данных]	T _{PV}	L _{PV}	PV	T _{LE}	L _{LE}	L _e	T _{CC}	L _{CC}	CC	'00'
					'81'	L _c	[Поле данных]	'97'	'01'	L _e	'8E'	'04'	CC	

Данные, подлежащие учету в контрольной сумме = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB, где

PB = байты заполнения (80 .. 00) в соответствии со стандартом ISO-IEC 7816-4 и ISO 9797 (метод 2).

DOs PV и LE присутствуют только тогда, когда в незащищенной команде есть соответствующие данные.

Криптозащищенный ответ:

1. Если поле данных ответа не является пустым, но не нуждается в защите конфиденциальности:

Текст ответа				Концевая метка ответа			
[Новое поле данных]				Новые SW1 SW2			
T _{PV}	L _{PV}	PV	T _{CC}	L _{CC}	CC		
'81'	L _c	[Поле данных]	'8E'	'04'	CC		

Данные, учитываемые в контрольной сумме = T_{PV} || L_{PV} || PV || PB

2. Если поле данных ответа не является пустым, но не нуждается в защите конфиденциальности:

Текст ответа				Концевая метка ответа			
[Новое поле данных]				Новые SW1 SW2			
T _{PI CG}	L _{PI CG}	PI CG	T _{CC}	L _{CC}	CC		
'87'		PI CG	'8E'	'04'	CC		

Данные, передаваемые в виде криптограммы: данные без кодировки BER-TLV и заполняющие байты.

Данные, учитываемые в контрольной сумме = T_{PI CG} || L_{PI CG} || PI CG || PB

3. Если поле данных ответа пустое:

Текст ответа				Концевая метка ответа			
[Новое поле данных]				Новые SW1 SW2			
T _{SW}	L _{SW}	SW	T _{CC}	L _{CC}	CC		
'99'	'02'	Новые SW1 SW2	'8E'	'04'	CC		

5.2 Обработка ошибок при криптозащищенном обмене сообщениями

CSM_026 Когда карточка тахографа обнаруживает ошибку КЗОС при расшифровке команды, она возвращает соответствующие байты состояния, не используя КЗОС. В соответствии со стандартом ISO/IEC 7816-4 для указания на ошибки КЗОС предусматриваются следующие байты состояния:

- ‘66 88’: Несоответствие криптографической контрольной суммы;
- ‘69 87’: Отсутствие ожидаемых объектов данных SM;
- ‘69 88’: Неверные объекты данных КЗОС.
- CSM_027 Если карточкой тахографа возвращены байты состояния без ОД КЗОС или с неверным ОД КЗОС, то БУ должно прервать сеанс обмена данными.

5.3 Алгоритм расчета криптографических контрольных сумм

CSM_028 Криптографические контрольные суммы вычисляются на основе алгоритма аутентификации сообщений «retail-MAC» в соответствии с ANSI X9.19 и системой DES:

- начальный этап: в качестве первого контрольного блока y_0 используется $E(K_a, SSC)$;
- последующие этапы: на основе K_a рассчитываются контрольные блоки y_1, \dots, y_n ;
- заключительный этап: по последнему контрольному блоку y_n рассчитывается криптографическая контрольная сумма: $E(K_a, D(K_b, y_n))$.

где $E()$ означает шифрование по системе DES, а $D()$ — расшифровку по системе DES.

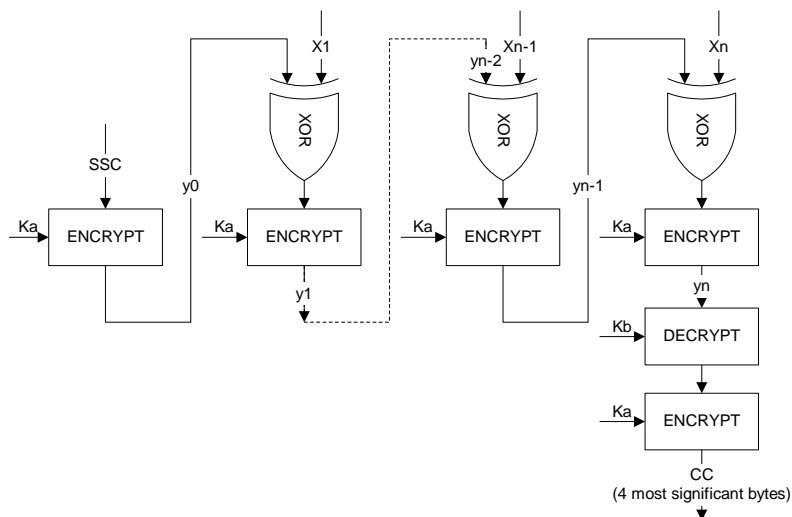
Передаче подлежат четыре старших байта криптографической контрольной суммы.

CSM_029 В ходе процедуры согласования ключей счетчику исходящих сообщений (SSC) задаются следующие начальные значения:

Initial SSC: Rnd3 (4 младших байта) || Rnd1 (4 младших байта).

CSM_030 Счетчик последовательности отправки должен увеличиваться на 1 каждый раз перед вычислением MAC (т. е. SSC для первой команды равен Initial SSC + 1, SSC для первого ответа равен Initial SSC + 2).

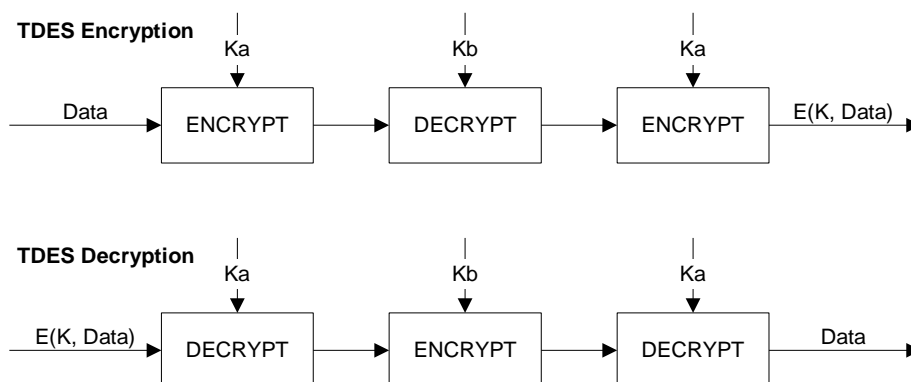
Способ вычисления retail-MAC изображен на диаграмме ниже:



5.4 Алгоритм расчета криптограмм для защиты конфиденциальности Dos

CSM_031 Криптограммы рассчитываются с помощью алгоритма TDEA в режиме TCBC, как указано в цитируемых источниках [TDES] и [TDES-OP], причем в качестве блока начальной величины используется нуль-вектор.

Применение ключей TDES показано на следующей диаграмме:



6. Механизмы цифровой подписи при загрузке данных

CSM_032 Данные, полученные из того или иного аппаратного источника (БУ или карточки) за один сеанс загрузки, сохраняются специализированной программируемой аппаратурой (СПА) в виде одного физического файла данных. Этот файл должен содержать сертификаты MSi.C и EQT.C. Файл содержит цифровые подписи блоков данных, как указано в **Приложении Подразделе 7: Протоколы загрузки данных.**

CSM_033 Цифровые подписи загружаемых данных создаются по схеме, предполагающей добавление информации, которая позволяет при желании производить считку загруженных данных в нерасшифрованном виде.

6.1 Генерация подписей

CSM_034 Подписи данных генерируются аппаратурой согласно схеме подписи с соответствующим добавлением, которая определена в цитируемом источнике [PKCS1], при помощи хеш-функции SHA-1:

Подпись = EQT.SK[‘00’ || ‘01’ || PS || ‘00’ || DER(SHA-1(данные))]

PS = заполняющая октетная строка со значением ‘FF’ до общей длины 128.

DER(SHA-1(M)) — кодированное представление идентификатора алгоритма хеш-функции и значения хеш-функции в виде величины стандарта ASN.1 типа DigestInfo (правила однозначного шифрования):

‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’||‘05’||‘00’||‘04’||‘14’ || значение хеш-функции.

6.2 Проверка подписей

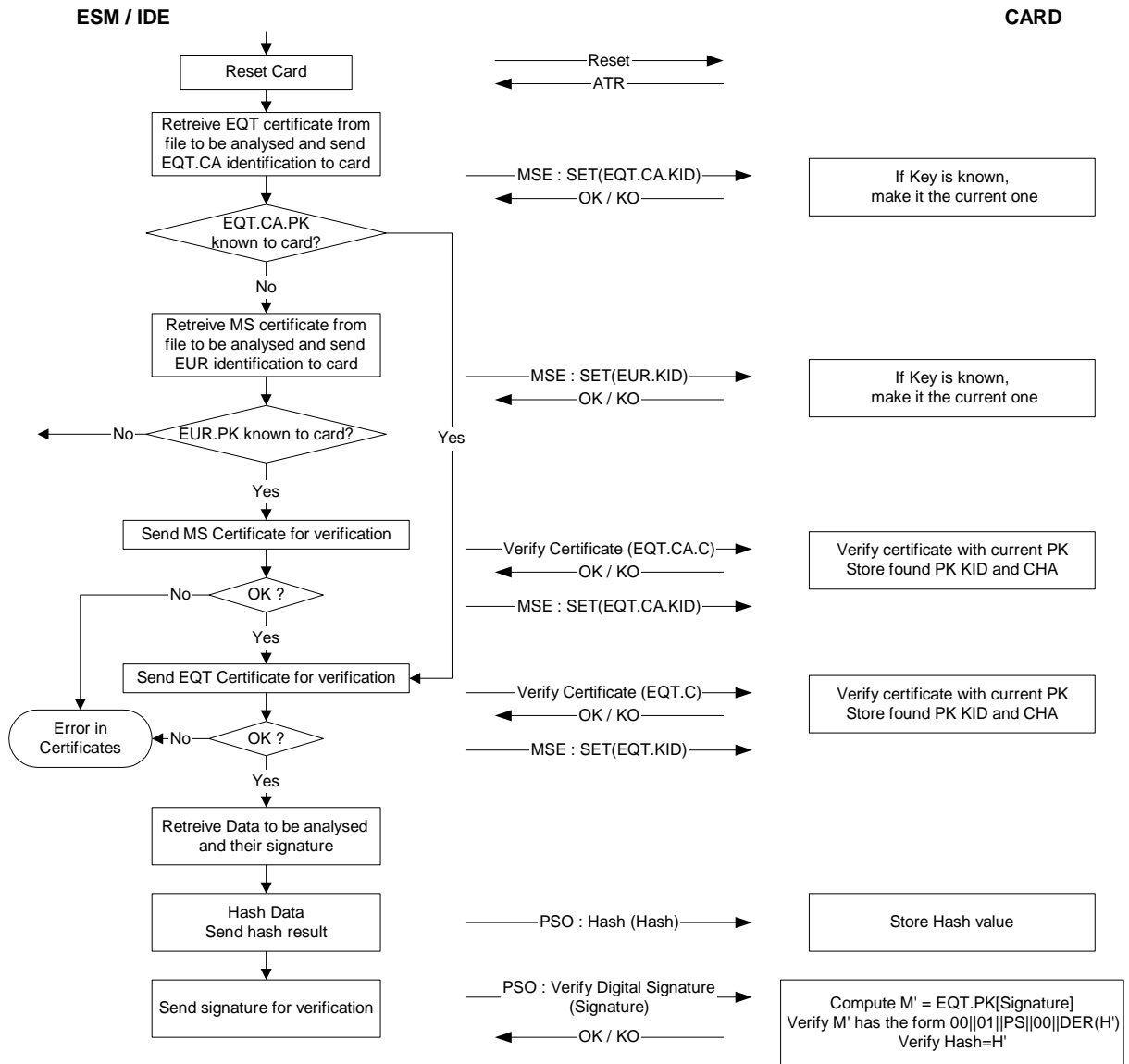
CSM_035 Проверка подписи загружаемых данных производится согласно схеме подписи с соответствующим добавлением, которая определена в цитируемом источнике [PKCS1], при помощи хеш-функции SHA-1.

Проверяющей стороне должен быть известен ~~европейский~~ **корневой** открытый ключ EUR.PK, который она должна получить из независимого (и пользующегося доверием) источника.

В нижеследующей таблице представлен протокол, в соответствии с которым СПА после ввода в нее карточки контролера может проверять целостность загруженных данных, сохраненных на ВН (внешнем носителе). Для расшифровки цифровых

подписей используется карточка контролера. В этом случае данная функция не обязательно должна быть предусмотрена в СПА.

Аппаратура, с помощью которой были загружены и подписаны подлежащие анализу данные, обозначена буквами EQT.



ЧАСТЬ В СИСТЕМА ТАХОГРАФОВ ВТОРОГО ПОКОЛЕНИЯ

7. Введение

7.1 Справочные материалы

В этой части настоящего приложения подраздела добавления используются следующие источники:

Национальный институт стандартов и технологий AES (NIST), FIPS PUB 197: Расширенный стандарт шифрования (AES), 26 ноября 2001 года.

DSS Национальный институт стандартов и технологий (NIST), FIPS PUB 186-4: Расширенный стандарт цифровой подписи (DSS), июль 2013 года.

ISO 7816-4 ISO/IEC 7816-4, Карточки идентификационные — карточки на интегральных микросхемах. Часть 4: организация, безопасность и команды обмена. 3-е издание. 15 апреля 2013 года.

ISO 7816-8 ISO/IEC 7816-8, Карточки идентификационные — карточки на интегральных микросхемах. Часть 8: команды операций по обеспечению безопасности. 2-е издание. 1 июня 2004 года.

ISO 8825-1 ISO/IEC 8825-1, Информационные технологии. Правила кодирования — ASN.1: Спецификация базовых правил кодирования (BER), канонических правил кодирования (CER) и особых правил кодирования (DER). 4-е издание, 15 декабря 2008 года.

ISO 9797-1 ISO/IEC 9797-1, Информационные технологии. Методы обеспечения безопасности — Коды аутентификации сообщений (MAC). 2-е издание, 1 марта 2011 года.

ISO 10116 ISO/IEC 10116, Информационные технологии. Методы обеспечения безопасности. Режимы работы n-битного блока шифрования. 3-е издание. 1 февраля 2006 года.

ISO 16844-3 ISO/IEC 16844-3, Транспортные средства дорожные. Системы тахографов. Часть 3: интерфейс датчика движения. 1-е издание, 2004 года, включая техническую поправку 1, 2006 год.

RFC 5480 Эллиптическая криптография. Информация об открытом ключе субъекта, март 2009 года.

RFC 5639 Эллиптическая криптография (ECC). Стандартные кривые «Brainpool» и генерирование кривых, 2010 год.

RFC 5869 Функция формирования ключа извлечения и расширения на базе HMAC (HKDF), май 2010 года.

SHS Национальный институт стандартов и технологий (NIST), FIPS PUB 180-4: Стандарт безопасного хеширования, март 2012 года.

SP 800-38B Национальный институт стандартов и технологий (NIST), специальный выпуск 800-38B: Рекомендация по режимам работы с шифрованием блоками: режим аутентификации CMAC, 2005 год.

TR-03111 Технические рекомендации BSI TR-03111, эллиптическая криптография, версия 2.00, 28 июня 2012 года.

7.2 Условные обозначения и сокращения

В настоящем ~~приложении~~ **подразделе добавления** используются следующие условные обозначения и сокращения:

AES	Расширенный стандарт шифрования
CA	Служба сертификации
CAR	Указатель сертификационного органа
CBC	Сцепление криптоблоков (режим работы)
CH	Заголовок команды
CHA	Полномочия держателя сертификата
CHR	Указатель держателя сертификата
CV	Постоянный вектор
DER (OBC)	Особые правила кодирования
DO	Объект данных
DSRC	Выделенная связь ближнего действия
ECC	Эллиптическая криптография
ECDSA	Алгоритм цифровой подписи эллиптической кривой
ECDH	Эллиптическая кривая Диффи-Хеллмана (алгоритм согласования ключей)
EGF	внешнее устройство ГНСС
EQT	Оборудование
СПА	Специализированная программируемая аппаратура
K _M	Ключ старшего разряда датчика движения, позволяющий соединять бортовое устройство с датчиком движения
K _{M-UEV}	Ключ, введенный в бортовые устройства, что позволяет БУ генерировать ключ старшего разряда датчика движения, если в БУ вставлена карточка мастерской
K _{M-WC}	Ключ, введенный в карточки мастерской, что позволяет БУ генерировать ключ старшего разряда датчика движения, если в БУ вставлена карточка мастерской
MAC	Код аутентификации сообщений
MoS	Датчик движения
MSB	Самый значимый бит
ИПК	Инфраструктура открытых ключей
RCF	Средство удаленной связи
SSC	Счетчик исходящих сообщений
SM	Защищенный обмен сообщениями
TDES	Стандарт тройного шифрования данных
TLV	Значение длины метки
БУ	Бортовое устройство
X.C	Сертификат открытого ключа пользователя X
X.CA	Сертификационный орган, выдавший сертификат пользователя X

X.CAR	Идентификатор сертификационного органа, указанного в сертификате пользователя X
X.CHR	Идентификатор сертификата, указанного в сертификате пользователя X
X.PK	Открытый ключ пользователя X
X.SK	Закрытый ключ пользователя X
X.PK _{eph}	Кратковременный открытый ключ пользователя X
X.SK _{eph}	Кратковременный закрытый ключ пользователя X
'xx'	Шестнадцатеричное значение
	Оператор конкатенации

7.3 Определения

Определения терминов, употребляемых в настоящем ~~приложении~~ подразделе, включены в раздел I ~~приложения~~ добавления 1С.

8. Криптографические системы и алгоритмы

8.1 Криптографические системы

CSM_38 В бортовых устройствах и карточках тахографа применяется вариант криптосистемы на основе эллиптической кривой с открытым ключом для решения следующих задач в области защиты:

- взаимная аутентификация между бортовым устройством и соответствующей карточкой;
- согласование сеансовых ключей AES между бортовым устройством и соответствующей карточкой;
- обеспечение подлинности, целостности и невозможности отказа от данных, загружаемых с бортовых устройств или карточек тахографа на внешние носители.

CSM_39 В бортовых устройствах и внешних устройствах ГНСС применяется вариант криптосистемы на основе эллиптической кривой с открытым ключом для решения следующих задач в области защиты:

- сопряжение бортового устройства и внешнего устройства ГНСС;
- взаимная аутентификация бортового устройства и внешнего устройства ГНСС;
- согласование сеансовых ключей AES между бортовым устройством и внешним устройством ГНСС.

CSM_40 В бортовых устройствах и карточках тахографа применяется вариант симметричной криптосистемы на основе AES в целях решения следующих задач в области защиты:

- обеспечение подлинности и целостности данных, которыми обмениваются бортовое устройство и соответствующая карточка тахографа;
- обеспечение, в случае применимости, конфиденциальности данных, которыми обмениваются бортовое устройство и соответствующая карточка тахографа.

- CSM_41 В бортовых устройствах и внешних устройствах ГНСС применяется вариант симметричной криптосистемы на основе AES в целях решения следующих задач в области защиты:
- обеспечение подлинности и целостности данных, которыми обмениваются бортовое устройство и соответствующее внешнее устройство ГНСС.
- CSM_42 В бортовых устройствах и датчиках движения применяется вариант симметричной криптосистемы на основе AES в целях решения следующих задач в области защиты:
- сопряжение бортового устройства и датчика движения;
 - взаимная аутентификация бортового устройства и датчика движения;
 - обеспечение, в случае применимости, конфиденциальности данных, которыми обмениваются бортовое устройство и датчик движения.
- CSM_43 В бортовых устройствах и карточках контролера применяется вариант симметричной криптосистемы на основе AES в целях выполнения следующих функций защиты на уровне интерфейса удаленной связи:
- обеспечение конфиденциальности, подлинности и целостности данных, которые передаются бортовым устройством на контрольную карточку.

Примечания:

- Строго говоря, данные передаются с бортового устройства на средство удаленного мониторинга под надзором контролера с использованием соответствующего средства удаленной связи, которое может быть внутренним или внешним по отношению к БУ; см. приложение подраздел 14. При этом средство удаленного мониторинга передает данные на контрольную карточку для расшифровки и подтверждения подлинности. С точки зрения защиты средство удаленной связи и средство удаленного мониторинга полностью прозрачны.
- Карточка мастерской предлагает те же самые функции защиты интерфейса DSRC, что и карточка контролера. Это позволяет мастерской проверять надлежащую работу интерфейса удаленной связи БУ, включая параметры безопасности. Более подробно см. в разделе 9.2.3 9.2.2.

8.2 Криптографические алгоритмы

8.2.1 Симметричные алгоритмы

- CSM_44 Бортовые устройства, карточки тахографов, датчики движения и внешние устройства ГНСС поддерживают алгоритм AES, определенный в [AES], с длиной ключей 128, 192 и 256 битов.

8.2.2 Асимметричные алгоритмы и стандартизованные параметры домена

- CSM_45 Бортовые устройства, карточки тахографов и внешние устройства ГНСС поддерживают эллиптическую криптографию с размером ключей 256, 384 и 512/521 битов.
- CSM_46 Бортовые устройства, карточки тахографов и внешние устройства ГНСС поддерживают алгоритм подписи ECDSA, как описано в источнике [DSS].
- CSM_47 Бортовые устройства, карточки тахографов и внешние устройства ГНСС поддерживают алгоритм подписи ECKA-EG, как описано в источнике [TR 03111].
- CSM_48 Бортовые устройства, карточки тахографов и внешние устройства ГНСС поддерживают все стандартизованные параметры домена, указанные ниже в таблице 43 применительно к эллиптической криптографии.

Таблица 1
Стандартизированные параметры домена

Название	Размер (биты)	Ссылка	Идентификатор объекта
NIST P-256	256	[DSS], [RFC 5480]	secp256r1
BrainpoolP256r1	256	[RFC 5639]	brainpoolP256r1
NIST P-384	384	[DSS], [RFC 5480]	secp384r1
BrainpoolP384r1	384	[RFC 5639]	brainpoolP384r1
BrainpoolP512r1	512	[RFC 5639]	brainpoolP512r1
NIST P-521	521	[DSS], [RFC 5480]	secp521r1

Примечание: Идентификаторы объектов, упомянутые в последней колонке ~~таблицы 43~~ **таблицы 1**, указаны в [RFC 5639] для кривых Brainpool и в [RFC 5480] для кривых NIST.

Пример 1: идентификатор объекта для кривых BrainpoolP256r1 имеет вид {iso(1)identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1) versionOne(1) 7}.

Или в точечной нотации: 1.3.36.3.3.2.8.1.1.7.

Пример 2: идентификатор объекта кривой NIST P-384 имеет вид

{iso(1) identified-organization(3) certicom(132) curve(0) 34}

или в точечной нотации: 1.3.132.0.34.

8.2.3 Алгоритмы хеширования

CSM_49 Бортовые устройства **и**, карточки тахографов **и внешние устройства ГНСС** поддерживают алгоритмы SHA-256, SHA-384 и SHA-512, как описано в источнике [DSS].

8.2.4 Последовательности шифров

CSM_50 Если симметричный алгоритм, несимметричный алгоритм и/или алгоритм хеширования используются вместе для формирования соответствующего протокола безопасности, то длина их соответствующих ключей и размеры хеш-параметров (примерно) равны. ~~Таблица 44~~ **Таблица 2** отображает допустимые последовательности шифров:

Таблица 2
Допустимые последовательности шифров

Идентификатор набора шифров	Размер ключа ECC (биты)	Длина ключа AES (биты)	Алгоритм хеширования	Длина MAC (байты)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Примечание: Размеры ключей ECC, составляющие 512 битов и 521 бит, считаются равными по качеству для выполнения всех задач, предусмотренных в настоящем ~~приложении~~ **подразделе**.

9. Ключи и сертификаты

9.1 Асимметричные пары ключей и сертификаты открытых ключей

9.1.1 Общие положения

Примечание: Ключи, описанные в настоящем разделе, используются для взаимной аутентификации и защищенного обмена сообщениями между бортовыми устройствами и карточками тахографов и между бортовыми устройствами и внешними устройствами ГНСС. Данные процессы подробно освещены в главах 0 и 0 настоящего подраздела.

CSM_51 В рамках ~~европейской~~ системы смарт-тахографов пары ключей ECC и соответствующие сертификаты генерируются и управляются на трех функциональных иерархических уровнях:

- ~~европейский~~ **корневой** уровень;
- уровень ~~государства-члена~~ **Договаривающейся стороны**;
- аппаратный уровень.

CSM_52 Во всей ~~европейской~~ системе смарт-тахографов открытые и закрытые ключи и сертификаты генерируются, управляются и передаются при помощи стандартизированных защищенных средств.

9.1.2 Европейский Корневой уровень

CSM_53 На ~~европейском~~ **корневом** уровне генерируется единая пара общеевропейских ключей ECC, обозначаемых как EUR. В нее входят закрытый ключ (EUR.SK) и открытый ключ (EUR.PK). Данная пара ключей формирует пару корневых ключей для PKI всей европейской системы смарт-тахографов. Эту задачу выполняет ~~европейский~~ **корневой** сертификационный орган (ERCA) ~~под руководством и под ответственность Европейской комиссии.~~

CSM_54 ERCA использует ~~европейский~~ **корневой** закрытый ключ для подписания (самоподписывающегося) корневого сертификата ~~европейского~~ **корневого** открытого ключа и передает этот ~~европейский~~ **корневой** сертификат всем ~~государствам-членам~~ **Договаривающимся сторонам**.

CSM_55 ERCA использует ~~европейский~~ **корневой** закрытый ключ для подписания сертификатов открытых ключей ~~государств-членов~~ **Договаривающихся сторон** по запросу. ERCA ведет записи всех подписанных сертификатов открытых ключей ~~государств-членов~~ **Договаривающихся сторон**.

CSM_56 Как показано на рисунке 1 в разделе 9.1.7, ERCA генерирует новую пару ~~европейских~~ **корневых** ключей каждые 17 лет. Когда ERCA генерирует новую пару ~~европейских~~ **корневых** ключей, он создает новый самоподписывающийся ~~европейского~~ **корневого** сертификата для нового ~~европейского~~ **корневого** открытого ключа. Срок действия ~~европейского~~ **корневого** сертификата составляет 34 года и 3 месяца.

Примечание: Введение новой пары корневых ключей также означает, что ERCA создаст новый ключ старшего разряда для датчика движения и новый ключ старшего разряда DSRC; см. разделы ~~9.2.2.2 и 9.2.3.2~~ **9.2.1.2 и 9.2.2.2**.

CSM_57 До генерирования новой пары ~~европейских~~ **корневых** ключей ERCA проводит анализ криптографической надежности, необходимой для новой пары ключей, учитывая, что оно должно быть защищено на протяжении следующих 34 лет. При необходимости ERCA переходит на

последовательность шифров, более надежную по сравнению с текущей, как указано в ~~TCS_192~~ CSM_50.

CSM_58 Когда ERCA генерирует новую пару ~~европейских~~ корневых ключей, он создает соответствующий связующий сертификат для нового ~~европейского~~ **корневого** открытого ключа и подписывает его предыдущим ~~европейским~~ **корневым** закрытым ключом. Срок действия связующего сертификата составляет 17 лет **и 3 месяца**. Данный процесс также показан на **рис. 1** в разделе **9.1.7**.

Примечание: поскольку связующий сертификат включает в себя открытый ключ ERCA поколения *X* и подписан закрытым ключом ERCA поколения *X-1*, такой сертификат обеспечивает аппаратным средствам поколения *X-1* соответствующее средство доверия аппаратным средствам поколения *X*.

CSM_59 С момента вступления в силу нового сертификата корневого ключа ERCA больше не использует закрытый ключ пары корневых ключей ни для каких целей.

CSM_60 В любой момент времени ERCA располагает следующими криптографическими ключами и сертификатами:

- текущая пара ключей EUR и соответствующий сертификат;
- все прежние сертификаты EUR для проверки сертификатов MSCA, которые все еще действительны;
- связующие сертификаты для всех поколений сертификатов EUR, кроме первого.

9.1.3 ~~Уровень государства-члена~~ **Уровень государства-члена Договаривающейся стороны**

CSM_61 На уровне ~~государств-членов~~ **Договаривающихся сторон** все ~~государства-члены~~ **Договаривающиеся стороны**, которые должны подписать сертификаты карточек тахографов, генерируют одну или несколько уникальных пар ключей ECC под обозначением MSCA_Card. Все ~~государства-члены~~ **Договаривающиеся стороны**, которые должны подписать сертификаты для бортовых устройств или внешних устройств ГНСС, также генерируют одну или несколько уникальных пар ключей ECC, обозначаемых как MSCA_VU-EGF.

CSM_62 Задача генерирования пар ключей ~~государства-члена~~ **Договаривающейся стороны** должна выполняться Уполномоченным органом по сертификации ~~государства-члена~~ **Договаривающейся стороны** (MSCA). Когда MSCA генерирует пару ключей ~~государства-члена~~ **Договаривающейся стороны**, он передает открытый ключ ERCA, чтобы получить соответствующий сертификат ~~государства-члена~~ **Договаривающейся стороны**, подписанный ERCA.

CSM_63 MSCA должен выбрать уровень надежности пары ключей ~~государства-члена~~ **Договаривающейся стороны**, равный уровню надежности пары корневых ~~европейских~~ ключей, используемых для подписания соответствующего сертификата ~~государства-члена~~ **Договаривающейся стороны**.

CSM_64 Пара ключей MSCA_VU-EGF, если она есть, состоит из закрытого ключа MSCA_VU-EGF.SK и открытого ключа MSCA_VU-EGF.PK. MSCA использует закрытый ключ MSCA_VU-EGF.SK исключительно для подписания сертификатов открытых ключей бортовых устройств и внешних устройств ГНСС.

CSM_65 Пара ключей MSCA_Card состоит из закрытого ключа MSCA_Card.SK и открытого ключа MSCA_Card.PK. MSCA использует закрытый ключ MSCA_Card.SK исключительно для подписания сертификатов открытых ключей карточек тахографа.

- CSM_66 MSCA ведет учет всех подписанных сертификатов БУ, внешних устройств ГНСС и карточек вместе с идентификационными данными оборудования, для которого предназначен каждый сертификат.
- CSM_67 Срок действия сертификата MSCA_VU-EGF составляет 17 лет и 3 месяца. Срок действия сертификата MSCA_Card составляет 17 лет и 1 месяц.
- CSM_68 Как показано на **рисунке 1** в разделе **9.1.7**, закрытый ключ пары ключей MSCA_VU-EGF и закрытый ключ пары ключей MSCA_Card используются в течение двух лет.
- CSM_69 С момента окончания периода применения закрытого ключа пары ключей MSCA_VU-EGF MSCA больше не использует его ни для каких целей. Аналогичным образом с момента окончания периода применения закрытого ключа пары ключей MSCA_Card MSCA больше не использует его ни для каких целей.
- CSM_70 В любой момент времени MSCA располагает следующими криптографическими ключами и сертификатами:
- текущая пара ключей MSCA_Card и соответствующий сертификат;
 - все прежние сертификаты MSCA_Card для проверки сертификатов карточек тахографа, которые все еще действительны;
 - текущий сертификат EUR, необходимый для проверки текущего сертификата MSCA;
 - все прежние сертификаты EUR для проверки сертификатов MSCA, которые все еще действительны.
- CSM_71 Если от MSCA требуется подписывать сертификаты бортовых устройств или внешних устройств ГНСС, то он дополнительно располагает следующими ключами и сертификатами:
- текущая пара ключей MSCA_VU-EGF и соответствующий сертификат;
 - все прежние сертификаты MSCA_VU-EGF для проверки сертификатов БУ или внешних устройств ГНСС, которые все еще действительны.

9.1.4 Аппаратный уровень: бортовые устройства

- CSM_72 Для каждого бортового устройства генерируются две уникальные пары ключей ECC, обозначаемые как VU_MA и VU_Sign. Эту задачу выполняют изготовители БУ. При генерировании пары ключей БУ сторона, генерирующая ключ, передает открытый ключ ~~MSCA-страны, в которой она зарегистрирована,~~ **своему MSCA** с целью получить соответствующий сертификат БУ, подписанный MSCA. Закрытый ключ используется только бортовым устройством.
- CSM_73 У сертификатов VU_MA и VU_Sign данного бортового устройства срок действия сертификата один и тот же.
- CSM_74 Изготовитель БУ выбирает уровень надежности пары ключей БУ, который был бы равен по своему уровню надежности той паре ключей MSCA, которые используются для подписания соответствующего сертификата БУ.
- CSM_75 Бортовое устройство использует свою пару ключей VU_MA, состоящую из закрытого ключа VU_MA.SK и открытого ключа VU_MA.PK, исключительно для аутентификации БУ относительно карточек тахографов и внешних устройств ГНСС, как указано в разделах **10.3 и 11.4 настоящего приложения подраздела**.
- CSM_76 Бортовое устройство способно генерировать кратковременные пары ключей ECC и использует такую пару ключей исключительно для

согласования сеансовых ключей с карточкой тахографа или внешним устройством ГНСС, как указано в частях **10.4** и **11.4** настоящего приложения подраздела добавления.

- CSM_77 Бортовое устройство использует закрытый ключ VU_Sign.SK своей пары ключей VU_Sign исключительно для загрузки файлов данных, как указано в главе **14** настоящего приложения подраздела. Соответствующий открытый ключ VU_Sign.PK используется исключительно для проверки подписей, созданных бортовым устройством.
- CSM_78 Как показано на **рисунке 1** в разделе **9.1.7**, срок действия сертификата VU_MA составляет 15 лет и 3 месяца. Срок действия сертификата VU_Sign составляет также 15 лет и 3 месяца.

Примечания:

Продленный срок действия сертификата VU_Sign позволяет бортовому устройству создавать действительные подписи по отношению к загружаемым данным в течение первых трех месяцев по истечении его срока действия, ~~как требуется в Регламенте (ЕС)~~.

Продленный срок действия сертификата VU_MA нужен для аутентификации БУ по отношению к карточке контролера или карточке предприятия в течение первых трех месяцев по истечении его срока действия, с тем чтобы можно было загрузить соответствующие данные.

- CSM_79 С момента истечения срока действия соответствующего сертификата бортовое устройство не использует закрытый ключ пары ключей БУ ни для каких целей.
- CSM_80 После начала эксплуатации бортового устройства пары ключей БУ (кроме кратковременных пар ключей) и соответствующие сертификаты данного бортового устройства на месте не заменяются и не обновляются.

Примечания:

Данное требование не касается кратковременных пар ключей, так как новая кратковременная пара ключей генерируется БУ всякий раз, когда проводится аутентификация микросхемы и согласуются сеансовые ключи; см. раздел **10.4**. Следует отметить, что у кратковременных пар ключей соответствующих сертификатов нет.

Данное требование не исключает возможности замены статичных пар ключей БУ во время реконструкции или ремонта в защищенной среде, контролируемой изготовителем БУ.

- CSM_81 После ввода в эксплуатацию бортовые устройства содержат следующие криптографические ключи и сертификаты:
- текущая пара закрытых ключей VU_MA и соответствующий сертификат;
 - текущая пара закрытых ключей VU_Sign и соответствующий сертификат;
 - сертификат MSCA_VU-EGF, содержащий открытый ключ MSCA_VU-EGF.PK для проверки сертификата VU_MA и сертификата VU_Sign;
 - сертификат EUR, содержащий открытый ключ EUR.PK, для проверки сертификата MSCA_VU-EGF;
 - сертификат EUR, срок действия которого непосредственно предшествует сроку действия сертификата EUR, используемого для проверки сертификата MSCA_VU-EGF, если таковой существует;
 - связующий сертификат, соединяющий эти два сертификата EUR, если таковые существуют.

CSM_82 Помимо криптографических ключей и сертификатов, перечисленных в ~~TCS_223~~ **CSM_81**, в бортовых устройствах также есть ключи и сертификаты, указанные в части А настоящего ~~приложения~~ **подраздела**, позволяющие бортовому устройству вступать во взаимодействие с карточками тахографов первого поколения.

9.1.5 Аппаратный уровень: карточки тахографа

CSM_83 Для каждой карточки тахографа генерируется одна уникальная пара ключей ECC, обозначенная как Card_MA. Вторая уникальная пара ключей ECC, обозначенная как Card_Sign, дополнительно генерируется для каждой карточки водителя и каждой карточки мастерской. Эта задача может выполняться изготовителями карточек или учреждениями по персонализации карт. При генерировании пары ключей карточки сторона, генерирующая ключ, передает открытый ключ ~~MSCA страны, в которой она зарегистрирована,~~ **своему MSCA** с целью получить соответствующий сертификат карточки, подписанный MSCA. Закрытый ключ используется только карточкой тахографа.

CSM_84 У сертификатов Card_MA и Card_Sign данной карточки водителя или карточки мастерской сертификата один и тот же.

CSM_85 Изготовитель или учреждение по персонализации карточек выбирает уровень надежности пары ключей карточки, который был бы равен уровню надежности пары ключей MSCA, используемых для подписания соответствующего сертификата карточки.

CSM_86 Карточка тахографа использует свою пару ключей Card_MA, состоящую из закрытого ключа Card_MA.SK и открытого ключа Card_MA.PK, исключительно для взаимной аутентификации и согласования сеансового ключа по отношению к бортовому устройству, как указано в разделах **10.3 и 10.4 настоящего приложения подраздела**.

CSM_87 Карточка водителя и карточка мастерской используют закрытый ключ Card_Sign.SK своей пары ключей Card_Sign исключительно для подписи загруженных файлов данных, как указано в главе **14** настоящего ~~приложения~~ **подраздела**. Соответствующий открытый ключ Card_Sign.PK используется исключительно для проверки подписей, созданных бортовым устройством.

CSM_88 Срок действия сертификата Card_MA составляет, как указано ниже:

Карточки водителя: 5 лет

Карточки предприятия: ~~2 года~~ 5 лет

Карточки контролера: 2 года

Карточки мастерской: 1 год

CSM_89 Срок действия сертификата Card_Sign составляет, как указано ниже:

Карточки водителя: 5 лет и 1 месяц

Карточки мастерской: 1 год и 1 месяц

Примечание: Продленный срок действия сертификата Card_Sign позволяет карточке водителя создавать действительные подписи загружаемых данных в течение первого месяца после его истечения. ~~Это необходимо в соответствии с Регламентом (ЕС) № 581/2010, который требует, чтобы загрузку данных с карточки водителя можно было произвести в течение периода до 28 дней после записи последних данных.~~

CSM_90 После выдачи карточки данные пары ключей и соответствующие сертификаты данной карточки тахографа не меняются и не возобновляются.

- CSM_91 Карточки тахографа, после их выдачи, содержат следующие криптографические ключи и сертификаты:
- частный ключ Card_MA и соответствующий сертификат;
 - дополнительно для карточек водителя и мастерской: закрытый ключ Card_Sign и соответствующий сертификат;
 - сертификат MSCA_Card, содержащий открытый ключ MSCA_Card.PK для проверки сертификата Card_MA и сертификата Card_Sign;
 - сертификат EUR, содержащий открытый ключ EUR.PK, для проверки сертификата MSCA_Card;
 - сертификат EUR, срок действия которого непосредственно предшествует сроку действия сертификата EUR, используемого для проверки сертификата MSCA_Card, если таковой существует;
 - связующий сертификат, связывающий эти два сертификата EUR, если таковые существуют;
 - **кроме того, только для карточек контролера, карточек предприятия и карточек мастерской, и только в том случае, если такие карточки выдаются в течение первых трех месяцев срока действия нового сертификата EUR: сертификат EUR, который на два поколения старше, если он существует.**

Примечание к последнему абзацу: Например, в первые три месяца действия сертификата ERCA(3) (см. рис. 1) упомянутые карточки содержат сертификат ERCA(1). Это необходимо для того, чтобы эти карточки можно было использовать для загрузки данных с БУ ERCA(1), в случае которых обычный 15-летний срок службы плюс 3-месячный период загрузки данных истекает в течение этих месяцев; см. последний абзац требования 13) в добавлении 1С.

CSM_92 Помимо криптографических ключей и сертификатов, перечисленных в ~~ТCS_223~~ **CSM_91**, карточки тахографов также содержат ключи и сертификаты, указанные в части А настоящего ~~приложения~~ **подраздела**, которые позволяют этим карточкам взаимодействовать с БУ первого поколения.

9.1.6 Аппаратный уровень: внешние устройства ГНСС

- CSM_93 Для каждого внешнего устройства ГНСС генерируется одна уникальная пара ключей ECC, обозначаемая как EGF_MA. Эту задачу выполняют изготовители внешних устройств ГНСС. Во всех случаях, когда генерируется пара ключей EGF_MA, **стороне, генерирующей этот ключ**, передается открытый ключ ~~ее MSCA страны, в которой она проживает, чтобы~~ с целью получить соответствующий сертификат EGF_MA, подписанный MSCA. Закрытый ключ используется только устройством ГНСС.
- CSM_94 Изготовитель EGF выбирает уровень надежности пары ключей EGF_MA, который был бы равен уровню надежности пары ключей MSCA, используемых для подписания соответствующего сертификата EGF_MA.
- CSM_95 Внешнее устройство ГНСС использует свою пару ключей EGF_MA, состоящую из закрытого ключа EGF_MA.SK и открытого ключа EGF_MA.PK, исключительно для взаимной аутентификации и согласования сеансового ключа применительно к бортовым устройствам, как указано в разделе **11.4 настоящего приложения подраздела добавления**.
- CSM_96 Срок действия сертификата EGF_MA составляет 15 лет.

CSM_97 По истечении срока действия соответствующего сертификата внешнее устройство ГНСС не использует закрытый ключ пары ключей EGF_MA для соединения с бортовым устройством.

Примечание: Как поясняется в разделе **11.3.3**, EGF может, в принципе, использовать свой закрытый ключ для взаимной аутентификации применительно к БУ, с которым оно уже соединено, даже после истечения срока действия соответствующего сертификата.

CSM_98 После ввода EGF в действие пара ключей и соответствующий сертификат EGF_MA данного внешнего объекта ГНСС замене или обновлению в условиях эксплуатации не подлежат.

Примечание: Данное требование не исключает возможности замены пар ключей EGF во время восстановления или ремонта в защищенной среде, контролируемой изготовителем EGF.

CSM_99 После ввода в эксплуатацию внешнее устройство ГНСС содержит следующие криптографические ключи и сертификаты:

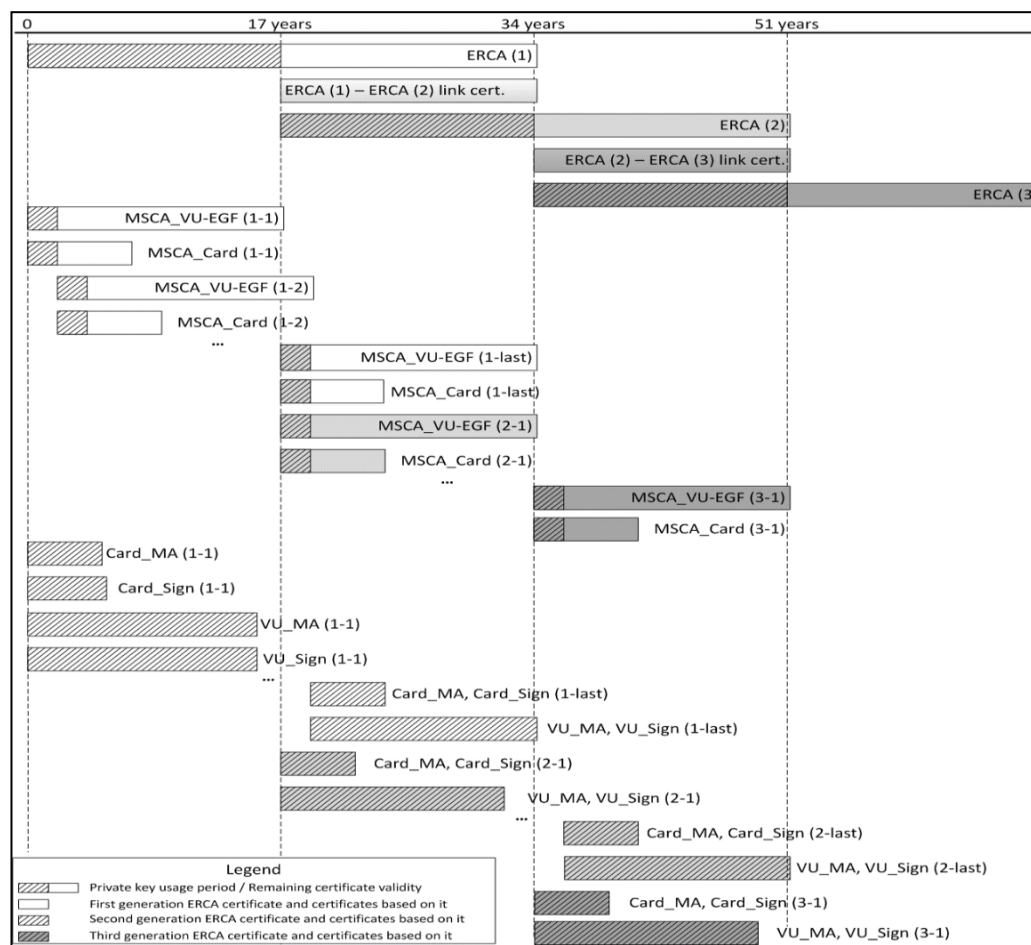
- текущая пара закрытых ключей EGF_MA и соответствующий сертификат;
- сертификат MSCA_VU-EGF, содержащий открытый ключ MSCA_VU-EGF.PK, используемый для проверки сертификата EGF_MA;
- сертификат EUR, содержащий открытый ключ EUR.PK, используемый для проверки сертификата MSCA_VU-EGF;
- сертификат EUR, срок действия которого непосредственно предшествует сроку действия сертификата EUR, используемого для проверки сертификата MSCA_VU-EGF, если таковой существует;
- связующий сертификат, соединяющий эти два сертификата EUR, если таковые существуют.

9.1.7 Обзор: замена сертификата

На **рис. 1** ниже показано, как выпускаются и с течением времени используются корневые сертификаты ERCA различных поколений, связующие сертификаты ERCA, сертификаты MSCA и сертификаты аппаратных средств (БУ и карточки):

Рис. 1

Выдача и использование корневых сертификатов ERCA различных поколений, связующих сертификатов ERCA, сертификатов MSCA и сертификатов оборудования



Примечания к рис. 1:

1. Различные поколения корневого сертификата обозначаются цифрой в скобках. Например, ERCA (1) — первое поколение корневого сертификата ERCA; ERCA (2) — второе поколение и т. д.
2. Другие сертификаты обозначаются двумя цифрами в скобках, первая из которых указывает на поколение выдачи корневого сертификата, вторая - на поколение самого сертификата. Например, MSCA_Card (1-1) — первый сертификат MSCA_Card, выданный по линии ERCA (1); MSCA_Card (2-1) — это первый сертификат MSCA_Card, выданный по линии ERCA (2); MSCA_Card (2-last) — это последний сертификат MSCA_Card, выданный по линии ERCA (2); Card_MA(2-1) — это первый сертификат «Card» для взаимной аутентификации, который выдается по линии ERCA (2) и т. д.
3. Сертификаты MSCA_Card (2-1) и MSCA_Card (1-last) выдаются почти в тот же день, но не совсем. MSCA_Card (2-1) — первый сертификат MSCA_Card, выдаваемый по линии ERCA (2), будет выдан немного позднее, чем MSCA_Card (1-last) — последний сертификат MSCA_Card, выдаваемый по линии ERCA (1).
4. Как показано на рисунке, первые сертификаты БУ и карточки, выдаваемые по линии ERCA (2), появятся почти за два года до последних сертификатов БУ и карточек, выпускаемых по линии ERCA (1). Это связано с тем, что сертификаты БУ и карточки выдаются в соответствии с процедурой выдачи сертификата MSCA, а не непосредственно в соответствии с процедурой выдачи сертификата ERCA. Сертификат MSCA (2-1) будет выдаваться непосредственно после вступления в силу ERCA (2), а сертификат MSCA (1-last) будет выдаваться лишь незадолго до истечения

срока действия, практически в последний момент, когда сертификат ERCA (1) будет еще действовать. Таким образом, срок действия этих двух сертификатов MSCA почти одинаковый, несмотря на то, что они принадлежат к разным поколениям.

5. Срок действия, указываемый в отношении карточек, — это срок действия карточек водителей (5 лет).

6. Ради экономии места разница в сроках действия между сертификатами Card_MA и Card_Sign ~~и между сертификатами VU_MA и VU_Sign~~ отображается только в случае первого поколения.

9.2 Симметричные ключи

9.2.1 Ключи для обеспечения связи между БУ и датчиком движения

~~9.2.2 Ключи для обеспечения связи DSRC~~

9.2.1.1 Общие положения

Примечание: предполагается, что читатели данного раздела знакомы с содержанием [ISO 16844-3], описывающего интерфейс между бортовым устройством и датчиком движения. Процесс соединения БУ и датчика движения детально изложен в главе 12 настоящего приложения подраздела.

CSM_100 В целях соединения бортовых устройств и датчиков движения для взаимной аутентификации между бортовыми устройствами и датчиками движения и для шифрования связи между бортовыми устройствами и датчиками движения необходим ряд симметричных ключей, как показано в ~~Таблице 45~~ **таблице 3**. Все эти ключи — это ключи AES, длина которых равна длине ключа старшего порядка датчиков движения, что связано с длиной (планируемой) пары ~~европейских~~ **корневых** ключей, как описано в ~~TCS_192~~ **CSM_50**.

Таблица 45 3

Ключи для обеспечения связи между БУ и датчиком движения

Ключ	Символ	Сгенерированный	Метод генерации	Хранится
Ключ старшего разряда датчика движения — часть БУ	K_{M-VUU}	ERCA	На произвольной основе	ERCA, MSCA, участвующие в выдаче сертификатов БУ, изготовители БУ, бортовые устройства
Ключ старшего разряда датчика движения — часть мастерской	K_{M-WC}	ERCA	На произвольной основе	ERCA, MSCA, изготовители карточек, карточки мастерской
Ключ старшего разряда датчика движения	K_M	Отдельно не генерируется	Рассчитывается как $K_M = K_{M-VU} \text{ XOR } K_{M-WC}$	ERCA, MSCA участвуют в выдаче ключей для датчиков движения (факультативно)*
Идентификационный ключ	K_{ID}	Отдельно не генерируется	Рассчитывается как $K_{ID} = K_M \text{ XOR } CV$, причем CV указывается в TCS_248CSM_106	ERCA, MSCA участвуют в выдаче ключей для датчиков движения (факультативно)*
Ключ сопряжения	K_P	Изготовитель датчиков движения	На произвольной основе	Один датчик движения

Ключ	Символ	Сгенерированный	Метод генерации	Хранится
Сессионный ключ	K _S	VU (во время сопряжения VU и датчика движения)	На произвольной основе	Один БУ и один датчик движения

* Хранение K_M и K_{ID} факультативно, так как эти ключи можно извлечь из K_{M-VU}, K_{M-WC} и CV.

CSM_101 Европейский Корневой сертификационный орган (ERCA) генерирует K_{M-VU} и K_{M-WC} — два произвольных и уникальных ключа AES, по которым ключ старшего порядка датчика движения K_M можно вычислить как K_{M-VU} XOR K_{M-WC}. ERCA передает K_M, K_{M-VU} и K_{M-WC} сертификационным органам государств-членов Договаривающимся сторонам по их просьбе.

CSM_102 Каждому ключу старшего порядка датчика движения K_M ERCA присваивает уникальный номер версии, который также используется для составления ключей K_{M-VU} и K_{M-WC} и для связанного с ними идентификационного ключа K_{ID}. Когда ERCA отправляет информацию MSCAs о направлении им K_{M-VU} и K_{M-WC}, он информирует их о номере версии.

Примечание: Номер версии используется для дифференции разных поколений этих ключей, как подробно поясняется в разделе 9.2.2.2 **9.2.1.2**.

CSM_103 Сертификационный орган государства-члена Договаривающейся стороны передает K_{M-VU} вместе с номером его версии изготовителям бортового устройства по их просьбе. Изготовители БУ включают K_{M-VU} и номер его версии во все изготавливаемые БУ.

CSM_104 Сертификационный орган государства-члена Договаривающейся стороны передает K_{M-VU} вместе с номером его версии изготовителям бортового устройства по их просьбе.

Примечания:

- См. описание типа данных SensorInstallationSecData в подразделе 2.
- Фактически, как объясняется в разделе 9.2.2.2 **9.2.1.2**, необходимо предусмотреть возможность включения в одну карточку мастерской несколько поколений K_{M-WC}.

CSM_105 Помимо ключа AES, указанного в TCS_246 **CSM_104**, MSCA следит за тем, чтобы ключ TDES K_{MWC}, указанный в требовании CSM_037 в части А настоящего приложения подраздела, был включен в каждую карточку мастерской, которая выдается под его ответственность.

Примечания:

- Это позволяет использовать карточку мастерской второго поколения для сопряжения с БУ первого поколения.
- На карточке мастерской второго поколения содержатся два разных приложения, одно из которых соответствует части В настоящего приложения подраздела, а второе — части А. Это последнее приложение как раз и содержит в себе ключ TDES K_{MWC}.

CSM_106 MSCA, который причастен к выпуску датчиков движения, извлекает идентификационный ключ из главного ключа датчика движения с использованием логического оператора XOR и постоянного вектора CV. Значение CV представляет собой следующее:

В случае 128-битных ключей старшего порядка датчика движения: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E45ED 83'

В случае 192-битных ключей старшего порядка датчика движения: CV = '72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25'

В случае 256-битных ключей старшего порядка датчика движения: CV = '1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60'

Примечание: Постоянные векторы генерируются следующим образом:

Pi_10 = первые 10 байтов десятичной доли математической константы π = '24 3F 6A 88 85 A3 08 D3 13 19'

CV_128-bits = первые 16 байтов SHA-256(Pi_10)

CV_192-bits = первые 24 байта SHA-384(Pi_10)

CV_256-bits = первые 32 байта SHA-512(Pi_10)

CSM_107 **Каждый изготовитель датчиков движения** генерирует произвольный и уникальный ключ K_R для сопряжения с каждым датчиком движения и передает каждый парный ключ **своему** сертификационному органу ~~государства-члена Договаривающейся стороны~~. MSCA шифрует каждый парный ключ отдельно с ключом старшего порядка датчика движения K_M и возвращает зашифрованный ключ изготовителю датчика движения. В случае каждого зашифрованного ключа MSCA сообщает изготовителю датчиков движения номер версии соответствующего K_M .

Примечание: Как поясняется в разделе ~~9.2.2.2~~ **9.2.1.2**, на самом деле изготовителю датчиков движения, возможно, придется генерировать несколько уникальных парных ключей для одного датчика движения.

CSM_108 **Каждый изготовитель датчиков движения** генерирует уникальный серийный номер для каждого датчика движения и передает все серийные номера **своему** сертификационному органу ~~государства-члена Договаривающейся стороны~~. MSCA шифрует каждый серийный номер отдельно с идентификационным ключом K_{ID} и возвращает зашифрованный серийный номер изготовителю датчика движения. В случае каждого зашифрованного ключа MSCA сообщает изготовителю датчиков движения номер версии соответствующего K_{ID} .

CSM_109 Что касается требований ~~TCS_249~~ **CSM_107** и ~~TCS_250~~ **CSM_108**, то MSCA использует алгоритм AES в режиме сцепления криптоблоков, как описано в [ISO 10116], с параметром чередования $m = 1$ и вектором инициализации SV = '00' {16}, т. е. шестнадцать байтов с двоичным значением, равным 0. При необходимости MSCA использует метод заполнения 2, определенный в [ISO 9797-1].

CSM_110 Изготовитель датчиков движения хранит зашифрованный парный ключ и зашифрованный серийный номер на предусмотренном датчике движения, вместе с соответствующими значениями в формате обычного текста и номером версии K_M и K_{ID} , используемым для шифрования.

Примечание: Как поясняется в разделе ~~9.2.2.2~~ **9.2.1.2**, на самом деле изготовителю датчиков движения, возможно, придется генерировать несколько зашифрованных парных ключей и несколько зашифрованных серийных номеров для одного датчика движения.

CSM_111 Помимо криптографического материала на базе AES, как описано в ~~TCS_252~~ **CSM_110**, изготовитель датчиков движения может также хранить в каждом датчике движения криптографический материал на базе TDES, как указано в требовании CSM_037 в части A настоящего ~~приложения подраздела~~.

Примечание: Как следствие, датчик движения второго поколения можно будет сопрягать с БУ первого поколения.

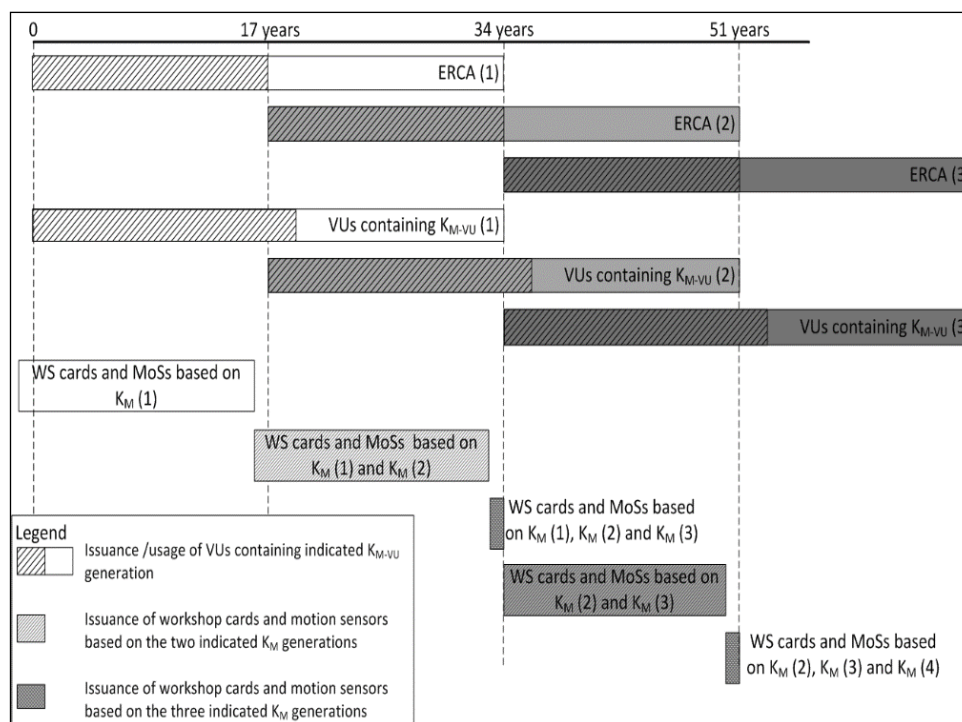
CSM_112 Длина сеансового ключа K_S , генерируемого БУ во время сопряжения с датчиком движения, связана с длиной его K_{M-VU} , как описано в TCS_192 CSM_50.

9.2.1.2 Замена ключа старшего порядка датчика движения в оборудовании второго поколения

CSM_113 Каждый старшего ключ датчика движения и все соответствующие ключи (см. ~~таблица 4~~ **таблица 3**) связаны с конкретным поколением пары корневых ключей ERCA. Как следствие, эти ключи заменяются через каждые 17 лет. Срок действия каждого поколения ключей старшего порядка датчиков движения начинается за год до вступления в действие соответствующей пары корневых ключей ERCA и заканчивается в тот момент, когда истекает срок действия соответствующей пары корневых ключей ERCA. Это показано на **рис. 2**.

Рис. 1

Генерирование и использование разных поколений ключей старшего порядка датчиков движения в бортовых устройствах, датчиках движения и карточках мастерской



CSM_114 По крайней мере, за один год до генерирования новой пары европейских корневых ключей, как описано в TCS_198 CSM_56, ERCA генерирует новый ключ старшего порядка датчика движения K_M посредством генерирования новых K_{M-VU} и K_{M-WC} . Длина ключа старшего порядка датчика движения связана с установленным уровнем надежности новой пары европейских корневых ключей в соответствии с TCS_192 CSM_50. ERCA передает MSCA новые K_M , K_{M-VU} и K_{M-WC} по их просьбе вместе с их номером версии.

CSM_115 MSCA следит за тем, чтобы все действующие поколения K_{M-WC} хранились на каждой карточке мастерской, выданной под его ответственность, вместе с номерами их версий, как показано на рис. 2.

Примечание: Это означает, что в последний год срока действия сертификата ERCA карточки мастерской выдаются с K_{M-WC} трех разных поколений, как показано на **рис. 2**.

CSM_116 Что касается процесса, описанного выше в ~~TCS_249~~ **CSM_107** и ~~TCS_250~~ **CSM_108**, то MSCA шифрует каждый парный ключ K_P , который он получает от изготовителя датчиков движения отдельно для каждого действующего поколения ключа старшего порядка датчика движения K_M . MSCA также шифрует каждый серийный номер, который он получает от изготовителя датчиков движения, отдельно для каждого действующего поколения идентификационного ключа K_{ID} . Изготовитель датчиков движения хранит все зашифрованные варианты парного ключа и все зашифрованные варианты серийного номера на предусмотренном датчике движения, вместе с соответствующими значениями в формате обычного текста и номером(ами) версии K_M и K_{ID} , используемым(и) для шифрования.

Примечание: Это означает, что в последний год срока действия сертификата ERCA датчики движения выдаются с зашифрованными данными на основе K_M трех разных поколений, как показано на рисунке 2.

CSM_117 Что касается процесса, описанного выше в ~~TCS_249~~ **CSM_107**, то поскольку длина ключа сопряжения K_P связана с длиной K_M (см. ~~TCS_242~~ (**TCS_253**), изготовителю датчиков движения, возможно, придется генерировать до трех разных парных ключей (разной длины) для одного датчика движения в том случае, если длина ключей K_M разных поколений будет разной. В этом случае изготовителю придется отправлять каждый ключ сопряжения в MSCA. MSCA следит за тем, чтобы каждый ключ сопряжения был зашифрован с учетом правильного генерирования ключа старшего порядка датчика движения, т. е. ключа такой же длины.

Примечание: Если изготовитель датчика движения решает генерировать для датчика движения второго поколения парный ключ на основе TDES (см. ~~TCS_253~~ **CSM_111**), то изготовитель извещает MSCA о том, что для шифрования данного парного ключа должен использоваться ключ старшего порядка датчика движения на основе TDES. Это связано с тем, что длина ключа TDES может быть равной длине ключа AES, вследствие чего MSCA не следует ориентироваться лишь на длину ключа.

CSM_118 Изготовители бортовых устройств включают в каждое бортовое устройство лишь одно поколение K_{M-VU} вместе с его номером версии. Это поколение K_{M-VU} связано с сертификатом ERCA, который положен в основу сертификатов БУ.

Примечание:

- В бортовое устройство, в основу которого положен сертификат ERCA поколения X , будет содержать только K_{M-VU} поколения X , даже если оно выпускается после начала срока действия сертификата ERCA поколения $X+1$. Этот момент показан на рис. 2.
- БУ поколения X нельзя подсоединять к датчику движения поколения $X-1$.
- Поскольку карточки мастерской действуют в течение года, все карточки мастерской, согласно ~~TCS_255~~ ~~TCS_260~~ **CSM_113–CSM_118**, будут содержать новый K_{M-WC} в момент выпуска первого БУ, содержащего новый K_{M-VU} . Таким образом, такое БУ всегда сможет рассчитать новый K_M . Кроме того, к тому времени большинство новых датчиков движения также будут содержать зашифрованные данные на основе нового K_M .

9.2.2 Ключи для обеспечения надежной связи DSRC

9.2.2.1 Общие положения

CSM_119 Подлинность и конфиденциальность данных, передаваемых из бортового устройства контрольному органу по каналу удаленной связи DSRC, обеспечивается при помощи ряда ключей AES, конкретно связанных с БУ, которые построены на основе единого ключа старшего порядка DSRC, — $K_{M_{DSRC}}$.

- CSM_120 Ключ старшего порядка DSRC — $K_{M_{DSRC}}$ представляет собой ключ AES, который в защищенном виде генерируется, хранится и распространяется ERCA. Длина ключа может быть 128, 192 или 256 битов и увязываться с длиной пары ~~европейских~~ корневых ключей, как описано в ~~FCS_192~~ CSM_50.
- CSM_121 ERCA передает ключ старшего порядка DSRC сертификационным органам ~~государства-члена~~ **Договаривающейся стороны** по их просьбе в защищенном виде, с тем чтобы они могли извлечь ключи DSRC, конкретно связанные с БУ, и проследить за тем, чтобы ключ старшего порядка DSRC был включен во все карточки контролера и карточки мастерской, выданные под их ответственность.
- CSM_122 Каждому ключу старшего порядка DSRC ERCA присваивает уникальный номер версии. Когда ERCA отправляет MSCA ключ старшего порядка DSRC, он доводит до их сведения номер версии.

Примечание: Номер версии используется для проведения различия между разными поколениями ключей старшего порядка DSRC, как это подробно поясняется в разделе ~~9.2.3.2~~ **9.2.2.2**.

- CSM_123 Для каждого бортового устройства изготовитель бортовых устройств создает уникальный серийный номер БУ и передает его сертификационному органу ~~своего~~ ~~государства-члена~~ **своей Договаривающейся стороны** с запросом на получение набора из двух ключей DSRC, связанных с конкретным БУ. Серийный номер БУ содержит данные типа `VuSerialNumber`, ~~при том что для кодирования применяются особые правила кодирования (DER) в соответствии с [ISO 8825-1].~~

Примечания:

- Этот серийный номер БУ должен быть идентичен элементу `vuSerialNumber` позиции `VuIdentification`, см. подраздел 1, и ссылке на держателя сертификата в сертификатах БУ.
- В тот момент, когда изготовитель бортового устройства запрашивает ключи DSRC для конкретного БУ, серийный номер БУ может быть неизвестен. В этом случае изготовитель БУ отправляет вместо него запрос на уникальный ИД сертификата, который он использовал в момент направления запроса на сертификаты БУ; см. CSM_153. В этой связи данный идентификатор запроса на сертификат должен быть равен ссылке держателя сертификата в сертификатах БУ.

- CSM_124 По получении запроса на ключи DSRC, связанные с конкретным БУ, MSCA генерирует два ключа AES для бортового устройства под обозначением $K_{VU_{DSRC_ENC}}$ и $K_{VU_{DSRC_MAC}}$. Длина этих ключей для конкретного БУ такая же, как длина ключа старшего порядка DSRC. MSCA использует функцию создания ключей, описанную в [RFC 5869]. Хеш-функция, необходимая для обработки хеш-функции HMAC, связана с длиной ключа старшего порядка DSRC, как описано в 0. Функция создания ключей в [RFC 5869] используется следующим образом:

Этап 1 (извлечение):

– $PRK = \text{HMAC-Hash}(salt, IKM)$, где *salt* — пустая строка ‘’, а *IKM* — $K_{M_{DSRC}}$.

Этап 2 (извлечение):

– $OKM = T(1)$, где

$T(1) = \text{HMAC-Hash}(PRK, T(0) \parallel info \parallel '01')$ с

$T(0) =$ пустая строка (‘’)

info = серийный номер БУ или идентификатор запроса на сертификат, как указано в ~~TCS_265~~ CSM_123

$K_{VU_{DSRC_ENC}}$ = первые L -октеты *ОКМ* и

$K_{VU_{DSRC_ENC}}$ = последние L -октеты *ОКМ*,

где L — требуемая длина $K_{VU_{DSRC_ENC}}$ и $K_{VU_{DSRC_MAC}}$ в октетах.

CSM_125 MSCA направляет $K_{VU_{DSRC_ENC}}$ и $K_{VU_{DSRC_MAC}}$ в защищенном виде изготовителю БУ для включения в предусмотренное бортовое устройство.

CSM_126 На выходе с конвейера в защищенном блоке памяти бортового устройства уже есть $K_{VU_{DSRC_ENC}}$ и $K_{VU_{DSRC_MAC}}$, что позволяет ему обеспечить целостность, подлинность и конфиденциальность данных, передаваемых по каналу удаленной связи. Бортовое устройство также хранит номер версии ключа старшего порядка DSRC, используемого в целях получения этих ключей для конкретного БУ.

CSM_127 На выходе с конвейера на контрольных карточках и карточках мастерской в защищенном блоке памяти уже есть $K_{M_{DSRC}}$, что позволяет ему проверить целостность и подлинность данных, передаваемых БУ по каналу удаленной связи, и расшифровать эти данные. На карточках контролера и карточках мастерской также хранится номер версии ключа старшего порядка DSRC.

Примечание: В принципе, как объясняется в пункте ~~9.2.3.2~~ 9.2.2.2, необходимо предусмотреть возможность включения в одну карточку мастерской или карточку контролера несколько поколений $K_{M_{DSRC}}$.

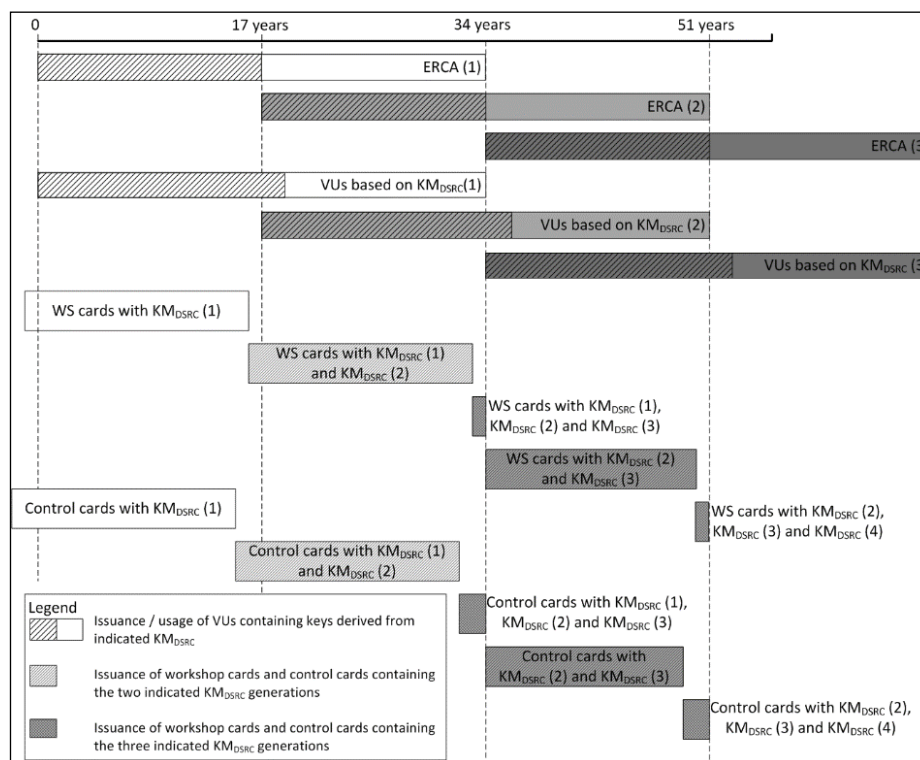
CSM_128 MSCA хранит записи обо всех созданных им ключах DSRC конкретных БУ, номере их версий и идентификационных данных БУ, для которого предназначен каждый набор ключей и серийном номере БУ или ИД запроса на сертификат, использованный для их создания.

9.2.2.2 ~~9.2.3.2~~ Замена ключа старшего порядка DSRC

CSM_129 Каждый ключ старшего порядка DSRC связан с определенным поколением пары корневых ключей ERCA. В этой связи ERCA заменяет ключ старшего порядка DSRC каждые 17 лет. Срок действия каждого поколения ключей старшего порядка DSRC начинается за два года до ввода в действие соответствующей пары корневых ключей ERCA и заканчивается в тот момент, когда истекает срок действия этой пары корневых ключей ERCA. Этот момент отражен на рис. 3.

Рис. 3

Генерирование и использование разных поколений ключей старшего порядка DSRC в бортовых устройствах, карточках мастерской и карточках контролера



CSM_130 По крайней мере за один год до генерирования новой пары европейских корневых ключей, как описано в TCS_198 CSM_56, ERCA генерирует новый ключ старшего порядка DSRC. Длина ключа DSRC связана с установленным уровнем надежности новой пары европейских корневых ключей в соответствии с TCS_192 CSM_50. ERCA передает новый ключ старшего порядка DSRC сертификационным органам MSCA по их просьбе вместе с их номером версии.

CSM_131 MSCA следит за тем, чтобы все действующие поколения KM_{DSRC} хранились на каждой карточке мастерской, изданной под его ответственность, вместе с номерами их версий, как показано на рис. 3.

Примечание: Это означает, что в последние два года срока действия сертификата ERCA карточки контролера выдаются с KM_{DSRC} трех разных поколений, как показано на рис. 3.

CSM_132 MSCA следит за тем, чтобы все поколения KM_{DSRC} , которые действовали, как минимум, в течение года и действуют до сих пор, хранились на каждой карточке мастерской, изданной под его ответственность, вместе с номерами их версий, как показано на рис. 3.

Примечание: Это означает, что в последний год срока действия сертификата ERCA карточки мастерской выдаются с KM_{DSRC} трех разных поколений, как показано на рис. 3.

CSM_133 Изготовители бортовых устройств включают в каждое бортовое устройство ключи DSRC, конкретно связанные с БУ, вместе с его номером версии. Этот набор ключей получают посредством генерации KM_{DSRC} в связи с сертификатом ERCA, который положен в основу сертификатов БУ.

Примечания:

Это означает, что бортовое устройство, в основу которого положен сертификат ERCA поколения X, содержит только K_VU_{DSRC}_ENC и K_VU_{DSRC}_MAC поколения X, даже если БУ выпускается после начала срока действия сертификата ERCA поколения X+1. Этот момент отражен на **рис. 3**.

Поскольку карточки мастерской действительны в течение одного года, а карточки контролера в течение двух лет, результатом является то, что согласно ~~TCS_273–TCS_275~~ **CSM_131– CSM_133** в момент выпуска первого БУ, содержащего конкретно связанные с ним ключи, которые создаются на основе того же ключа старшего порядка, все карточки мастерской и карточки контролера будут содержать новый ключ старшего порядка DSRC.

9.3 Сертификаты

9.3.1 Общие положения

CSM_134 Все сертификаты европейской системы смарт-тахографов являются сертификатами, не требующими дополнительного описания, с возможностью проверки по карточке (CV) в соответствии с [ISO 7816-4] и [ISO 7816-8].

CSM_135 Для шифрования структур данных ASN.1 и (связанных с конкретным приложением) объектов данных в сертификатах применяются особые правила шифрования (DER) в соответствии с [ISO 8825-1]. **В таблице 4 показано полное шифрование сертификата, включая все байты метки и длины.**

Примечание: Результатом такого шифрования является следующая структура значения длины метки (TLV):

- метка: метка шифруется одним или двумя октетами и указывает на содержание;
- длина: длина шифруется как неподписанное целое число одним, двумя или тремя октетами, в результате чего максимальная длина составляет 65 535 октетов. Используется минимальное число октетов;
- значение шифруется с помощью нулевого или большего количества октетов.

9.3.2 Содержание сертификатов

CSM_136 Структура всех сертификатов показана в описании сертификата в **таблице 4 46**.

Таблица 4
Описание сертификата, версия 1

Поле	ИД поля	Valise	Длина (байты)	Тип данных ASN.1 (см. добавление 1)
Сертификат ECC	C	'7F 21'	перемен.	
Текст сертификата ECC	B	'7F 4E'	перемен.	
Идентификатор описания сертификата	CPI	'5F 29'	'01'	ЦЕЛОЕ ЧИСЛО (0..255)
Ссылка на орган по сертификации	CAR	'42'	'08'	KeyIdentifier
Разрешение держателя сертификата	CHA	'5F 4C'	'07'	CertificateHolderAuthorisation
Открытый ключ	PK	'7F 49'	перемен.	
Параметры домена	DP	'06'	перемен.	ИДЕНТИФИКАТОР ОБЪЕКТА
Открытая точка	PP	'86'	перемен.	ОКТЕТНАЯ СТРОКА
Ссылка на держателя сертификата	CHR	'5F 20'	'08'	KeyIdentifier

Поле	ИД поля	Balise	Длина (байты)	Тип данных ASN.1 (см. добавление 1)
Дата введения сертификата в действие	CEfD	'5F 25'	'04'	Реальное время
Дата истечения срока действия сертификата	CExD	'5F 24'	'04'	Реальное время
Подпись сертификата ECC	S	'5F 37'	перемен.	ОКТЕТНАЯ СТРОКА

Примечание: ИД поля используется в последующих частях настоящего приложения подраздела с целью указать на отдельные поля сертификата, например, X.CAR — это указатель органа по сертификации, содержащийся в сертификате пользователя X.

9.3.2.1 Идентификатор описания сертификата

CSM_137 Идентификатор описания сертификата используется в сертификатах для указания на его описание, взятое за основу. Версия 1, как указано в таблице 4 46, идентифицируется значением '00'.

9.3.2.2 Ссылка на орган по сертификации

CSM_138 Ссылка на орган по сертификации используется для идентификации открытого ключа, который надлежит использовать для проверки подписи сертификата. Таким образом, ссылка на орган по сертификации в его сертификате равнозначна указателю на держателя сертификата.

CSM_139 Корневой сертификат ERCA является самоподписывающимся, т. е. ссылка на орган по сертификации и указатель на держателя сертификата в сертификате равнозначны.

CSM_140 Что касается связующего сертификата ERCA, то указатель на держателя сертификата равнозначен CHR нового корневого сертификата ERCA. Ссылка на орган по сертификации в связующем сертификате равнозначен CHR прежнего корневого сертификата ERCA.

9.3.2.3 Полномочия держателя сертификата

CSM_141 Полномочия держателя сертификата используются для идентификации типа сертификата. Он состоит из шести старших байтов идентификатора приложения тахографа, конкатенированных с типом оборудования, для которого предназначен сертификат, с типом оборудования, указывающим именно на тип оборудования, для которого предназначен этот сертификат. В случае сертификата БУ, сертификата карточки водителя или сертификата карточки мастерской тип оборудования также используется для проведения различия между сертификатом на взаимную аутентификацию и сертификатом на создание цифровых подписей (см. раздел 9.1 и подраздел 1, тип данных «EquipmentType»).

9.3.2.4 Открытый ключ

Открытый ключ включает в себя два элемента данных: стандартизированные параметры домена, используемые с открытым ключом в сертификате, и значение открытой точки.

CSM_142 Элемент данных параметров домена содержит один из идентификаторов объектов, упомянутых в таблице 1 43, с целью указать на набор стандартизированных параметров домена.

CSM_143 Элемент данных открытой точки содержит в себе параметры открытой точки. Открытые точки эллиптической кривой преобразуются в октетные строки, как указано в [TR-03111]. В этом случае используется несжатый формат шифрования. При восстановлении точки эллиптической кривой из зашифрованного формата всегда проводятся проверки, описанные в [TR-03111].

9.3.2.5 Ссылка на держателя сертификата

- CSM_144 Ссылка на держателя сертификата представляет собой своего рода идентификатор открытого ключа, содержащегося в сертификате. Она используется для указания этого открытого ключа в других сертификатах.
- CSM_145 В случае сертификатов карточек и сертификатов внешних устройств ГНСС ссылка на держателя сертификата содержит данные типа ExtendedSerialNumber, указанные в ~~приложении~~ **подразделе 1**.
- CSM_146 В случае бортовых устройств изготовитель, подавая запрос на сертификат, необязательно знает серийный номер БУ изготовителя, для которого предназначен этот сертификат и связанный с ним закрытый ключ. В первом случае ссылка на держателя сертификата содержит тип данных ExtendedSerialNumber, указанный в **приложении подразделе 1**. Во втором случае ссылка на держателя сертификата содержит тип данных CertificateRequestID, указанный в **приложении подразделе 1**.

Примечание: Для сертификата карточки значение CHR должно быть равно значению cardExtendedSerialNumber в EF_ICC; см. Подраздел 2. Для сертификата EGF значение CHR должно быть равно значению sensorGNSSSerialNumber в EF_ICC; см. подраздел 14. Для сертификата БУ значение CHR должно быть равно элементу vuSerialNumber идентификационным данным VuIdentification, см. подраздел 1, если только изготовитель не знает серийный номер конкретного изготовителя на момент запроса сертификата.

- CSM_147 Для сертификатов ERCA и MSCA ссылка на держателя сертификата должна соответствовать данным типа CertificationAuthorityKID, указанного в ~~приложении~~ **подразделе 1**.

9.3.2.6 Дата введения сертификата в действие

- CSM_148 Дата введения сертификата в действие указывает на дату и время начала срока действия сертификата. ~~Датой введения сертификата в действие является дата генерации сертификата.~~

9.3.2.7 Дата истечения срока действия сертификата

- CSM_149 Дата введения сертификата в действие указывает на дату и время начала срока действия сертификата.

9.3.2.8 Подписание сертификата

- CSM_150 Подпись на сертификате создается по зашифрованной основной части сертификата, включая метку и длину основной части сертификата. Алгоритмом подписи является ECDSA, как указано в [DSS], с использованием алгоритма хеширования, связанного с размером ключа подписывающего органа, как указано в ~~TCS_19~~ **CSM_50**. Формат подписи обычный, как указано в [TR-03111].

9.3.3 Запрос на сертификаты

- CSM_151 При подаче запроса на сертификат ~~заявитель~~ **соответствующий MSCA** передает **ERCA** своему сертификационному органу следующие данные:

идентификатор описания запрашиваемого сертификата;

указатель органа по сертификации, в который планируется обратиться за подписью сертификата;

открытый ключ, подлежащий подписи.

- CSM_152 Помимо данных в ~~TCS_293~~ **CSM_151**, MSCA направляет следующие данные в запросе на сертификат ERCA, что позволяет ERCA создать для

нового сертификата соответствующую ссылку на держателя сертификата:

цифровой код государства, в котором находится орган по сертификации (тип данных NationNumeric, определенный в ~~приложении~~ **подразделе 1**);

буквенно-цифровой код государства, в котором находится орган по сертификации (тип данных NationAlpha, определенный в ~~приложении~~ **подразделе 1**);

1-байтовый серийный номер в целях дифференциации разных ключей органа по сертификации в случае смены ключей;

двухбайтовое поле, содержащее конкретную дополнительную информацию, касающуюся органа по сертификации.

CSM_153 ~~Помимо данных в TCS_293,~~ Соответствующий изготовитель оборудования направляет MSCA следующие данные в запросе на сертификат, что позволяет MSCA создать для нового сертификата на оборудование соответствующую ссылку на держателя сертификата:

~~идентификатор типа оборудования конкретного производителя;~~

серийный номер оборудования, если он известен (см. ~~TCS_296~~ **CSM_154**), который является уникальным для данного изготовителя, тип оборудования и месяц изготовления. В противном случае — уникальный идентификатор запроса на сертификат;

месяц и год изготовления оборудования или запроса на сертификат.

Изготовитель следит за тем, чтобы эта дата была правильной и чтобы выданный MSCA сертификат был введен в оборудование, для которого он предназначен.

CSM_154 В случае бортовых устройств изготовитель, подавая запрос на сертификат, необязательно знает серийный номер БУ изготовителя, для которого предназначен этот сертификат и связанный с ним закрытый ключ. Если серийный номер известен, то изготовитель БУ передает его MSCA. Если он неизвестен, изготовитель присваивает уникальный идентификатор каждому запросу на сертификат и передает этот серийный номер запроса MSCA. Выданный впоследствии сертификат будет содержать серийный номер запроса на этот сертификат. После ввода сертификата в соответствующее БУ изготовитель передает MSCA параметры связи между серийным номером запроса на сертификат и идентификационными данными БУ.

10. Взаимная аутентификация и безопасный обмен сообщениями с карточкой БУ

10.1 Общие положения

CSM_155 На высоком уровне защищенная связь между бортовым устройством и карточкой тахографа осуществляется в следующем порядке:

- во-первых, каждая сторона подтверждает другой стороне наличие у нее действительного сертификата открытого ключа, подписанного сертификационным органом ~~государства-члена~~ **Договаривающейся стороны**. Сертификат открытого ключа MSCA в свою очередь должен быть подписан ~~европейским~~ **корневым** сертификационным органом. Данный этап именуется проверкой сертификата на последовательность и подробно рассматривается в разделе **10.2**;
- во-вторых, бортовое устройство подтверждает карточке наличие у него закрытого ключа, соответствующего открытому ключу в представленном сертификате. В этой связи оно подписывает произвольное число, присланное

карточкой. Карточка проверяет подпись, сгенерированную под этим произвольным числом. Если проверка выполнена успешно, то БУ считается аутентифицированным. Данный этап именуется аутентификацией БУ и подробно рассматривается в разделе **10.3**;

- в-третьих, обе стороны самостоятельно рассчитывают два сеансовых ключа AES с использованием алгоритма согласования асимметричного ключа. С помощью одного из этих сеансовых ключей карточка создает соответствующий код аутентификации сообщения (MAC), связанный с некоторыми данными, переданными из БУ. БУ проверяет MAC. Если проверка выполнена успешно, происходит аутентификация карточки. Данный этап именуется проверкой аутентификации карточки и подробно рассматривается в разделе **10.4**;
- в-четвертых, БУ и карточка используют согласованные сеансовые ключи в целях обеспечения конфиденциальности, целостности и подлинности всех передаваемых сообщений. Данный этап именуется защищенным обменом сообщениями и подробно рассматривается в разделе **10.5**.

CSM_156 Механизм, описанный в ~~TCS_297~~ **CSM_155**, вводится в действие бортовым устройством всякий раз, когда в одно из его считывающих устройств вводится соответствующая карточка.

10.2 Взаимная проверка последовательности сертификата

10.2.1 Проверка последовательности сертификата карточки БУ

CSM_157 Для проверки последовательности сертификата карточки тахографа бортовые устройства используют протокол, отображенный на рисунке 4. **В случае каждого сертификата, считываемого с карточки, БУ проверяет правильность поля «Полномочия держателя сертификата» (СНА):**

- **поле СНА сертификата карточки должно указывать на соответствующий сертификат карточки в целях взаимной аутентификации (см. подраздел 1, тип данных «EquipmentType»);**
- **СНА сертификата Card.CA указывает на MSCA;**
- **СНА сертификата Card.CA указывает на ERCA.**

Примечания к рисунку 4:

- Сертификаты карточки и открытые ключи, указанные на рисунке, предназначены для взаимной аутентификации. В части **9.1.5** они указаны под обозначением Card_MA.
- Сертификаты Card.CA и открытые ключи, указанные на рисунке, предназначены для подписания сертификатов карточек, как указано в CAR сертификата соответствующей карточки. В части **9.1.3** они указаны под обозначением MSCA_Card.
- Сертификаты Card.CA.EUR, указанные на рисунке, представляют собой ~~европейский~~ **европейский** корневой сертификат, который указан в CAR сертификата Card.CA.
- Сертификат Card.Link, указанный на рисунке, — это связующий сертификат карточки, если он имеется. Как указано в части **9.1.2**, это — связующий сертификат для новой пары ~~европейских~~ **европейских** корневых ключей, созданной ERCA и подписанной прежним ~~европейским~~ **европейским** **корневым** закрытым ключом.
- Сертификат Card.Link.EUR представляет собой ~~европейский~~ **европейский** корневой сертификат, который указан в CAR сертификата Card.Link.

CSM_158 Как показано на **рис. 4**, проверка последовательности сертификата карточки начинается с момента ввода карточки. Бортовое устройство считывает ссылку на владельца карточки (cardExtendedSerialNumber) из EF ICC. БУ проверяет, известна ли ему эта карточка, т. е. была ли в прошлом проведена успешная проверка последовательности сертификата карточки, которая была сохранена в целях ее использования в будущем. Если она известна и если сертификат карточки все еще действителен, то процесс продолжается в виде проверки последовательности цепочки сертификата БУ. В противном случае БУ после этого считывает с карточки сертификат MSCA_Card в целях его использования для проверки сертификата карточки Card.CA. Сертификат EUR, подлежащий использованию для проверки сертификата MSCA_Card и, в случае применимости, связующего сертификата, используется до тех пор, пока не будет найден известный ему сертификат или сертификат, который он может проверить. Если такой сертификат найден, то БУ использует его для проверки базовых сертификатов карточек, которые он считывает с данной карточки. В случае успеха этот процесс продолжается в виде проверки последовательности цепочки сертификатов БУ. Если этот сертификат не найден, БУ эту карточку игнорирует.

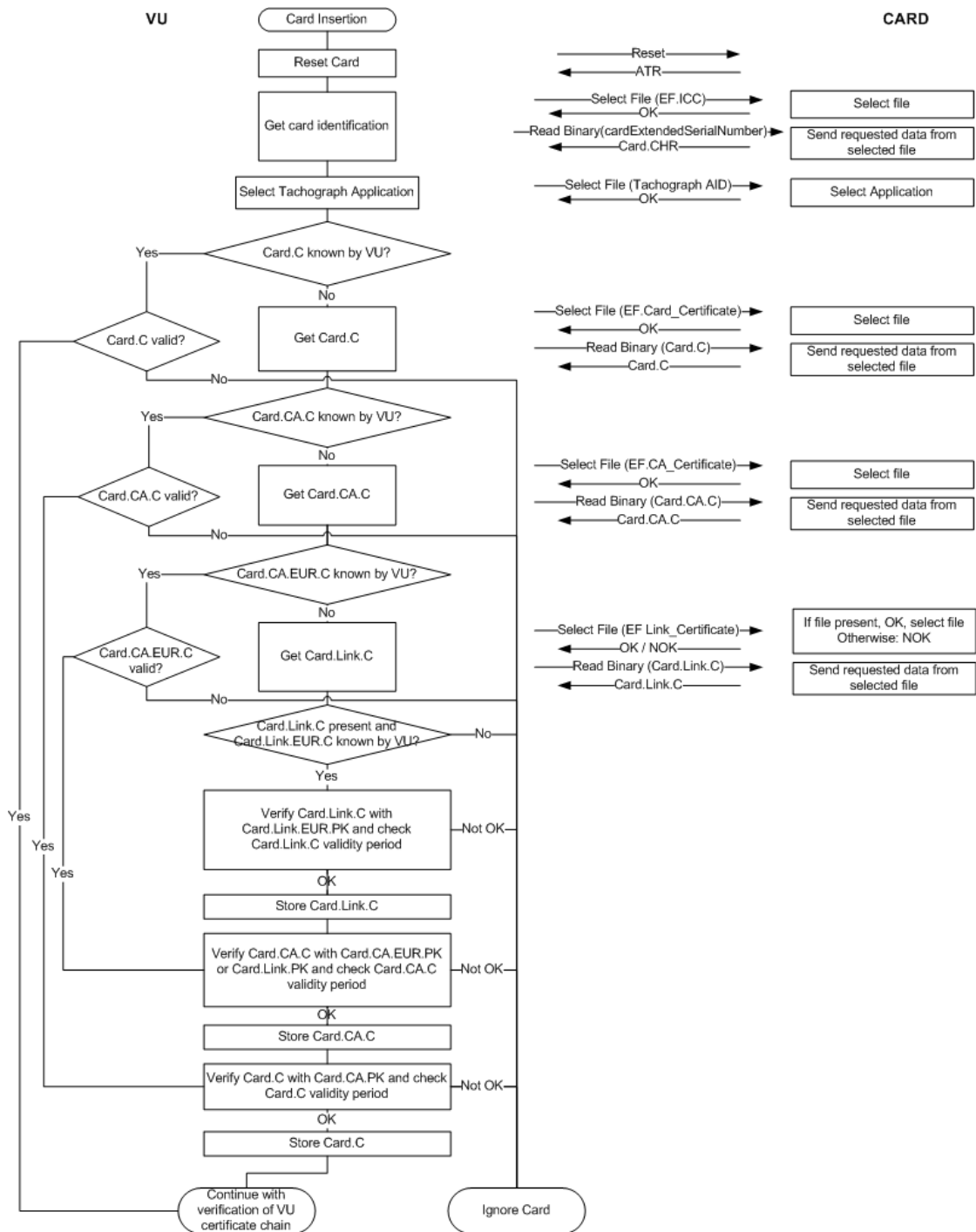
Примечание: Есть три способа, по которым БУ может распознать данный сертификат Card.CA.EUR:

- сертификат Card.CA.EUR — это тот же самый сертификат, что и собственный сертификат EUR БУ;
- сертификат Card.CA.EUR предшествует собственному сертификату EUR БУ, поэтому данный сертификат уже содержался в БУ в момент его ввода в эксплуатацию (см. CSM_81);
- сертификат Card.CA.EUR выдан позднее собственного сертификата EUR БУ, но в прошлом БУ получил связующий сертификат с другой карточки тахографа, проверил его и сохранил на будущее.

CSM_159 Как показано на **рисунке 4**, как только БУ проверит аутентичность и действительность ранее неизвестного сертификата, он может сохранить его на будущее, с тем чтобы не проверять еще раз его подлинность, если он будет опять введен в БУ. Вместо хранения всего сертификата БУ может сохранить только содержание его основной части, как указано в части **9.3.2. Если хранение всех других типов сертификатов является необязательным, то в случае БУ хранение нового связующего сертификата, представленного в соответствующей карточке, является обязательным.**

CSM_160 БУ проверяет срок действия любого сертификата, считываемого с карточки или хранящегося в его памяти, и отклоняет просроченные сертификаты. Для проверки срока действия сертификата, представленного карточкой, БУ использует внутренние часы.

Рис. 4
Протокол проверки последовательности сертификатов карточки бортовым устройством



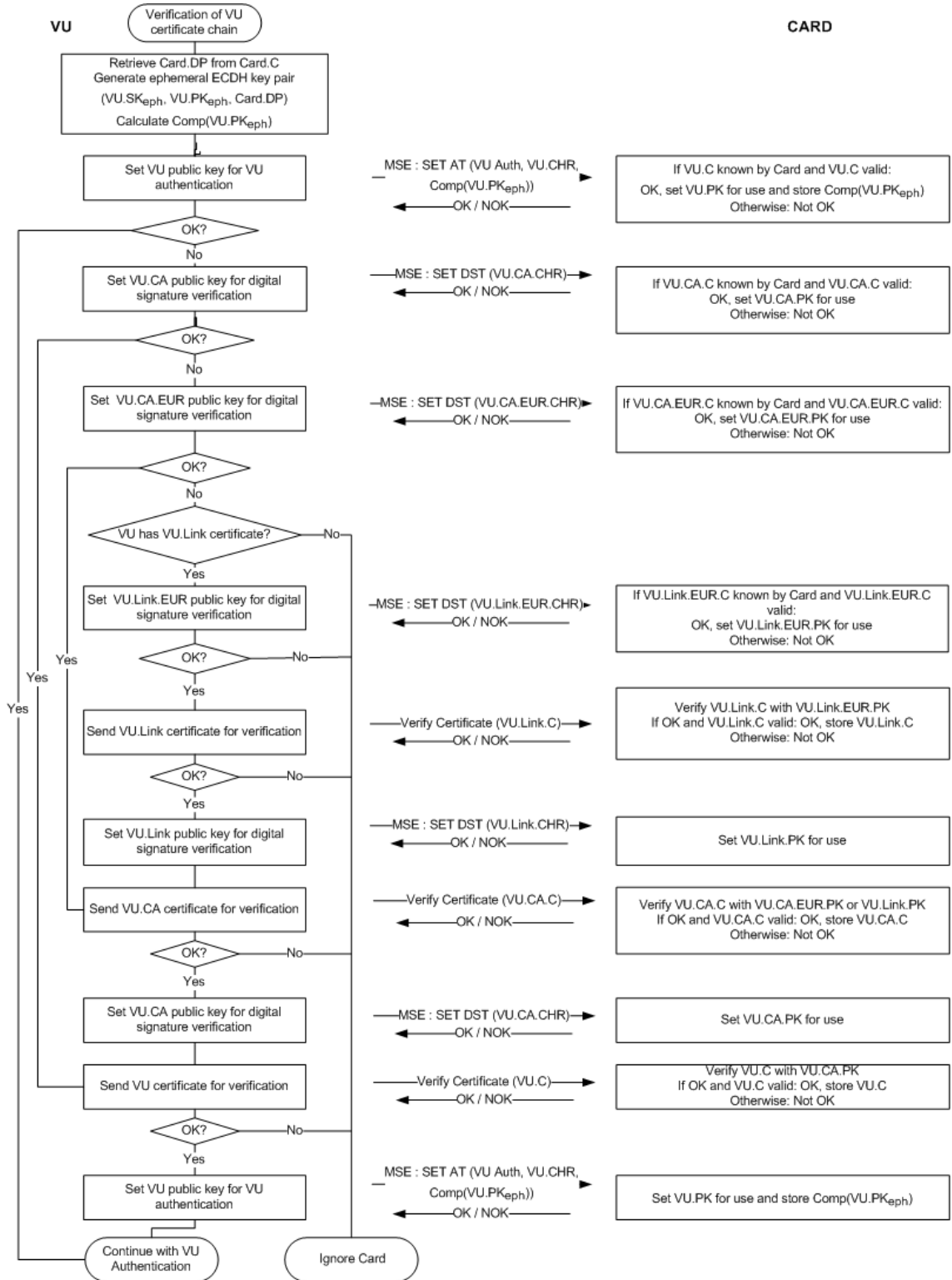
10.2.2 Проверка последовательности сертификатов в БУ карточкой

CSM_161 Для проверки последовательности сертификатов в БУ карточкой тахографа используется протокол, отображенный на рисунке 5. **В случае каждого сертификата, сохраненного в БУ, карточка проверяет правильность поля «Полномочия держателя сертификата» (СНА):**

- СНА сертификата VU.Link указывает на ERCA;
- СНА сертификата VU.CA указывает на MSCA.

Рис. 5
Протокол проверки последовательности сертификатов в БУ с помощью карточки

– Поле СНА сертификата БУ указывает на сертификат БУ в целях взаимной аутентификации (см. подраздел 1, тип данных «EquipmentType»).



Примечания к рисунку:

- Сертификаты БУ и открытые ключи, указанные на рисунке, предназначены для взаимной аутентификации. В части **9.1.4** они указаны под обозначением VU_MA.
- Сертификаты VU.CA и открытые ключи, указанные на данном рисунке, предназначены для подписания сертификатов БУ и внешнего устройства ГНСС. В разделе **9.1.3** они указаны под обозначением MSCA_VU-EGF.
- Сертификат VU.CA.EUR, указанный на рисунке, представляют собой ~~европейский~~ корневой сертификат, который указан в CAR сертификата VU.CA.
- Сертификат VU.Link, указанный на рисунке, представляет собой связующий сертификат БУ, если таковой имеется. Как указано в части **9.1.2**, это — связующий сертификат для новой пары ~~европейских~~ корневых ключей, созданной ERCA и подписанной прежним ~~европейским~~ **корневым** закрытым ключом.
- Сертификат VU.Link.EUR представляют собой ~~европейский~~ корневой сертификат, который указан в CAR сертификата VU.Link.

CSM_162 Как показано на **рисунке 5**, проверка последовательности сертификатов бортового устройства начинается с того, что бортовое устройство попытается сначала установить свой собственный открытый ключ для его использования в карточке тахографа. Если эта попытка окажется успешной, то это будет означать, что данная карточка успешно проверила последовательность сертификатов БУ в прошлом и сохранила данный сертификат БУ в целях его дальнейшего использования. В этом случае сертификат БУ признается пригодным для использования, и данный процесс продолжается в порядке аутентификации БУ. Если сертификат БУ карточке неизвестен, то БУ последовательно выдает сертификат VU.CA для проверки ее сертификата БУ, сертификат VU.CA.EUR для проверки сертификата VU.CA и, возможно, связующий сертификат для обнаружения известного сертификата или сертификата, который карточка может проверить. Если такой сертификат обнаружен, то карточка использует этот сертификат для проверки базовых сертификатов, которые были в нее введены ранее. В случае успеха БУ окончательно настраивает свой открытый ключ для его использования в карточке тахографа. Если данная попытка оказалась безуспешной, то БУ игнорирует карточку.

Примечание: Есть три способа, позволяющие БУ распознать сертификат VU.CA.EUR:

- Сертификат VU.CA.EUR — это тот же самый сертификат, что и собственный сертификат EUR карточки.
- Сертификат VU.CA.EUR предшествует собственному сертификату EUR карточки, и этот сертификат уже содержался на карточке в момент ее ввода в эксплуатацию (см. CSM_91).
- Сертификат VU.CA.EUR выдан позднее собственного сертификата EUR карточки, но в прошлом карточка получила связующий сертификат с другого бортового устройства, проверила его и сохранила на будущее.

CSM_163 БУ использует команду MSE: Set AT для установки своего открытого ключа в целях его использования в карточке тахографа. Как указано в ~~добавлении~~ **подразделе 2**, эта команда содержит указание на криптографический механизм, который будет использоваться с установленным ключом. Этот механизм представляет собой аутентификацию БУ на основе алгоритма ECDSA в сочетании с алгоритмом хеширования, связанным с размером ключа пары ключей БУ VU_MA, как указано в ~~TCS_192~~ **CSM_50**.

- CSM_164 Команда MSE: Set AT также содержит указание на кратковременную пару ключей, которую БУ использует во время согласования сеансовых ключей (см. часть **10.4**). В этой связи перед тем как передать команду MSE: Set AT, БУ генерирует кратковременную пару ключей ECC. Для генерирования такой кратковременной пары ключей БУ использует стандартизированные параметры домена, указанного в сертификате карточки. Это кратковременная пара ключей обозначается как $(VU.SK_{eph}, VU.PK_{eph}, Card.DP)$. В качестве идентификатора ключа БУ принимает координату x эфемерной открытой точки ECDH; этот порядок носит название «сжатое представление открытого ключа» и обозначается как $Comp(VU.PK_{eph})$.
- CSM_165 Если команда MSE: Set AT выполнена успешно, то карточка устанавливает указанный VU.PK в целях последующего использования во время аутентификации транспортного средства и временно хранит $Comp(VU.PK_{eph})$. Если до согласования сеансовых ключей передаются две или несколько команд MSE: Set AT, то карточка сохраняет только последнюю полученную команду $Comp(VU.PK_{eph})$. **Если команда GENERAL AUTHENTICATE прошла, то карточка устанавливает $Comp(VU.PK_{eph})$ в исходное положение.**
- CSM_166 Карточка проверяет срок действия любого сертификата, считываемого с БУ или хранящегося в его памяти, и отклоняет просроченные сертификаты.
- CSM_167 Для проверки срока действия сертификата, представленного БУ, каждая карточка тахографа на внутреннем уровне сохраняет в своем блоке памяти некоторые данные, указывающие на текущий момент времени. На уровне БУ эти данные напрямую не обновляются. В момент сдачи в эксплуатацию текущее время карточки устанавливается в качестве фактической даты сертификата Card_MA карточки. Карточка обновляет свое текущее время в том случае, если фактическая дата аутентичного «действительного источника времени» сертификата, представленного БУ, более поздняя, чем текущее время карточки. В таком случае карточка устанавливает свое текущее время по фактической дате этого сертификата. В качестве действительного источника времени карточка принимает только следующие сертификаты:
- связующие сертификаты ERCA второго поколения;
 - сертификаты MSCA второго поколения;
 - сертификаты БУ второго поколения, выданные той же страной, что и собственный(е) сертификат(ы) карточки.

Примечание: Последнее требование означает, что карточка способна распознавать CAR сертификата БУ, т. е. сертификата MSCA_VU-EGF. Он будет отличаться от CAR ее собственного сертификата, т. е. сертификата MSCA_Card.

- CSM_168 Как показано на **рис. 5**, как только карточка проверит аутентичность и действительность ранее неизвестного сертификата, она может сохранить его на будущее, с тем чтобы не проверять еще раз подлинность этого сертификата, если он будет опять введен в карточку. Вместо хранения всего сертификата карточка может сохранить только содержание основной части сертификата, как указано в разделе 9.3.2.

10.3 Аутентификация БУ

- CSM_169 В целях аутентификации БУ по отношению к карточке бортовые устройства и карточки используют протокол аутентификации БУ, отображенный на **рис. 6**. Аутентификация БУ позволяет карточке тахографа однозначно проверить подлинность БУ. В этой связи для

подписания запросов, сгенерированных карточкой, БУ использует закрытый ключ.

CSM_170 Помимо запроса карточки, БУ включает в подпись ссылку на держателя ~~карточки~~ сертификата, взятую из сертификата карточки.

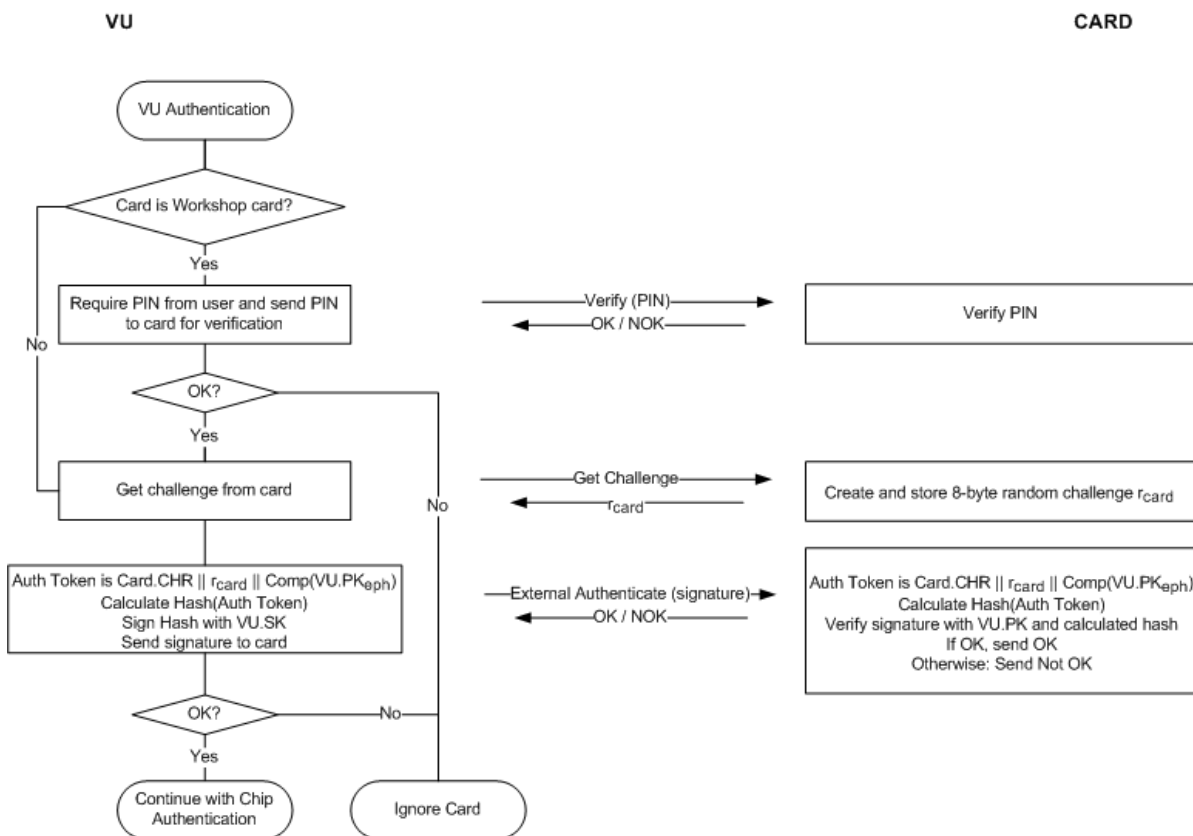
Примечание: Это позволяет обеспечить такое положение, при котором карточка, по которой производится аутентификация БУ, является той же самой карточкой, которую БУ уже проверяло на предмет последовательности сертификата.

CSM_171 БУ также включает в подпись идентификатор кратковременного открытого ключа $\text{Comp}(VU.PK_{eph})$, который БУ использует для настройки на защищенный обмен сообщениями в процессе аутентификации микросхемы, указанный в части 10.4.

Примечание: Это позволяет обеспечить такую схему, в случае которой БУ, с которым карточка установила связь в ходе сеанса защищенного обмена сообщениями, будет тем же самым БУ, который был аутентифицирован данной карточкой.

Рис. 6

Протокол аутентификации БУ



CSM_172 Если в процессе аутентификации БУ передает несколько команд GET CHALLENGE, то карточка каждый раз возвращает новый 8-байтовый произвольный запрос, но сохраняет только последний из них.

CSM_173 Алгоритм подписи, используемый БУ для аутентификации БУ, представляет собой алгоритм ECDSA, как указано в [DSS], в сочетании с алгоритмом хеширования, связанным с размером ключа пары ключей БУ VU_MA, как указано в ~~TCS_192~~ CSM_50. Формат подписи простой, как указано в [TR-03111]. БУ передает полученную подпись на карточку.

CSM_174 По получении подписи БУ в команде EXTERNAL AUTHENTICATE карточка:

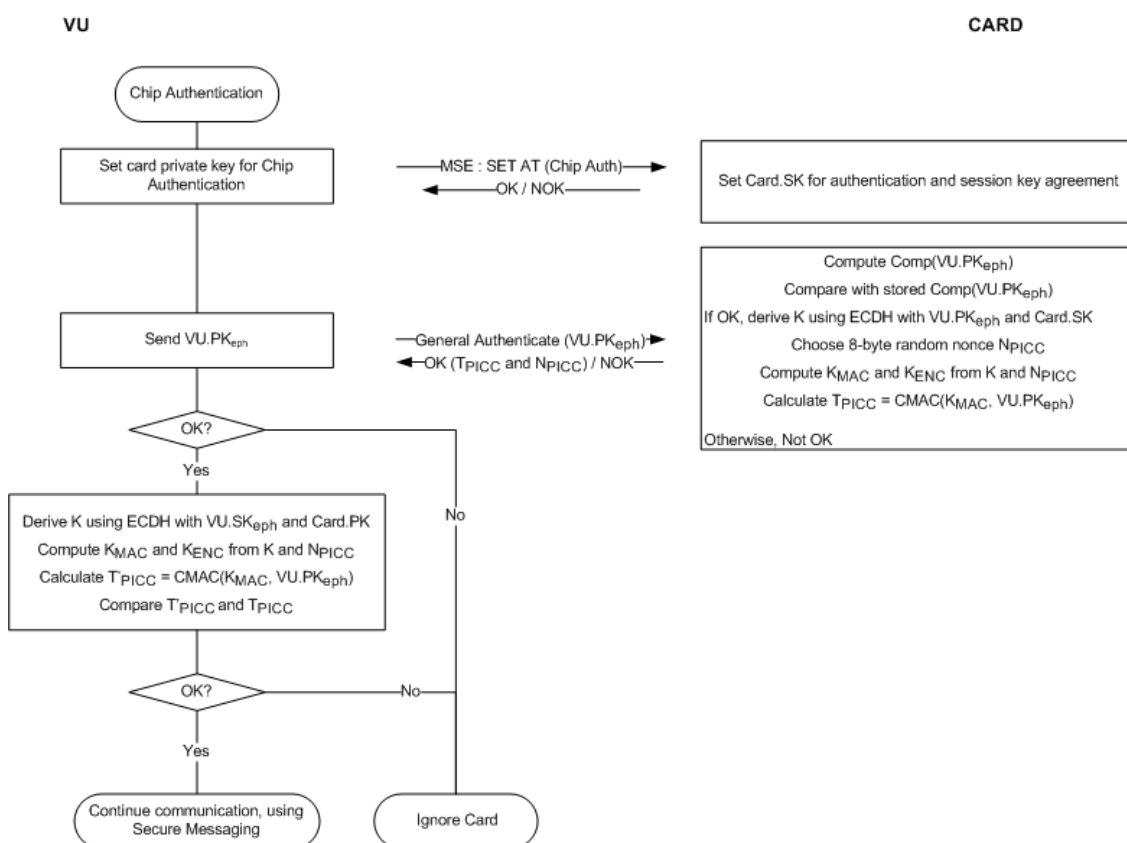
- вычисляет маркер аутентификации путем конкатенации Card.CHR, запроса карточки «card» и идентификатора кратковременного открытого ключа БУ $\text{Comp}(VU.PK_{eph})$,
- вычисляет **проверяет** хеш-функцию, связанную с маркером аутентификации, с **подпись БУ** с применением алгоритма хеширования ECDSA, связанного с размером ключа пары ключей БУ VU_MA, как указано в TCS_192, CSM_50;
- проверяет подпись БУ с применением алгоритма ECDSA CSM_50 в сочетании с VU.PK и вычисленной хеш-функцией маркером аутентификации.

10.4 Аутентификация микросхемы и согласование сеансовых ключей

CSM_175 Бортовые устройства и карточки используют протокол аутентификации микросхемы, отображенный на рис. 7, в целях аутентификации карточки по отношению к БУ. Аутентификация микросхемы позволяет бортовому устройству достоверно проверить аутентичность карточки.

Рис. 7

Аутентификация микросхемы и согласование сеансовых ключей



CSM_176 БУ и карточка производят следующие действия:

1. Бортовое устройство инициирует процесс аутентификации микросхемы, передавая команду MSE: Set AT с указанием аутентификации микросхемы с помощью алгоритма ECDSA, в результате чего вычисляется длина сеансового ключа AES, связанная с размером ключа пары ключей Card_MA карточки, как указано в TCS_192 CSM_50'. БУ определяет размер ключа пары ключей карточки по сертификату карточки.

2. БУ отправляет параметры открытой точки $VU.PK_{eph}$ своей пары кратковременных ключей на карточку. **Открытая точка преобразуется в октетную строку, как указано в [TR-03111]. Используется несжатый формат кодирования.** Как поясняется в ~~TCS_306~~ **CSM_164**, БУ сгенерировал эту кратковременную пару ключей до проверки последовательности сертификата БУ. БУ передает идентификатор кратковременного открытого ключа $Comp(VU.PK_{eph})$ на карточку, и карточка его сохраняет.
3. Карточка вычисляет $Comp(VU.PK_{eph})$ по $VU.PK_{eph}$ и сравнивает полученное значение с сохраненным значением $Comp(VU.PK_{eph})$.
4. Используя алгоритм ECDH в сочетании со статичным закрытым ключом карточки и кратковременным открытым ключом БУ, карточка вычисляет секретный параметр K .
5. Карточка выбирает произвольный 8-байтовый код NPICC и использует его для генерирования двух сеансовых ключей AES KMAC и KENC из K . См. ~~TCS_322~~ **CSM_179**.
6. Карточка вычисляет с помощью KMAC маркер аутентификации по идентификатору кратковременного открытого ключа БУ: $TRICC = CMAC(KMAC, VU.PK_{eph})$. **Открытая точка должна быть в формате, который используется БУ (см. пункт 2 выше).** Карточка передает NPICC и TRICC в бортовое устройство.
7. Используя алгоритм ECDH в сочетании со статичным закрытым ключом карточки и кратковременным открытым ключом БУ, бортовое устройство вычисляет секретный K таким же способом, как это было сделано на этапе 30.
8. БУ извлекает сеансовые ключи KMAC и KENC из K и NPICC; см. ~~TCS_324~~ **CSM_179**.
9. БУ проверяет маркер аутентификации TRICC.

CSM_177 На указанном выше этапе 2 карточка вычисляет $Comp(VU.PK_{eph})$ в качестве координаты x открытой точки в $VU.PK_{eph}$.

CSM_178 На указанных выше этапах 3 и 6 карточка и бортовое устройство используют алгоритм ECKA-EG, как определено в [TR-03111].

CSM_179 На указанных выше этапах 4 и 7 карточка и бортовое устройство используют функцию генерирования ключей для сеансовых ключей AES, как определено в [TR-03111], с учетом следующих уточнений и изменений:

- значение счетчика: '00 00 00 01' для K_{ENC} и '00 00 00 02' для K_{MAC} ;
- используется факультативное временное значение r , равное N_{TRICC} ;
- для получения 128-битовых ключей AES используется алгоритм хеширования SHA-256;
- для получения 192-битовых ключей AES используется алгоритм хеширования SHA-384;
- для получения 256-битовых ключей AES используется алгоритм хеширования SHA-512.

Длина сеансовых ключей (т. е. длина, на которой усекается хеш) связана с размером пары ключей $Card_MA$, как указано в ~~TCS_192~~ **CSM_50**.

CSM_180 На указанных выше этапах 6 и 9 карточка и бортовое устройство используют алгоритм AES в режиме CMAC, как определено в [SP 800-38B]. Длина $TRICC$ связана с длиной сеансовых ключей AES, как определено в ~~TCS_192~~ **CSM_50**.

10.5 Защищенный обмен сообщениями

10.5.1 Общие положения

- CSM_181 Все команды и ответы, которыми обмениваются бортовое устройство и карточка тахографа после успешной аутентификации микросхемы и до конца сеанса, предохраняются системой защищенного обмена сообщениями.
- CSM_182 За исключением случаев считывания данных из соответствующего файла с соблюдением условия доступа SM-R-ENC-MAC-G2 (см. ~~добавление~~ **подраздел 2, часть 4**), защищенный обмен сообщениями используется только в режиме аутентификации. В этом режиме ко всем командам и ответам добавляется криптографическая контрольная сумма (MAC) с целью обеспечить аутентичность и целостность сообщения.
- CSM_183 При считывании данных из соответствующего файла с соблюдением условия доступа SM-R-ENC-MAC-G2 защищенный обмен сообщениями используется в режиме шифрования с последующей аутентификацией, т. е. данные ответа сначала шифруются с целью обеспечить конфиденциальность сообщения, а затем вычисляется MAC по отформатированным зашифрованным данным в порядке обеспечения аутентичности и целостности.
- CSM_184 Механизм защищенного обмена сообщениями использует AES, как определено в [AES], в сочетании с сеансовыми ключами K_{MAC} и K_{ENC} , согласованными в процессе аутентификации микросхемы.
- CSM_185 Для предотвращения повторных атак в качестве счетчика исходящих сообщений (SSC) используется неподписанное целое число. Размер SSC равен размеру блока AES, т. е. 128 битам. SSC выполняется в формате самого значимого левого бита (MSB). Когда начинается защищенный обмен сообщениями, счетчик исходящих сообщений выставляется на ноль (т. е. '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'). SSC увеличивается всякий раз перед генерированием команды или ответа APDU, вследствие чего в первой команде значение SSC будет равно 1, поскольку стартовое значение SSC в сеансе SM равно 0. Значение SSC в первом ответе будет равно 2.
- CSM_186 Для шифрования сообщения используется K_{ENC} в сочетании с AES в режиме сцепления криптоблоков (CBC), как определено в [ISO 10116], с параметром чередования $m = 1$ и вектором инициализации $SV = E(K_{ENC}, SSC)$, т. е. с текущим значением счетчика исходящих сообщений, зашифрованным с помощью K_{ENC} .
- CSM_187 Для аутентификации сообщений используется K_{MAC} в сочетании с AES в режиме S_{MAC} , как определено в [SP 800-38B]. Длина MAC уязвляется с длиной сеансовых ключей AES, как указано в ~~TCS-192~~ **CSM_50**. Счетчик исходящих сообщений включается в MAC путем его добавления перед аутентификацией дейтаграммы.

10.5.2 Структура защищенного сообщения

- CSM_188 Механизм защищенного обмена сообщениями использует только объекты данных защищенного обмена сообщениями (см. [ISO 7816-4]), перечисленные в таблице 547. В любом сообщении эти объекты данных используются в порядке, указанном в данной таблице.

Таблица 5
Объекты данных защищенного обмена сообщениями

Наименование объекта данных	Метка	Наличие (М)обязательное, (С)условное или (F)запрещенное в	
		Командах	Ответах
Обычное значение, не закодированное в BER-TLV	'81'	C	C
Обычное значение, закодированное в BER-TLV, но не включающее ОД КЗОС	'B3'	C	C
Индикатор содержимого подшивки с последующей криптограммой, обычное значение в BER-TLV не кодируется	'87'	C	C
Защищенный байт «Le»	'97'	C	F
Статус обработки	'99'	F	M
Криптографическая контрольная сумма	'8E'	M	M

Примечание: Как указано в ~~добавлении~~ **подразделе 2**, карточки тахографа могут поддерживать команды READ BINARY и UPDATE BINARY с нечетным байтом INS ('B1', соответственно 'D7'). Эти варианты команд необходимы для считывания и обновления файлов, содержащих 32 768 байтов или более. В случае использования такого варианта вместо объекта с меткой '81' используется объект данных с меткой 'B3'. Более подробную информацию см. в ~~добавлении~~ **подразделе 2**.

CSM_189 Все объекты данных SM кодируются в DER TLV, как указано в [ISO 8825-1]. Такое кодирование приводит к следующей структуре значения длины метки (TLV):

Метка: метка кодируется одним или двумя октетами и указывает на содержание.

Длина: длина кодируется как неподписанное целое число одним, двумя или тремя октетами, что приводит к максимальной длине 65 535 октетов. Используется минимальное число октетов.

Значение: значение кодируется в виде нулевого или большего количества октетов.

CSM_190 APDU, предохраняемые механизмом защищенного обмена сообщениями, создаются следующим образом:

- заголовок команды включается в вычисление MAC, в результате чего значение '0C' используется для классового байта CLA;
- как указано в ~~добавлении~~ **подразделе 2**, все байты INS четные, но с возможным исключением нечетных байтов INS для команд READ BINARY и UPDATE BINARY;
- после применения механизма защищенного обмена сообщениями фактическое значение Lc изменяется на Lc';
- поле данных состоит из объектов данных SM;
- в защищенной команде APDU новый байт Le устанавливается на '00'. При необходимости объект данных '97' включается в поле данных в порядке передачи исходного значения Le.

CSM_191 Любой объект данных, подлежащий шифрованию, заполняется в соответствии с [ISO 7816-4] с использованием показателя заполнения '01'. Для целей вычисления MAC ~~каждый объект~~ **объекты** данных в APDU ~~также отдельно заполняются~~ заполняются в соответствии с [ISO 7816-4].

Примечание: Заполнение в механизме защищенного обмена сообщениями всегда производится на уровне защищенного обмена сообщениями, а не с помощью алгоритмов CMAC или CBC.

Резюме и примеры

Команда APDU с применяемым механизмом защищенного обмена сообщениями будет иметь следующую структуру в зависимости от соответствующей незащищенной команды (DO — объект данных):

- Случай 1: CLA INS P1 P2 || Lc' || DO '8E' || Le
 Случай 2: CLA INS P1 P2 || Lc' || DO '97' || DO '8E' || Le
 Случай 3 (четный байт INS): CLA INS P1 P2 || Lc' || DO '8E' || Le
 Случай 3 (нечетный байт INS): CLA INS P1 P2 || Lc' || DO '97' || DO '8E' || Le
 Случай 4 (четный байт INS): CLA INS P1 P2 || Lc' || DO '81' || DO '97' || DO '8E' || Le
 Случай 4 (нечетный байт INS): CLA INS P1 P2 || Lc' || DO 'B3' || DO '97' || DO '8E' || Le

Где Le = '00' или '00 00' в зависимости от того, используются ли поля короткой длины или поля расширенной длины; см. [ISO 7816-4].

APDU ответа с защищенным обменом сообщениями будет иметь следующую структуру в зависимости от случая соответствующего незащищенного ответа:

- Случай 1 или 3: DO '99' || DO '8E' || SW1SW2
 Случай 2 или 4 (четный байт INS) с шифрованием: DO '81' || DO '99' || DO '8E' || SW1SW2
 Случай 2 или 4 (четный байт INS) без шифрования: DO '87' || DO '99' || DO '8E' || SW1SW2
 Случай 2 или 4 (четный байт INS) без шифрования: DO 'B3' || DO '99' || DO '8E' || SW1SW2

Примечание: Случай 2 или 4 (нечетный байт INS) с шифрованием в процессе обмена сообщениями между БУ и карточкой никогда не используется.

Ниже приводятся три примера преобразования APDU для команд с четным кодом INS. На **рис. 8** показана аутентифицированная команда APDU в случае 4, на **рис. 9** показан аутентифицированный ответ APDU в случаях 1/3 и на **рис. 10** показан зашифрованный и аутентифицированный ответ APDU — случай 2/случай 4.

Рис. 8

Преобразование аутентифицированной команды APDU в случае 4

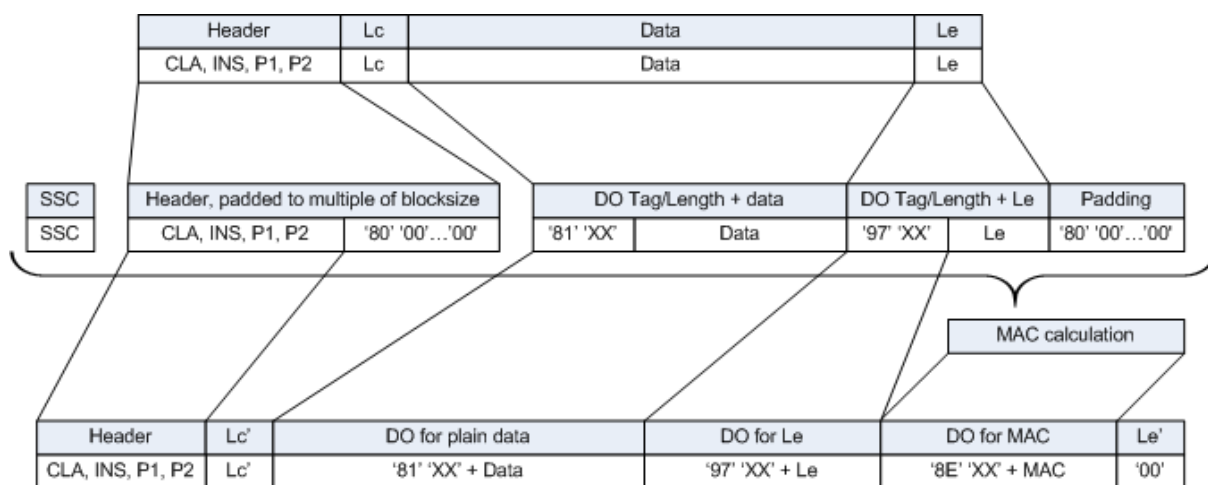


Рис. 9

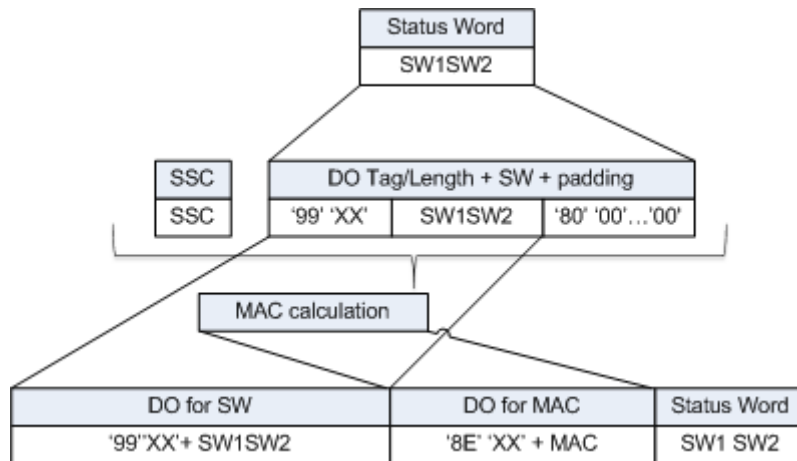
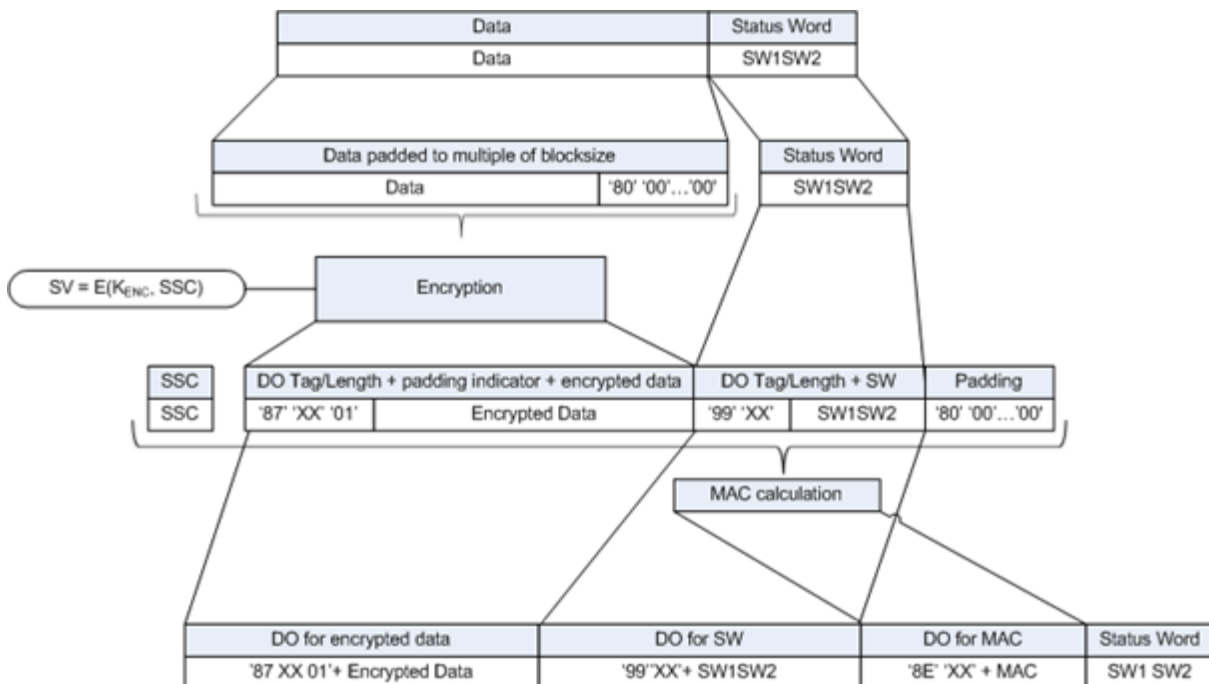
Преобразование аутентифицированного ответа APDU — случай 1/случай 3

Рис. 10

Преобразование зашифрованного и аутентифицированного ответа APDU в случае 2/случае 4**10.5.3 Отмена сеанса защищенного обмена сообщениями**

CSM_192 Бортовое устройство прерывает текущий сеанс защищенного обмена сообщениями, если и только в случае возникновения одного из следующих условий:

- оно получает простой ответ APDU;
- оно обнаруживает ошибку в защищенном обмене сообщениями в ответе APDU:
- отсутствие ожидаемого объекта данных защищенного обмена сообщениями, неверная последовательность объектов данных или наличие неизвестного объекта данных;
- объект данных защищенного обмена сообщениями неверный, например, неверное значение MAC, неверная структура TLV или показатель заполнения с меткой '87' не равен '01';

- карточка передает байт статуса, указывающий на то, что обнаружена ошибка SM (см. ~~TCS_336~~, **CSM_194**);
- достигнуто предельное число команд и соответствующих ответов в пределах текущего сеанса. В случае данного БУ такой предел устанавливает изготовитель, учитывающий требования безопасности к используемому аппаратному обеспечению, с учетом максимального значения 240 команд и ответов SM в расчете на один сеанс.

CSM_193 Карточка тахографа прерывает текущий сеанс защищенного обмена сообщениями, если и только в случае возникновения одного из следующих условий:

- оно получает простую команду APDU;
- оно обнаруживает ошибку, касающуюся защищенного обмена сообщениями, в команде APDU:
 - отсутствие ожидаемого объекта данных защищенного обмена сообщениями, неверная последовательность объектов данных или наличие неизвестного объекта данных;
 - о данных защищенного обмена сообщениями неверный, например, неверное значение MAC или неверная структура TLV;
- прекращение питания или перезагрузка;
- ~~БУ выбирает приложение на карточке;~~
- БУ начинает процесс аутентификации БУ;
- достигнуто предельное число команд и соответствующих ответов в пределах текущего сеанса. В случае данной карточки такой предел устанавливает изготовитель с учетом требований безопасности к используемому аппаратному обеспечению и максимального значения 240 команд и ответов SM в расчете на один сеанс.

CSM_194 Ошибка обработки SM на карточке тахографа:

- если в команде APDU отсутствуют некоторые ожидаемые объекты данных защищенного обмена сообщениями, неверный порядок объектов данных или присутствуют неизвестные объекты данных, то карточка тахографа отвечает байтами статуса '69 87';
- если в команде APDU есть неверный объект данных защищенного обмена сообщениями, то карточка тахографа выдает в ответ байты статуса '69 88'.

В таком случае байты статуса возвращаются без использования SM.

CSM_195 Если сеанс защищенного обмена сообщениями между БУ и карточкой тахографа прерван, то БУ и карточка тахографа

- уничтожают сохраненные сеансовые ключи безопасным образом;
- немедленно запускают новый сеанс защищенного обмена сообщениями, как описано в разделах **10.2–10.5**.

CSM_196 Если по какой-либо причине БУ решает перезапустить процесс взаимной аутентификации введенной карточки, то этот процесс снова начинается с проверки последовательности сертификатов карточки, как описано в разделе **10.2**, и продолжается, как описано в разделах **10.2–10.5**.

11. Соединение, взаимная аутентификация и защищенный обмен сообщениями между БУ и внешним устройством ГНСС

11.1 Общие положения

- CSM_197 Устройство ГНСС, которое БУ использует для установления местоположения, может быть внутренним (т. е. встроенным в корпус БУ и не съемным), или же оно может быть выполнено в виде внешнего модуля. В первом случае стандартизировать внутреннюю связь между устройством ГНСС и БУ нет необходимости, и в этой связи требования настоящей главы не применяются. В последнем случае связь между БУ и внешним устройством ГНСС стандартизируется и защищается, как описано в настоящей главе.
- CSM_198 Защищенная связь между бортовым устройством и внешним устройством ГНСС осуществляется так же, как и защищенная связь между бортовым устройством и карточкой тахографа, причем роль карточки выполняет внешнее устройство ГНСС (EGF). Все требования, упомянутые в главе 10 для карточек тахографа, должны выполняться EGF с учетом отклонений, уточнений и дополнений, упомянутых в данной главе. В частности, взаимная проверка последовательности сертификатов, аутентификация БУ и аутентификация микросхемы проводятся так же, как описано в разделах 11.3 и 11.4.
- CSM_199 Связь между бортовым устройством и EGF отличается от связи между бортовым устройством и карточкой в том плане, что бортовое устройство и EGF должны быть в определенный момент времени сопряжены в мастерской, что впоследствии позволит им обмениваться данными ГНСС в режиме нормальной эксплуатации. Процесс соединения описан в разделе 11.2.
- CSM_200 Для связи между бортовым устройством и EGF используются команды и ответы APDU согласно [ISO 7816-4] и [ISO 7816-8]. Точная структура таких APDU описана в приложении 2 к настоящему **дополнению**.

11.2 Соединение БУ и внешнего устройства ГНСС

- CSM_201 Бортовое устройство и EGF транспортного средства соединяются в мастерской. Бортовое устройство и EGF могут поддерживать связь в режиме нормальной эксплуатации только в том случае, если они соединены между собой.
- CSM_202 Соединение бортового устройства и EGF возможно только в том случае, если бортовое устройство находится в режиме калибровки. Соединение инициируется бортовым устройством.
- CSM_203 Мастерская может в любой момент подсоединить бортовое устройство к другому EGF или произвести повторное соединение с тем же самым EGF. Во время повторного соединения БУ безопасным образом уничтожает сохранившийся в его блоке памяти сертификат EGF_MA и сохраняет сертификат EGF_MA устройства EGF, с которым оно соединяется.
- CSM_204 Мастерская может в любой момент подсоединить внешнее устройство GNSS к другому БУ или произвести повторное соединение с тем же самым БУ. Во время повторного соединения EGF безопасным образом уничтожает сохранившийся в его блоке памяти сертификат VU_MA и сохраняет сертификат VU_MA бортового устройства, с которым оно соединяется.

11.3 Взаимная проверка последовательности сертификатов

11.3.1 Общие положения

CSM_205 Взаимная проверка последовательности сертификатов между БУ и EGF проводится только во время соединения БУ и EGF в мастерской. В процессе нормальной эксплуатации соединенных БУ и EGF проверка сертификатов не проводится. Вместо этого БУ и EGF доверяют сертификатам, которые они сохранили во время соединения, после проверки срока их действия. В целях защиты связи между БУ и EGF во время нормальной эксплуатации БУ и EGF не доверяют никаким другим сертификатам.

11.3.2 Во время соединения БУ и EGF

CSM_206 Во время соединения с EGF в целях проверки последовательности сертификатов внешнего устройства ГНСС бортовое устройство использует протокол, отображенный на **рис. 4** (раздел 10.2.1).

Примечания к **рис. 4** по этому вопросу:

- Контроль за связью не входит в область применения настоящего ~~приложения~~ **подраздела**. Вместе с тем EGF не является смарт-карточкой, поэтому БУ скорее всего не передаст команду Reset в порядке инициирования связи и не получит ATR.
- Сертификаты карточки и открытые ключи, указанные на рисунке, интерпретируются как сертификаты и открытые ключи EGF для взаимной аутентификации. В части **9.1.6** они указаны под обозначением EGF_MA.
- Сертификаты карточки и открытые ключи Card.CA, указанные на рисунке, интерпретируются как сертификаты и открытые ключи MSCA для подписания сертификатов EGF. В части **9.1.3** они указаны под обозначением MSCA_VU-EGF.
- Сертификаты Card.CA.EUR, указанные на рисунке, представляют собой ~~европейский~~ **европейский** корневой сертификат, который указан в CAR сертификата MSCA_VU-EGF.
- Сертификат Card.Link, указанный на рисунке, интерпретируется как связующий сертификат EGF, если он имеется. Как указано в разделе **9.1.2**, это — связующий сертификат для новой пары ~~европейских~~ **европейских** корневых ключей, созданной ERCA и подписанной прежним ~~европейским~~ **европейским** **корневым** закрытым ключом.
- Сертификат Card.CA.EUR представляет собой ~~европейский~~ **европейский** корневой сертификат, который указан в CAR сертификата Card.Link.
- Вместо cardExtendedSerialNumber БУ считывает sensorGNSSserialNumber из EF ICC.
- Вместо того, чтобы выбрать AID тахографа, БУ выбирает AID EGF.
- «Ignore Card» интерпретируется как «Ignore EGF».

CSM_207 После проверки сертификата EGF_MA бортовое устройство хранит этот сертификат для его использования во время нормальной эксплуатации; см. часть **11.3.3**.

CSM_208 Во время соединения с БУ в целях проверки последовательности сертификатов БУ внешнее устройство ГНСС использует протокол, отображенный на рисунке 5 (раздел 10.2.2).

Примечания к **рис. 5** по этому вопросу:

- БУ генерирует новую кратковременную пару ключей с параметрами домена в сертификате EGF.

- Сертификаты БУ и открытые ключи, указанные на рисунке, предназначены для взаимной аутентификации. В части **9.1.4** они указаны под обозначением VU_MA.
 - Сертификаты и открытые ключи VU.CA , указанные на данном рисунке, предназначены для подписания сертификатов БУ и внешнего устройства ГНСС. В части **9.1.3** они указаны под обозначением MSCA_VU-EGF.
 - Сертификат VU.CA.EUR, указанный на рисунке, представляют собой ~~европейский~~ европейский корневой сертификат, который указан в CAR сертификата VU.CA.
 - Сертификат VU.Link, упомянутый на рисунке, является связующим сертификатом БУ, если таковой имеется. Как указано в части **9.1.2**, это — связующий сертификат для новой пары ~~европейских~~ европейских корневых ключей, созданной ERCA и подписанной прежним ~~европейским~~ европейским **корневым** закрытым ключом.
 - Сертификат VU.Link.EUR представляют собой ~~европейский~~ европейский корневой сертификат, который указан в CAR сертификата VU.Link.
- CSM_209 В порядке отход от требования ~~TCS_309~~ **CSM_167**, EGF использует время ГНСС для проверки срока действия любого представленного сертификата.
- CSM_210 После проверки сертификата VU_MA внешнее **устройство** ГНСС хранит этот сертификат для его использования во время нормальной эксплуатации; см. часть **11.3.3**.

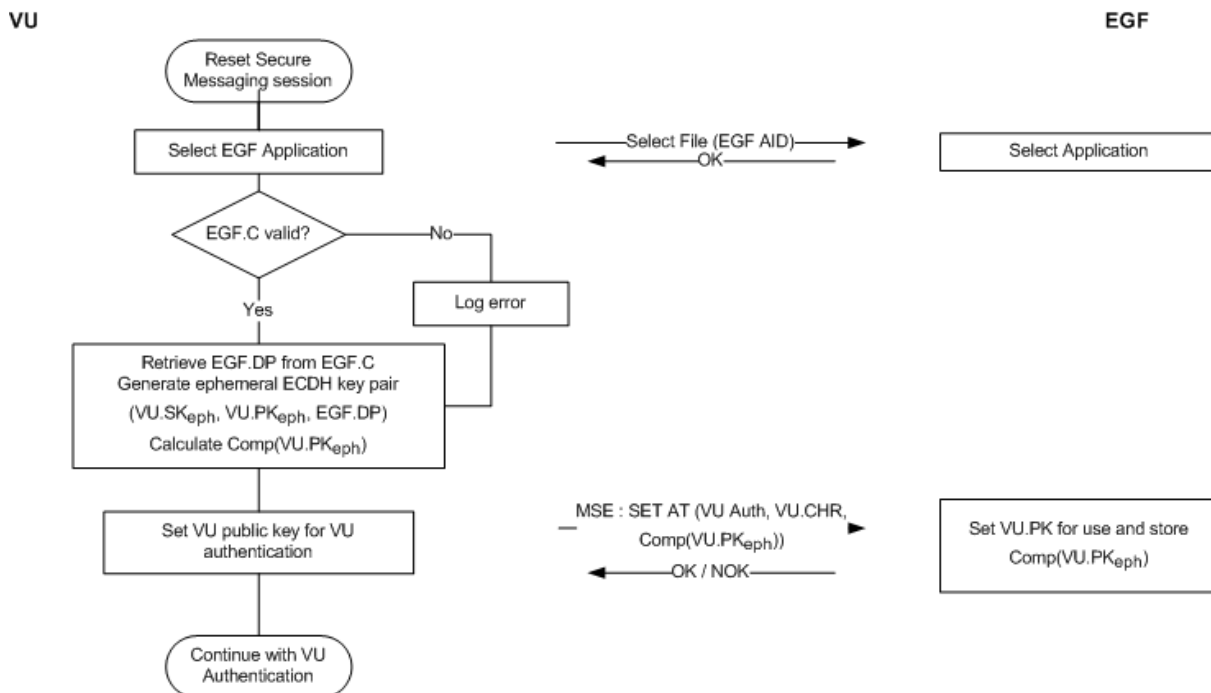
11.3.3 Во время нормальной эксплуатации

- CSM_211 В процессе нормальной эксплуатации бортовое устройство и EGF используют протокол, отображенный на рисунке 11, для проверки срока действия хранящихся сертификатов в EGF_MA и VU_MA и установки открытого ключа VU_MA в целях последующей аутентификации БУ. В процессе нормальной эксплуатации никакая дальнейшая взаимная проверка последовательности сертификатов не проводится.

Следует отметить, что **рис. 11** в целом состоит из первых этапов, отображенных на **рис. 4** и **рис. 5**. И в данном случае следует иметь в виду, что поскольку EGF не является смарт-карточкой, БУ скорее всего не передаст команду Reset в порядке инициализации связи и не получит ATR. В любом случае это не входит в область применения настоящего ~~приложения~~ **подраздела**.

Рис. 11

Взаимная проверка срока действия сертификата в процессе нормальной эксплуатации БУ и EGF



CSM_212 Как показано на рис. 11, если сертификат EGF_MA более недействителен, то бортовое устройство регистрирует ошибку. Вместе с тем взаимная аутентификация, согласование ключей и дальнейшая связь через механизм защищенного обмена сообщениями должны производиться в обычном порядке.

11.4 Аутентификация БУ, аутентификация микросхемы и согласование сеансовых ключей

CSM_213 Аутентификация БУ, аутентификация микросхемы и согласование сеансовых ключей между БУ и EGF производится во время соединения и во всех случаях, когда в условиях нормальной эксплуатации восстанавливается сеанс защищенного обмена сообщениями. БУ и EGF выполняют процессы, описанные в разделах 10.3 и 10.4. Все требования указанных разделов подлежат выполнению.

11.5 Защищенный обмен сообщениями

CSM_214 Все команды и ответы, которыми обмениваются бортовое устройство и внешнее устройство ГНСС после успешной аутентификации микросхемы и до конца сеанса, предохраняются системой защищенного обмена сообщениями только в режиме аутентификации. Все требования раздела 10.5 подлежат выполнению.

CSM_215 Если сеанс защищенного обмена сообщениями между БУ и EGF прерван, то БУ незамедлительно запускает новый сеанс защищенного обмена сообщениями, как описано в разделах 11.3.3 и 11.4.

12. Соединение и связь между БУ и датчиком движения

12.1 Общие положения

CSM_216 Бортовое устройство и датчик движения устанавливают связь на основе протокола интерфейса, указанного в [ISO 16844-3], в ходе процесса соединения и в условиях нормальной эксплуатации, с учетом изменений, предусмотренных в настоящей главе и в разделе 9.2.1.

Примечание: Предполагается, что читатели данной главы знакомы с содержанием [ISO 16844-3].

12.2 Соединение БУ и датчика движения с использованием различных поколений ключей

Как поясняется в разделе 9.2.1, ключ старшего порядка датчика движения и все связанные с ним ключи регулярно заменяются. Это приводит к тому, что на карточках мастерской хранится до трех ключей AES K_{M-WS} (последовательных поколений ключей), связанных с датчиком движения. Аналогичным образом, в случае датчиков движения также может быть до трех различных вариантов зашифрованных данных на базе AES (последовательных поколений ключа старшего порядка датчика движения K_M). В случае бортового устройства есть только один ключ, связанный с датчиком движения, K_{M-VU} .

CSM_217 БУ второго поколения и датчик движения второго поколения соединяются следующим образом (ср. таблицу 6 в [ISO 16844-3]):

1. Карточка мастерской второго поколения вводится в БУ, после чего БУ подсоединяется к датчику движения.
2. БУ считывает все имеющиеся ключи K_{M-WS} с карточки мастерской, проверяет номера их версий и выбирает одну, соответствующую номеру версии ключа K_{M-VU} БУ. Если соответствующего ключа K_{M-WS} на карточке мастерской нет, то БУ прерывает процесс соединения и выдает держателю карточки мастерской соответствующее сообщение об ошибке.
3. БУ вычисляет ключ старшего порядка датчика движения K_M по K_{M-VU} и K_{M-WS} , а идентификационный ключ K_{ID} — по K_M , как указано в части 9.2.1.
4. БУ передает указание начать процесс соединения на датчик движения, как описано в [ISO 16844-3], и шифрует серийный номер, который он получил от датчика движения, с помощью идентификационного ключа K_{ID} . БУ передает зашифрованный серийный номер обратно на датчик движения.
5. Датчик движения сравнивает зашифрованный серийный номер поочередно с каждым зашифрованным серийным номером, который в нем хранится. Если соответствие найдено, то производится аутентификация БУ. Датчик движения принимает к сведению генерацию K_{ID} , используемого БУ, и возвращает соответствующую зашифрованную версию своего ключа сопряжения, т. е. шифр, который был создан с использованием того же поколения K_M .
6. БУ расшифровывает ключ соединения при помощи K_M , генерирует сеансовый ключ K_S , шифрует его при помощи парного ключа соединения и передает результат на датчик движения. Датчик движения расшифровывает K_S .
7. БУ собирает информацию о соединении, как указано в [ISO 16844-3], шифрует эту информацию с помощью ключа соединения и передает результат на датчик движения. Датчик движения расшифровывает эту информацию о соединении.
8. Датчик движения шифрует полученную информацию о соединении при помощи полученного K_S и возвращает ее БУ. БУ проверяет, является ли информация о соединении той же информацией, которую БУ направил на датчик движения на предыдущем этапе. Если да, то это доказывает, что датчик движения использовал тот же K_S , что и БУ, и, как следствие, на этапе 5 передал

свой ключ соединения, зашифрованный с помощью правильного поколения K_M .
Результатом этого процесса является аутентификация датчика движения.

Следует иметь в виду, что этапы 2 и 5 отличаются от стандартного процесса в [ISO 16844-3]; остальные этапы стандартные.

Пример: предположим, что соединение производится в первый год действия сертификата ERCA 3); см. рисунок 2 в части ~~9.2.2.2~~ 9.2.1.2. Кроме того:

- предположим, что датчик движения был выпущен в последний год срока действия сертификата ERCA (1). В этой связи он будет содержать следующие ключи и данные:
- $N_s[1]$: свой серийный номер, зашифрованный при помощи K_{ID} поколения 1;
- $N_s[2]$: свой серийный номер, зашифрованный при помощи K_{ID} , поколения 2;
- $N_s[3]$: свой серийный номер, зашифрованный при помощи K_{ID} поколения 3;
- $K_p[1]$: свой спаренный ключ поколения 1¹³, зашифрованный при помощи K_M поколения 1;
- $K_p[2]$: свой спаренный ключ поколения 2, зашифрованный при помощи K_M поколения 2;
- $K_p[3]$: свой спаренный ключ поколения 3, зашифрованный при помощи K_M поколения 3;
- предположим, что карточка мастерской была выдана в первый год действия сертификата ERCA 3). Таким образом, она будет содержать поколение 2 и поколение 3 ключа K_{M-WS} ;
- предположим, что БУ — это БУ поколения 2, в котором содержится K_{M-VU} поколения 2;
- в этом случае на этапах 2–5 произойдет следующее:
- этап 2: БУ считывает K_{M-WS} поколения 2 и поколения 3 с карточки мастерской и проверяет номера их версий;
- этап 3: БУ комбинирует K_{M-WS} поколения 2 со своим K_{M-VU} с целью вычислить K_M и K_{ID} ;
- этап 4: БУ шифрует серийный номер, который оно получило из датчика движения, при помощи K_{ID} ;
- этап 5: Датчик движения сравнивает полученные данные с $N_s[1]$ и не находит соответствия. Затем он сравнивает эти данные с $N_s[2]$ и находит соответствие. Он делает вывод, что БУ представляет собой БУ поколения 2 и передает обратно $K_p[2]$.

12.3 Соединение и связь между БУ и датчиком движения с использованием AES

CSM_218 Как указано в таблице 345 в части 9.2.1, все ключи, задействованные в соединении бортового устройства (второго поколения) и датчика движения и в их последующей связи, представляют собой ключи AES, а не ключи TDES двойной длины, как указано в [ISO 16844-3]. Длина этих ключей AES может быть 128, 192 или 256 битов. Поскольку размер блока AES составляет 16 байтов, длина зашифрованного сообщения должна быть кратной 16 байтам, по сравнению с 8 байтами в случае TDES. Кроме того, некоторые из этих сообщений будут использоваться для передачи

¹³ Просьба обратить внимание на то, что ключи сопряжения поколения 1, поколения 2 и поколения 3 могут быть как одним и тем же ключом, так и тремя разными ключами разной длины, как объясняется в ~~TCS_259~~ CSM_117.

ключей AES, длина которых может быть 128, 192 или 256 битов. Таким образом, число байтов данных в расчете на одну инструкцию в таблице [ISO 16844-3] меняется, как показано в **таблице 648**:

Таблица 6

Число байтов простого текста и зашифрованных данных в одной инструкции в соответствии с [ISO 16844-3]

Инструкция	Запрос/ ответ	Описание данных	# байтов данных открытого текста в соответствии с [ISO 16844-3]	# байтов данных открытого текста в случае использования ключей AES	# зашифрованных байтов данных в случае использования ключей AES с длиной в битах		
					128	192	256
10	Запрос	Данные аутентификации + номер файла	8	8	16	16	16
11	Ответ	Данные аутентификации + содержание файла	16 или 32, в зависимости от файла	16 или 32, в зависимости от файла	±6 32/48	±6 32/48	±6 32/48
41	Запрос	Серийный номер датчика движения	8	8	16	16	16
41	Ответ	Ключ сопряжения	16	16/24/32	16	32	32
42	Запрос	Ключ сеанса	16	16/24/32	16	32	32
43	Запрос	Информация о сопряжении	24	24	32	32	32
50	Ответ	Информация о сопряжении	24	24	32	32	32
70	Запрос	Данные аутентификации	8	8	16	16	16
80	Ответ	Показания счетчика датчика движения + данные аутентификации	8	8	16	16	16

CSM_219 Информация о сопряжении, передаваемая в инструкциях 43 (запрос БУ) и 50 (ответ датчика движения), собирается, как указано в разделе 7.6.10 [ISO 16844-3], за исключением того, что в схеме шифрования данных сопряжения алгоритм AES используется вместо алгоритма TDES, что приводит таким образом к двум зашифрованным вариантам AES и заполнению, указанному в ~~TCS_363~~ CSM_220, соответствующему размеру блока AES. Ключ K'_p , используемый для такого шифрования, генерируется следующим образом:

- если длина ключа соединения K_p составляет 16 байтов: $K'_p = K_p \text{ XOR } (N_s || N_s)$;
- если длина ключа соединения K_p составляет 24 байта: $K'_p = K_p \text{ XOR } (N_s || N_s || N_s)$;
- если длина ключа соединения K_p составляет 32 байта: $K'_p = K_p \text{ XOR } (N_s || N_s || N_s || N_s)$,

где N_s — 8-байтовый серийный номер датчика движения.

CSM_220 Если длина открытого текста (с использованием ключей AES) не кратна 16 байтам, то в этом случае используется метод заполнения, определенный в [ISO 9797-1].

Примечание: В [ISO 16844-3] число байтов текстовых данных всегда кратно 8, вследствие чего при использовании TDES в заполнении нет необходимости. Определение данных и сообщений в [ISO 16844-3] в данной части настоящего приложения подраздела не меняется, что обуславливает необходимость применения заполнения.

CSM_221 В инструкции 11 и в том случае, когда необходимо зашифровать более одного блока данных, применяется режим сцепления криптоблоков, определенный в [ISO 10116], с параметром чередования $m = 1$. Позиция IV, которую надлежит использовать:

- в случае инструкции 11: 8-байтовый блок аутентификации, указанный в разделе 7.6.3.3 [ISO 16844-3], заполненный методом заполнения 2, определенным в [ISO 9797-1]; см. также части 7.6.5 и 7.6.6 [ISO 16844-3];
- в случае всех других инструкций, в которых передается больше 16 байтов данных, как указано в таблице 648: '0' {16}, т. е. 16 байтов с двоичным значением, равным 0.

Примечание: Как показано в частях 7.6.5 и 7.6.6 [ISO 16844-3], когда датчик движения шифрует файлы данных для их включения в инструкцию 11, блок аутентификации:

- используется как вектор инициализации для шифрования файлов данных в режиме CBC;
- зашифровывается и включается в качестве первого блока в данные, передаваемые в БУ.

12.4 Соединение БУ и датчика движения с использованием различных поколений оборудования

CSM_222 Как поясняется в разделе 9.2.1, ~~в датчике движения второго поколения может содержаться шифрование данных соединения на базе TDES~~ возможно второе шифрование данных соединения (в соответствии с частью А настоящего приложения подраздела), что позволяет датчику движения соединяться с БУ первого поколения. В этом случае они ~~БУ первого поколения и датчик движения второго поколения~~ соединяются, как описано в части А настоящего приложения подраздела и в [ISO 16844-3]. В процессе соединения может использоваться карточка мастерской первого или второго поколения.

Примечания:

- Соединить БУ второго поколения с датчиком движения первого поколения невозможно.
- Использовать карточку мастерской первого поколения для соединения БУ второго поколения с датчиком движения невозможно.

13. Защита удаленной связи по DSRC

13.1 Общие положения

Как указано в ~~приложении~~ подразделе 14, БУ регулярно генерирует данные удаленного мониторинга тахографа (RTM) и передает их во (внутреннее или внешнее) устройство удаленной связи (RCF). Устройство удаленной связи отвечает за передачу таких данных через интерфейс DSRC, описанный в ~~приложении~~ подразделе 14, средству удаленного мониторинга. В ~~приложении~~ подразделе 1 указано, что данные RTM представляют собой конкатенацию:

зашифрованных данных тахографа — шифрование текстовых данных тахографа
данных о безопасности DSRC — описаны ниже.

Текстовый формат данных тахографа представлен в ~~приложении~~ **подразделе 1** и более подробно описан в ~~приложении~~ **подразделе 14**. В этом разделе описывается структура данных о безопасности DSRC; формальная спецификация приведена в ~~приложении~~ **подразделе 1**.

CSM_223 Данные тахографа в виде обычного текста, передаваемые БУ на средство удаленной связи (если RCF является внешним по отношению БУ) или из БУ на средство удаленного мониторинга через интерфейс DSRC (если RCF является внешним по отношению к БУ), защищаются в режиме шифрования с последующей аутентификацией, т. е. данные тахографа сначала шифруются с целью обеспечить конфиденциальность сообщения, а затем вычисляется MAC с целью обеспечить аутентичность и целостность данных.

CSM_224 Данные о безопасности DSRC представляют собой конкатенацию нижеследующих элементов данных, производимую в следующем порядке; см. также **рис. 12**:

Текущие дата и время	текущие дата и время БУ (тип данных TimeReal)
Счетчик	3-байтовый счетчик, см. 0
Серийный номер БУ	серийный номер БУ или идентификатор запроса на сертификат (тип данных VuSerialNumber или CertificateRequestID) — см. CSM_123
Номер версии ключа старшего порядка DSRC	1-байтовый номер версии ключа старшего порядка DSRC, из которого были извлечены ключи DSRC для конкретного БУ, см. раздел 9.2.2
MAC	значение MAC, вычисляемое по всем прежним байтам в данных RTM.

CSM_225 3-байтовый счетчик в системе данных о безопасности DSRC представлен в формате самого значимого левого бита (MSB). Первый раз, когда БУ вычисляет набор данных RTM после их использования, значение счетчика устанавливается на 0. Каждый раз перед вычислением следующего набора данных RTM БУ увеличивает показания данных счетчика на 1.

13.2 Шифрование данных тахографа и генерирование MAC

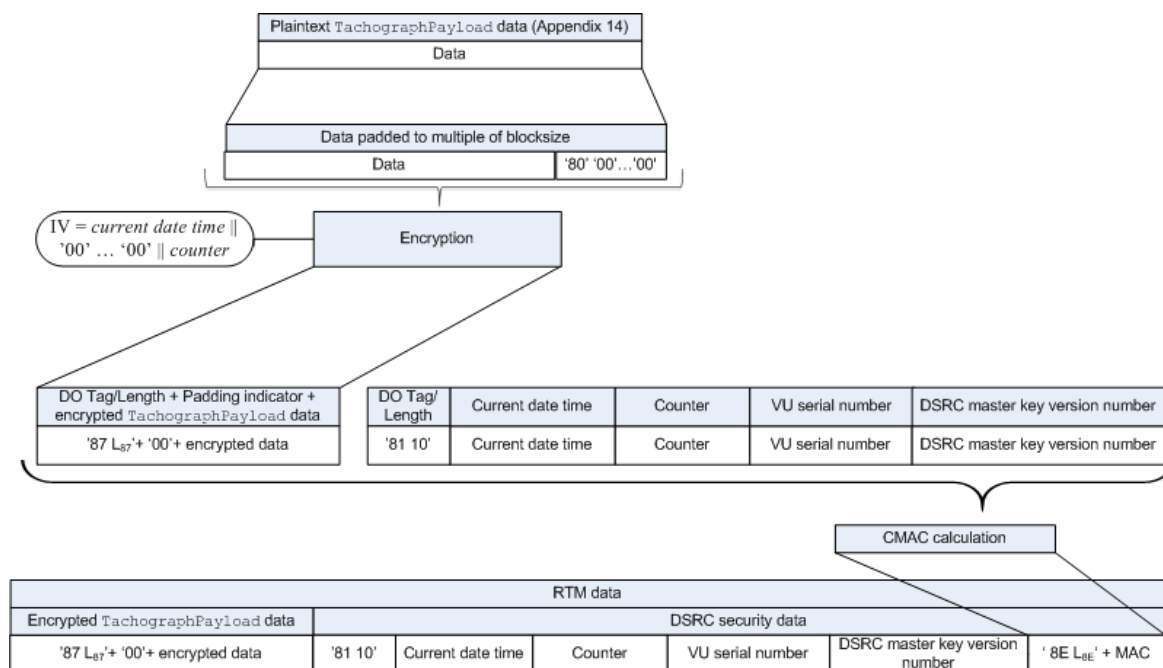
CSM_226 С учетом элемента данных в виде обычного текста с типом данных TachographPayload, как описано в ~~дополнении~~ **подразделе 14**, БУ шифрует эти данные, как показано на рис. 12: ключ DSRC VU для шифрования $K_{VU_{DSRC_ENC}}$ (см. часть ~~9.2.3~~ **9.2.2**) используется с AES в режиме сцепления криптоблоков (Cipher Block Chaining (CBC)), как определено в [ISO 10116], с параметром чередования $m = 1$. Вектор инициализации равен $IV = \text{текущие дата и время} || '00\ 00\ 00\ 00\ 00\ 00\ 00\ 00' || \text{счетчик}$, в случае которого *текущие дата и время* и *счетчик* описаны в ~~TCS_367~~ **CSM_224**. Данные, подлежащие шифрованию, заполняются по методу 2, определенному в [ISO 9797- 1].

CSM_227 БУ вычисляет MAC по данным о безопасности DSRC, как показано на **рис. 12**: MAC вычисляется по всем прежним байтам в данных RT

до номера версии ключа старшего порядка DSRC включительно, в том числе с учетом метки и длины объектов данных. БУ использует свой ключ DSRC для аутентификации K_{VUDSRC_MAC} (см. часть 9.2.3 9.2.2) с помощью алгоритма AES в режиме CMAC, как указано в [SP 800-38B]. Длина MAC увязывается с длиной сеансовых ключей DSRC для конкретного БУ, как указано в ~~TCS_192~~ CSM_50.

Рис. 12

Шифрование данных тахографа и генерирование MAC



13.3 Проверка и расшифровка данных тахографа

CSM_228 Когда средство удаленного мониторинга получает из БУ данные RTM, оно передает все данные RTM на карточку контролера в поле данных команды PROCESS DSRC MESSAGE, как описано в ~~приложении~~ **подразделе 2**. После этого:

1. Карточка контролера проверяет номер версии ключа старшего порядка DSRC в данных безопасности DSRC. Если карточке контролера указанный ключ старшего порядка DSRC неизвестен, она возвращает ошибку, указанную в ~~добавлении~~ **подразделе 2**, и прекращает процесс.
2. Карточка контролера использует указанный ключ старшего порядка DSRC в сочетании с серийным номером БУ **или сертификатом запроса ИД** в данных о безопасности DSRC с целью получить связанные с БУ ключи DSRC: K_{VUDSRC_ENC} и K_{VUDSRC_MAC} , как указано в ~~TCS_266~~ CSM_124.
3. Карточка контролера использует K_{VUDSRC_MAC} для проверки MAC в данных о безопасности DSRC, как указано в ~~TCS_370~~ CSM_227. Если MAC неправильный, то карточка контролера возвращает ошибку, указанную в ~~добавлении~~ **подразделе 2**, и прекращает процесс.
4. Карточка контролера использует K_{VUDSRC_MAC} для расшифровки зашифрованных данных тахографа, как указано в ~~TCS_368~~ CSM_226. Карточка контролера удаляет заполнение и возвращает расшифрованные данные тахографа средству удаленного мониторинга.

CSM_229 Для предотвращения повторных атак средство удаленного мониторинга проверяет новизну данных RTM с целью убедиться в том, что *текущие*

дата и время в данных о безопасности DSRC не слишком существенно отклоняются от текущего времени средства удаленного мониторинга.

Примечания:

- В этих целях средству удаленного мониторинга нужен *точный и надежный источник времени*.
- Поскольку в соответствии с ~~приложением~~ **подразделом 14**, БУ должно вычислять новый набор данных RTM каждые 60 секунд, а часы БУ могут отклоняться от реального времени на 1 минуту, нижний предел новизны данных RTM составляет 2 минуты. Фактическая требуемая новизна также зависит от точности часов средства удаленного мониторинга.

CSM_230 Когда мастерская проверяет правильность работы функциональных средств DSRC того или иного БУ, она передает все данные RTM, полученные от БУ, на карточку мастерской в поле данных команды PROCESS DSRC MESSAGE, как описано в ~~приложении~~ **подразделе 2**. Карточка мастерской выполняет все проверки и действия, указанные в ~~TCS_374~~ **CSM_228**.

14. Подписание загружаемых данных и проверка подписей

14.1 Общие положения

CSM_231 Данные, полученные из того или иного аппаратного источника (БУ или карточки) за один сеанс загрузки, сохраняются специализированной программируемой аппаратурой (СПА) в виде одного физического файла данных. Эти данные могут храниться на ~~ВН (внешнем носителе)~~ соответствующем носителе. Файл содержит цифровые подписи блоков данных в соответствии с указанными в ~~приложении~~ **подразделе 7**. Этот файл также содержит следующие сертификаты (см. раздел **9.1**):

- при загрузке из БУ:
 - сертификат VU_Sign;
 - сертификат MSCA_VU-EGF, содержащий открытый ключ для проверки сертификата VU_Sign;
- при загрузке из БУ:
 - сертификат VU_Sign;
 - сертификат MSCA_Card, содержащий открытый ключ для проверки сертификата Card_Sign.

CSM_232 СПА также располагает следующими средствами:

- если для проверки подписи используется карточка контролера, как показано на **рис. 13**: Связующий сертификат, связывающий последний сертификат EUR с сертификатом EUR, срок действия которого, если он существует, непосредственно ему предшествует;
- если проверяется сама подпись: все действительные европейские корневые сертификаты.

Примечание: Метод, используемый СПА для извлечения этих сертификатов, в настоящем ~~приложении~~ **подразделе** не указывается.

14.2 Генерация подписей

CSM_233 Алгоритмом подписи для создания цифровых подписей под загружаемыми данными будет алгоритм ECDSA, как указано в [DSS],

в сочетании с алгоритмом хеширования, связанным с размером ключа БУ или карточки, как указано в ~~TCS_192~~ CSM_50. Формат подписи простой, как указано в [TR-03111].

14.3 Проверка подписей

CSM_234 СПА может проверять подпись загружаемых данных самостоятельно или использовать для этого карточку контролера. Если используется карточка контролера, то проверка подписи производится так, как показано на рис. 13. Для проверки срока действия сертификата, представленного СПА, карточка контролера использует внутренние часы, как указано в CSM_167. Карточка обновляет свое текущее время в том случае, если фактическая дата аутентичного «действительного источника времени» сертификата более поздняя, чем текущее время карточки. В качестве действительного источника времени карточка принимает только следующие сертификаты:

- связующие сертификаты ERCA второго поколения;
- сертификаты MSCA второго поколения;
- сертификаты VU_Sign или Card_Sign второго поколения, выданные той же страной, что и собственный сертификат карточки контролера.

В том случае, если СПА проводит проверку подписи самостоятельно, то она проверяет аутентичность и срок действия всех сертификатов в той последовательности, в которой они значатся в файле данных, а также подпись данных в соответствии со схемой подписи, представленной в [DSS]. В обоих случаях каждый сертификат, считываемый из файла данных, необходимо проверить на правильность поля «Certificate Holder Authorisation» (CHA) (Полномочия держателя сертификата):

- поле CHA сертификата EQT должно указывать на соответствующий сертификат БУ или карточки (в случае применимости), подлежащий подписи (см. подраздел 1, тип данных “EquipmentType”);
- CHA сертификата EQT.CA указывает на MSCA;
- CHA сертификата EQT.Link указывает на ERCA.

Примечания к рис. 13:

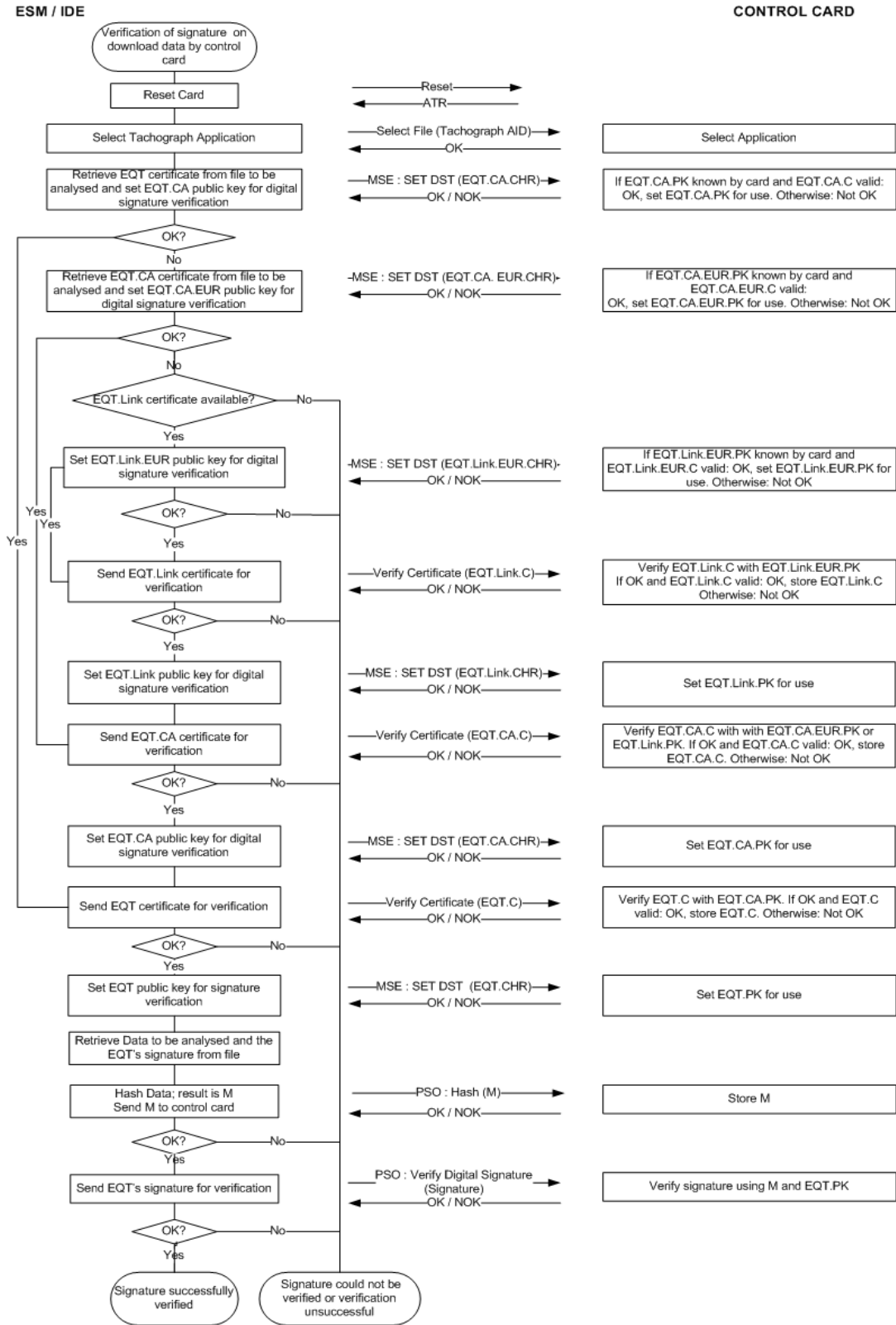
- Аппаратура, с помощью которой были подписаны подлежащие анализу данные, обозначена в виде EQT.
- Сертификаты EQT и открытые ключи, указанные на рисунке, предназначены для подписания, т. е. VU_Sign или Card_Sign.
- Сертификаты EQT.CA и открытые ключи, указанные на данном рисунке, предназначены для подписания, в зависимости от случая, сертификатов БУ или карточки.
- Сертификат EQT.CA.EUR, указанный на рисунке, представляют собой европейский корневой сертификат, который указан в CAR сертификата EQT.CA.
- Сертификат EQT.Link, упомянутый на рисунке, является связующим сертификатом EQT, если таковой имеется. Как указано в разделе 9.1.2, это — связующий сертификат для новой пары европейских корневых ключей, созданной ERCA и подписанной прежним европейским корневым закрытым ключом.
- Сертификат EQT.Link.EUR представляет собой европейский корневой сертификат, который указан в CAR сертификата EQT.Link.

CSM_235 Для вычисления хеша M, пересылаемого на карточку контролера в команде PSO:Hash, СПА использует алгоритм хеширования, связанный с размером ключа БУ или карточки, с которых загружаются данные, как указано в ~~TCS_192~~ CSM_50.

CSM_236 Для проверки подписи EQT карточка контролера использует схему подписи, представленную в [DSS].

Примечание: В настоящем документе не указываются конкретные действия, которые следует предпринимать в том случае, если подпись файла загружаемых данных невозможно проверить или если проверка оказалась безрезультатной.

Рис. 13
 Протокол проверки подписи файла загружаемых данных



Подраздел 12

Определение местоположения при помощи глобальной навигационной спутниковой системы (ГНСС)

Содержание

	<i>Стр.</i>
1. Введение	520
1.1 Сфера охвата	520
1.1.1 Справочные материалы	521
1.2 Сокращения и обозначения	521
2. Спецификация Основные характеристики приемника ГНСС	521
3. Сообщения NMEA, направляемые приемником ГНСС	523
4. Бортовое устройство с внешним устройством ГНСС	526
4.1 Конфигурация	526
4.1.1 Основные компоненты и интерфейсы	526
4.1.2 Состояние внешнего устройства ГНСС на выходе из конвейера	527
4.2 Связь между внешним устройством ГНСС и бортовым устройством.....	527
4.2.1 Протокол связи	527
4.2.2 Защищенная передача данных ГНСС	530
4.2.3 Структура команды Read Record (считывание записи)	531
4.2.4 Структура команды WriteRecord (регистрация записи)	532
4.2.5 Другие команды	532
4.3 Соединение, взаимная аутентификация и согласование сеансовых ключей между внешним устройством ГНСС и бортовым устройством	533
4.4 Обработка ошибок	533
4.4.1 Ошибка связи с внешним устройством ГНСС	533
4.4.2 Нарушение физической целостности внешнего устройства ГНСС	533
4.4.3 Отсутствие информации со стороны приемника ГНСС о местоположении	533
4.4.4 Истекший срок действия сертификата внешнего устройства ГНСС	533
5. Бортовое устройство без внешнего устройства ГНСС	534
5.1 Конфигурация	534
5.2 Ошибка в обработке передачи информации от приемника ГНСС в БУ	534
5.3 Передача информации от БУ к приемнику ГНСС	535
5.4 Обработка ошибок	535
5.4.1 Отсутствие информации от приемника ГНС о местоположении	535
6. Обработка и регистрация данных о местоположении с помощью БУГНСС Нестыковка во времени	535
7. Нестыковка во времени ГНСС.....	537
8. Противоречивые данные о движении транспортного средства	537

1. Введение

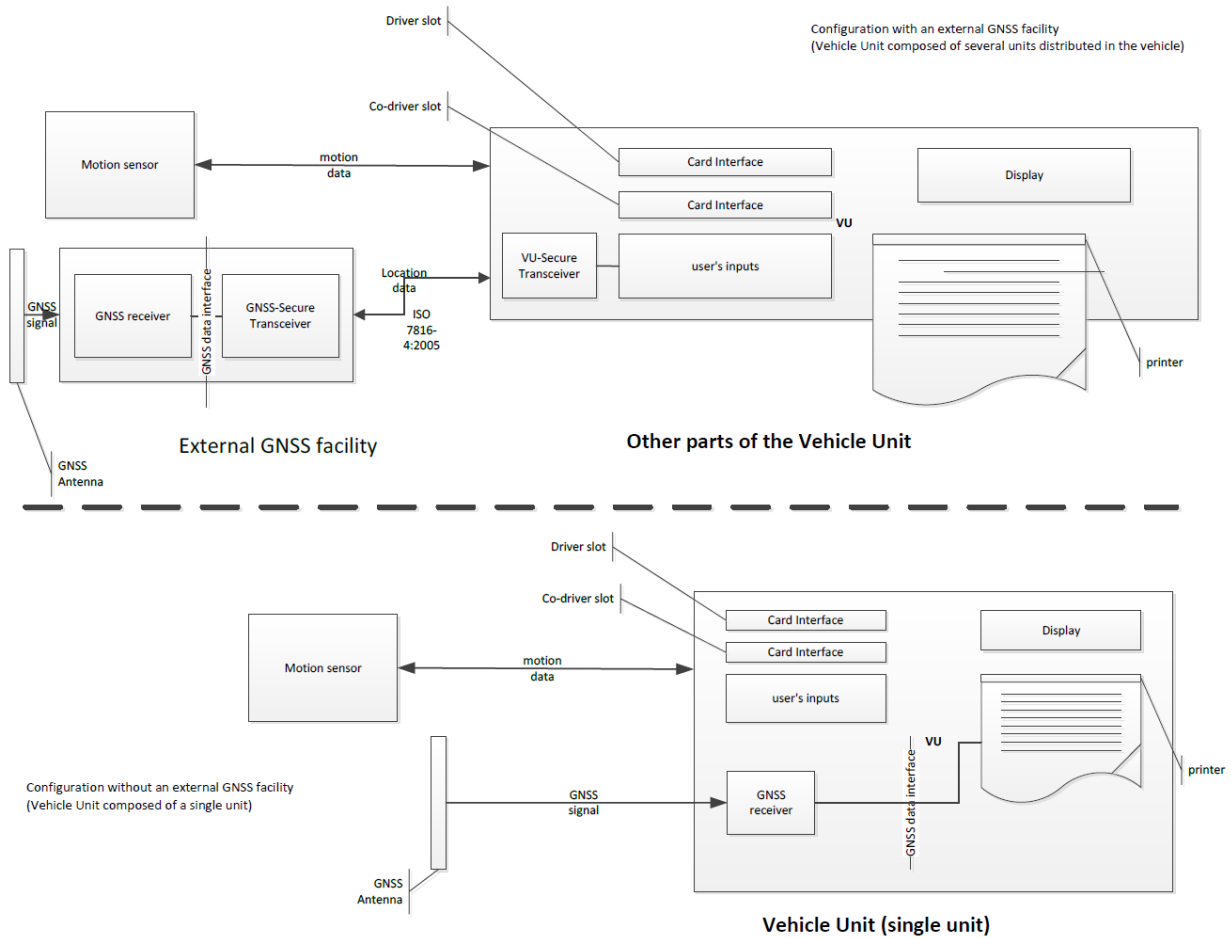
В данном ~~приложении подразделе добавления~~ содержатся технические требования, предъявляемые к ~~приемнику ГНСС~~ и данным ГНСС, используемым бортовым устройством, включая протоколы, которые должны быть соблюдены в целях обеспечения безопасной и правильной передачи данных информации о местоположении. ~~Основными статьями Регламента (ЕС) № 165/2014, определяющими эти требования, являются «Статья 8 Запись положения транспортного средства в определенные моменты в течение ежедневного рабочего периода», «Статья 10 Взаимодействие с интеллектуальными транспортными системами» и «Статья 11 Подробные положения для смарт-тахографа».~~

1.1 Сфера охвата

GNS_1 Бортовое устройство собирает данные о местоположении хотя бы из одной ~~спутниковой сети ГНСС~~ в целях выполнения требований ~~статьи 8~~.

Бортовое устройство может быть с внешним устройством ГНСС или без него для поддержки реализации объекта статьи 8, как изображено на рисунке 1-4:

Рис. 1
Различные конфигурации приемника ГНСС



1.1.1 Справочные материалы

В этой части настоящего подраздела используются следующие источники:

NMEA Стандарт на интерфейс NMEA (Национальная ассоциация морской электроники) 0183, V4.11.

1.2 Сокращения и обозначения

В данном подразделе используются следующие акронимы:

DOP	Показатель снижения точности
EGF	Элементарный файл устройства ГНСС
EGNOS	Европейская геостационарная служба навигационного покрытия
ГНСС	Глобальная навигационная спутниковая система
AOC	GPS DOP и активные спутники
HDOP	Снижение точности по горизонтали
ICD	Документ по контролю интерфейса
NMEA	Национальная ассоциация морской электроники
PDOP	Размывание точности из-за фактора положения
RMC	Рекомендуемый конкретный минимальный уровень
SIS	Сигнал в пространстве
VDOP	Вертикальное отклонение точности
БУ	Бортовое устройство
OSNMA	Открытая служба аутентификации навигационных сообщений «Галилей»
RTC	Часы реального времени

2. Спецификация Основные характеристики приемника ГНСС

~~Вне зависимости от конфигурации смарт-тахографа с внешним устройством ГНСС или без него, предоставление точной и надежной информации о местоположении является ключевым элементом эффективной эксплуатации смарт-тахографов. Таким образом, можно требовать его совместимости с услугами программ «Галилей» и Европейской геостационарной службы навигационного покрытия (EGNOS), как указано в Регламенте (ЕС) № 1285/2013 Европейского парламента и Совета¹⁴. Система, созданная в рамках системы «Галилей», это независимая глобальная спутниковая навигационная система, а система в рамках программы EGNOS представляет собой региональную спутниковую навигационную систему, позволяющую улучшить качество сигнала глобальной системы позиционирования.~~

GNS_2 Изготовители обеспечивают совместимость приемников ГНСС в смарт-тахографах в части услуг определения местоположения, которые предлагаются системами ГПС, ГЛОНАСС и «Галилей» и EGNOS. Изготовители также могут дополнительно выбирать совместимость с другими спутниковыми навигационными системами.

¹⁴ Регламент (ЕС) № 1285/2013 Европейского парламента и Совета от 11 декабря 2013 года о внедрении и эксплуатации европейских спутниковых навигационных систем, отменяющий Регламент Совета (ЕС) № 876/2002 и Регламент (ЕС) № 683/2008 Европейского парламента и Совета (OGL 347, 20.12.2013, стр. 1).

- GNS_3** Приемник ГНСС способен поддерживать аутентификацию **навигационных сообщений** с помощью открытой службы «Галилей» (OSNMA), если система «Галилей» предоставляет такую услугу ~~и если она поддерживается изготовителями приемников ГНСС. Однако в отношении смарт-тахографов, поставляемых на рынок до удовлетворения прежних условий и не способных поддерживать аутентификацию при помощи открытой услуги «Галилей», переоснащение проводить не придется.~~
- GNS_3a** Приемник ГНСС выполняет ряд проверок согласованности с целью убедиться в том, что измерения, произведенные приемником ГНСС на основе данных OSNMA, позволили получить правильную информацию о положении, скорости и данных транспортного средства и, как следствие, не подверглись влиянию какой-либо внешней атаки, такой как создание помех. Эти проверки согласованности должны включать в себя, например:
- обнаружение аномальных всплесков мощности с помощью комбинированного мониторинга автоматической регулировки усиления (AGC) и отношения плотности несущей к шуму (C/N0);
 - последовательность измерений псевдодальностей и последовательность доплеровских измерений во времени, включая обнаружение резких скачков результатов измерений;
 - методы автономного контроля достоверности результатов измерения приемником (RAIM), включая обнаружение несоответствия результатов измерений с расчетным положением;
 - проверки положения и скорости, включая аномальные расчеты положения и скорости, внезапные скачки и поведение, не соответствующее динамике транспортного средства;
 - согласованность по времени и частоте, включая скачки и дрейф часов, которые не соответствуют характеристикам часов приемника.
- GNS_3b** Европейская комиссия разработает и утвердит следующие документы:
- документ, регламентирующий управление пространственным интерфейсом сигнала (SIS ICD), который детально определяет информацию OSNMA, передаваемую в сигнале системы «Галилей»;
 - руководство по эксплуатации приемника OSNMA, содержащее соответствующие требования и описание процессов в приемниках с целью гарантировать надежное введение в действие OSNMA, а также рекомендации по повышению эффективности OSNMA.
- Приемники ГНСС, установленные в тахографах, как внутренние, так и внешние, изготавливаются в соответствии с документом SIS ICD и руководством по эксплуатации приемника OSNMA.
- GNS_3c** Приемник ГНСС выдает сообщения о местоположении под названием «аутентифицированные сообщения о местоположении», которые рассчитываются с использованием только тех спутников, в случае которых достоверность навигационных сообщений была успешно проверена.
- GNS_3d** Приемник ГНСС также выдает стандартные сообщения о местоположении, рассчитанные с использованием спутников, находящихся в поле зрения, независимо от того, аутентифицированы они или нет.
- GNS_3e** Приемник ГНСС использует часы реального времени (RTC) БУ в качестве эталона времени для произвольной синхронизации времени, необходимой для работы OSNMA.

GNS3f Время RTC БУ выдается бортовым устройством приемнику ГНСС.

GNS3f Максимальный дрейф времени, указанный в требовании 41 добавления 1С, выдается бортовым устройством приемнику ГНСС вместе с временем RTC БУ.

~~Приемники ГНСС также могут быть способны принимать и обрабатывать сигналы SBAS.~~

3. Сообщения NMEA, выдаваемые приемником ГНСС

В этом разделе описаны предложения NMEA, используемые в работе смарт-тахографа для передачи стандартных и аутентифицированных сообщений о местоположении. Данный раздел актуален для обеих конфигураций смарт-тахографа: с внешним устройством ГНСС или без него.

GNS_4 Данные о стандартном местоположении строятся на основе рекомендуемого конкретного минимального уровня (RMC) данных ГНСС в предложении NMEA, в которых содержится информация о местоположении (широта, долгота), время в формате UTC (~~hhmmssshmmss.ss Договаривающиеся стороны.ss~~) и скорость относительно грунта в узлах плюс дополнительные значения.

Формат предложения RMC выглядит следующим образом (по стандарту NMEA V4.1):

Рис. 2

Структура предложения RMC

1	23	45	67	8	9	10	11	12
↓	↓↓	↓↓	↓↓	↓	↓	↓	↓	↓

\$--RMC,hhmmss.ss,A,llll.ll,a,yyyyy.yy,a,x.x,x.x,xxxx,x.x,a* hh

- 1) Time (UTC)
- 2) Status, A = Valid position, V = Warning
- 3) Latitude
- 4) N or S
- 5) Longitude
- 6) E or W
- 7) Speed over ground in knots
- 8) Track made good, degrees true
- 9) Date, ddmmyy
- 10) Magnetic Variation, degrees
- 11) E or W
- 12) Checksum

Статус указывает на наличие или отсутствие сигнала ГНСС. Пока значение статуса не установлено на А, использовать получаемые данные (например, время или широту/долготу) для регистрации местоположения транспортного средства в БУ невозможно.

Точность местоположения с точки зрения разрешающей способности представлена в формате описанного выше предложения RMC. Первая часть полей 3 и 5 (первые два числа) используется для отображения градусов. Остальная часть используется для отображения минут с тремя десятичными знаками. Таким образом, разрешение составляет 1/1000 минуты или 1/60000 градуса (поскольку одна минута — это 1/60 градуса).

GNS_4a Данные, касающиеся аутентифицированного местоположения, строятся на основе аутентифицированного минимального конкретного уровня (AMC) данных ГНСС, в которых содержится информация о местоположении (широта, долгота), время в формате

UTC (hhmmsshhmmss.ss) и скорость относительно грунта в узлах плюс дополнительные значения.

Формат предложения AMC выглядит следующим образом (по стандарту NMEA V4.1, за исключением значения номер 2):

Рис. 3

Структура предложения AMC

1	2 3	4 5	6 7	8	9	10	11 12
↓	↓↓	↓↓	↓↓	↓	↓	↓	↓ ↓

\$—AMC, hhmmss.ss, A, llll.ll, a, yyyu.yu, a, x.x, x.x, xxxx, x.x, a*hh

- 1) Время (UTC).
- 2) Статус, А = аутентифицированное местоположение (установлено с использованием, как минимум, 4 спутников, в случае которых аутентичность навигационных сообщений была успешно проверена), J = помехи или O = другая атака на ГНСС в случае отсутствия факта несостоявшейся аутентификации навигационных сообщений (по результатам проверки согласованности в соответствии с GNS_3a), F = несостоявшаяся аутентификация навигационных сообщений (обнаруженная в результате проверок OSNMA, указанных в документах, упомянутых в GNS_3b), V = отсутствует (аутентифицированное положение недоступно по любой иной причине).
- 3) Широта.
- 4) N или S.
- 5) Долгота.
- 6) E или W.
- 7) Скорость относительно грунта в узлах (SOG).
- 8) Линия фактического пути, градусы относительно истинного меридиана.
- 9) Дата, ддммгг.
- 10) магнитные вариации, градусы.
- 11) В или З.
- 12) Контрольная сумма.

Статус показывает, доступна ли аутентифицированная позиция GNSS, обнаружены ли помехи на уровне сигналов GNSS, удалось ли аутентифицировать навигационные сообщения или установить, что позиция GNSS недействительна. До тех пор, пока значение статуса не установлено на А, использовать получаемые данные (например, время или широту/долготу) для регистрации местоположения транспортного средства в БУ невозможно. Если значение статуса установлено на «J» (помехи), «O» (другие помехи на уровне ГНСС) или «F» (несостоявшаяся аутентификация навигационных сообщений), то в БУ регистрируется событие аномалии ГНСС, как определено в добавлении 1С и подразделе 1 (EventFaultCode).

GNS_5 Бортовое устройство хранит в базе данных БУ информацию о местоположении в виде широты и долготы с разрешением 1/10 минуты или 1/600 градуса, как описано в ~~приложении~~ **подразделе 1** для данных типа «GeoCoordinates».

БУ может использовать команду GPS DOP и активных спутников (GSA), на основе стандарта NMEA V4.11, для определения и регистрации наличия сигнала и точности **стандартных местоположений**. В частности, для указания на уровень точности зарегистрированных данных о местоположении используется HDOP (см. 4.2.2). БУ хранит

значение горизонтального показателя снижения точности (HDOP), рассчитываемого в качестве минимума значений HDOP, собранных со всех имеющихся систем ГНСС.

Идентификатор системы GNSS указывает ГНСС, Глонасс, «Бейду» или соответствующий идентификатор NMEA для каждой совокупности ГНСС и спутниковой системы дифференциальной коррекции (ССДК).

Рис. 43

Структура предложения GSA (стандартные позиции)

```

      1234          14151617 18
      ↓↓↓↓          ↓ ↓ ↓ ↓ ↓
$--GSA,a,a,x,x,x,x,x,x,x,x,x,x,x,x,x,x,x,x *hh
1) Selection mode
2) Mode
3) ID of 1st satellite used for fix
4) ID of 2nd satellite used for fix
...
14) ID of 12th satellite used for fix
15) PDOP
16) HDOP
17) VDOP
18) Checksum

```

Аналогичным образом БУ может использовать команду (ASA) на аутентификацию активных спутников по типу предложения NMEA для определения и записи наличия сигнала и точности аутентифицированных местоположений. Значения от 1 до 18 определены в стандарте NMEA V4.11.

Рис. 5

Структура предложения GSA (стандартные местоположения)

```

      1234          14 151617 18
      ↓↓↓↓          ↓ ↓ ↓ ↓ ↓
$—ASA,a,a,x,x,x,x,x,x,x,x,x,x,x,x,x,x,x,x*x*hh
1) Режим выбора (A = автовыбор, M: не используется)
2) Режим
3) ИД 1-го спутника, используемого в качестве привязки
4) ИД 2-го спутника, используемого в качестве привязки
...
14) ИД 12-го спутника, используемого в качестве привязки
15) PDOP
16) HDOP
17) VDOP
18) Контрольная сумма

```

Если режим (2) указывает, что местоположение не определено (режим 1) или что местоположение определено для 2D (режим 2) или 3D (режим 3).

GNS_6 В случае использования внешнего устройства ГНСС предложение GSA хранится в защищенном приеме-передатчике ГНСС с номером записи от «02» до «06», а предложение ASA — с номером записи от «12» до «16».

GNS_7 Максимальный размер предложений ~~NMEA~~ (например, RMC, AMC, GSA, ASA или других), который можно использовать для определения размера команды записи, составляет 85 байтов (см. ~~таблицу 49~~ таблицу 1).

4. Бортовое устройство с внешним устройством ГНСС

4.1 Конфигурация

4.1.1 Основные компоненты и интерфейсы

В этой конфигурации приемник ГНСС является частью внешнего устройства ГНСС.

GNS_8 Внешнее устройство ГНСС должно обеспечиваться питанием через специальный интерфейс транспортного средства.

GNS_9 Внешнее устройство ГНСС состоит из следующих компонентов (см. рисунок ~~64-17~~):

a) коммерческий приемник ГНСС, выдающий данные о местоположении через интерфейс данных ГНСС. Например, интерфейс данных ГНСС может соответствовать стандарту NMEA V4.10 в том случае, если приемник ГНСС действует в качестве рации и передает предложения NMEA на безопасный трансивер ГНСС с частотой 1 Гц для predetermined набора предложений NMEA, в которые должны быть, как минимум, включены предложения RMC, AMC, ~~и GSA и ASA~~. Использование интерфейса данных ГНСС определяется изготовителем внешнего устройства ГНСС по своему усмотрению;

b) блок трансивера (безопасный трансивер ГНСС), способный поддерживать стандарт ISO/IEC 7816-4:2013 (см. ~~5-2-1 4.2.1~~) в целях связи с бортовым устройством и поддержки интерфейса данных ГНСС с приемником ГНСС. Этот блок оснащен блоком памяти для хранения идентификационных данных приемника ГНСС и внешнего устройства ГНСС;

c) замкнутая система с функцией обнаружения взлома, вмещающая приемник ГНСС и безопасный трансивер ГНСС. Функция обнаружения взлома обеспечивает срабатывание системы обеспечения безопасности, требуемой в соответствии с характеристиками защиты смарт-тахографа;

d) антенна ГНСС, установленная на транспортном средстве и соединенная с приемником ГНСС через замкнутую систему.

GNS_10 Внешнее устройство ГНСС снабжено, как минимум, следующими внешними интерфейсами:

a) интерфейс с антенной ГНСС, установленной на транспортном средстве, если используется внешняя антенна;

b) интерфейс с бортовым устройством.

GNS_11 В БУ другим конечным объектом защищенной связи с безопасным трансивером ГНСС является безопасный трансивер БУ, который должен, в целях поддержания связи с внешним устройством ГНСС, соответствовать ISO/IEC 7816-4:2013.

GNS_12 В случае физического уровня связи с внешним устройством ГНСС бортовое устройство должно соответствовать ISO/IEC 7816-12:2005 или другому стандарту, который соответствует ISO/IEC 7816-4:2013 (см. ~~5-2-1 4.2.1~~).

4.1.2 Состояние внешнего устройства ГНСС на выходе из конвейера

GNS_13 На момент выпуска с завода внешнее устройство ГНСС хранит следующие параметры в постоянной памяти безопасного трансивера ГНСС:

- пара ключей EGF_MA и соответствующий сертификат;
- сертификат MSCA_VU-EGF, содержащий открытый ключ MSCA_VU-EGF.PK для проверки сертификата EGF_MA;
- сертификат EUR, содержащий открытый ключ EUR.PK для проверки сертификата MSCA_VU-EGF;
- сертификат EUR, срок действия которого непосредственно предшествует сроку действия сертификата EUR, используемого для проверки сертификата MSCA_VU-EGF, если таковой существует;
- связующий сертификат, соединяющий эти два сертификата EUR, если таковые существуют;
- расширенный серийный номер внешнего устройства ГНСС;
- идентификатор операционной системы устройства ГНСС;
- номер официального утверждения типа внешнего устройства ГНСС;
- идентификатор компонента защиты внешнего модуля ГНСС.

4.2 Связь между внешним устройством ГНСС и бортовым устройством

4.2.1 Протокол связи

GNS_14 Протокол передачи данных между внешним устройством ГНСС и бортовым устройством поддерживает три функции:

1. сбор и рассылка данных ГНСС (например, о местоположении, времени, скорости);
 2. сбор данных о конфигурации внешнего устройства ГНСС;
 3. протокол управления для поддержки соединения, взаимной аутентификации и согласования сеансовых ключей между внешним устройством ГНСС и БУ;
- 4. передача внешнему устройству GNSS показаний времени RTC БУ и максимальной разницы между истинным временем и временем RTC БУ.**

GNS_15 Протокол передачи данных строится на основе стандарта ISO/IEC 7816-4:2013, причем безопасный трансивер БУ играет в данном случае роль ведущего, а безопасный трансивер ГНСС — роль ведомого. В случае физической связи с внешним устройством ГНСС бортовое устройство поддерживает ISO/IEC 7816-12:2005 или другой стандарт, соответствующий стандарту ISO/IEC 7816-4:2013.

GNS_16 В протоколе передачи данных поля расширенной длины не поддерживаются.

GNS_17 Протокол передачи данных по стандарту ISO 7816 (как *-4:2013, так и *-12:2005) между внешним устройством ГНСС и БУ устанавливается как T = 1.

GNS_18 Что касается функций 1) сбора и рассылки данных ГНСС, 2) сбора данных о конфигурации внешнего устройства ГНСС и 3) протокола управления, то безопасный трансивер ГНСС имитирует смарт-карточку с архитектурой файловой системы, включающей в себя главный файл (MF), **специальный** файл (DF) с идентификатором приложения, указанным в ~~приложении~~ **подразделе** 1, глава 6.2 ('FF 44 54 45 47 4D')

и с тремя EF, содержащими сертификаты, а также с одним элементарным файлом (EF.EGF) с идентификатором файла, равным '2F2F', как описано в ~~таблице 49~~ **таблице 1**.

- GNS_18a** **Что касается функции 4) «передача внешнему средству ГНСС показаний времени RTC БУ и максимальной разницы между истинным временем и временем RTC БУ», то защищенный приемопередатчик ГНСС использует EF (EF VU) в том же DF с идентификатором файла, равным '2F30', как описано в таблице 1.**
- GNS_19 Безопасный трансивер ГНСС хранит данные, поступающие из приемника ГНСС, и конфигурацию в EF.EGF. Это — линейный файл с записями переменной длины, идентификатор которого в шестнадцатеричном формате равен '2F2F'.
- GNS_19a** **Безопасный трансивер ГНСС хранит данные, поступающие из БУ в EF VU. Это — линейный файл с записями фиксированной длины, идентификатор которого в шестнадцатеричном формате равен '2F30'.**
- GNS_20 Защищенный приемопередатчик ГНСС использует память для хранения данных **и должен быть** в состоянии выполнять ~~столько не менее 20 млн циклов записи/чтения/записи, сколько это необходимо~~ в течение срока службы не менее 15 лет. Помимо данного аспекта, внутренний дизайн и внедрение надежного приемопередатчика ГНСС оставляют на усмотрение изготовителей.

Структура номеров записей и данных представлена в ~~таблице 49~~ **таблице 1**. Следует отметить, что в настоящее время есть ~~четыре фразы~~ **пять предложений** GSA для ~~четырёх спутниковых систем~~ **спутниковых группировок ГНСС** и спутниковой системы контроля и коррекции (SBAS).

- GNS_21 Структура файла представлена в ~~таблице 49~~ **таблице 1**. Условия доступа (ALW, NEV, SM-MAC) см. в ~~добавлении~~ **подразделе 2**, глава 3.5.

Таблица 1
Структура файла

Файл	ИД файла	Чтение	Условия доступа	
			Обновление	Зашифрованный
MF	3F00			
EF.ICC	0002	ВСЕГДА	НИКОГДА (по БУ)	Нет
Устройство DF ГНСС	0501	ВСЕГДА	НИКОГДА	Нет
EF EGF_MACertificate	C100	ВСЕГДА	НИКОГДА	Нет
EF CA_Certificate	C108	ВСЕГДА	НИКОГДА	Нет
EF Link_Certificate	C109	ВСЕГДА	НИКОГДА	Нет
EF .EGF	2F2F	SM-MAC	НИКОГДА (по БУ)	
EF VU	2F30	SM-MAC	SM-MAC	Нет

Файл/элемент данных	Запись №	Размер (байты)	Значения по умолчанию		
			Мин.	Макс.	
MF			552	1031	
EF.ICC					
sensorGNSSSerialNumber			8	8	
DF устройства ГНСС			612	1023	
EF EGF_MACertificate			204	341	
EGFCertificate			204	341	{00..00}
EF CA_Certificate			204	341	
MemberStateCertificate			204	341	{00..00}
EF Link_Certificate			204	341	
LinkCertificate			204	341	{00..00}
EF -EGF					
Предложение NMEA RMC	'01'		85	85	
1-е предложение GSA NMEA	'02'		85	85	
2-е предложение GSA NMEA	'03'		85	85	
3-е предложение GSA NMEA	'04'		85	85	
4-е предложение GSA NMEA	'05'		85	85	
5-е предложение GSA NMEA	'06'		85	85	
Расширенный серийный номер внешнего устройства ГНСС, определенный в приложении подразделе 1 в качестве SensorGNSSSerialNumber	'07'		8	8	
Идентификатор операционной системы ГНСС, Безопасный приемо-передатчик определен в приложении подразделе 1 в качестве SensorGNSSSerialNumber	'08'		2	2	
Номер официального утверждения типа внешнего устройства ГНСС, определенного в приложении подразделе 1 в качестве SensorExternalGNSSApprovalNumber	'09'		16	16	
Идентификатор компонента защиты внешнего модуля ГНСС определен в приложении подразделе 1 в качестве SensorExternalGNSSIdentifier	'10'		8	8	
Предложение AMC	'11'		85	85	
1-е предложение ASA	'12'		85	85	
2-е предложение ASA	'13'		85	85	
3-е предложение ASA	'14'		85	85	
4-е предложение ASA	'15'		85	85	
5-е предложение ASA	'16'		85	85	
RFU — зарезервировано для использования в будущем	От '17' к 'FD'				
EF BU					
VuRtcTime (см. подраздел 1 добавления)	'01'		4	4	{00..00}
VuGnssMaximalTimeDifference (см. подраздел 1)	'02'		2	2	{00..00}

4.2.2 Защищенная передача данных ГНСС

GNS_22 Безопасная передача данных о местоположении ГНСС, **времени RTC БУ и максимальной разницы между истинным временем и временем RTC БУ** разрешается только в следующих условиях:

1. Процесс соединения завершен, как описано в ~~приложении~~ **подразделе 11**. Общие механизмы защиты.
2. Периодическая взаимная аутентификация и согласование сеансовых ключей между БУ и внешним устройством ГНСС, также описанные в ~~приложении~~ **подразделе 11**. Общие механизмы защиты действуют с указанной частотой.

GNS_23 Каждые T секунд, где T — значение, меньшее или равное ~~420~~, если только не происходит соединение или взаимная аутентификация и согласование сеансовых ключей, БУ направляет внешнему устройству ГНСС запрос на выдачу информации о местоположении в следующем порядке:

1. БУ запрашивает данные о местоположении из внешнего устройства ГНСС вместе с данными о показателе снижения точности (из предложений GSA и ~~ASA/NMEA~~). Безопасный трансивер БУ использует команды SELECT и READ RECORD(S) в соответствии с ISO/IEC 7816-4:2013 в порядке защищенного обмена сообщениями в режиме только аутентификации, как описано в ~~приложении 11~~, части **11.5 подраздела 11**, с идентификатором файла “2F2F” и значением RECORD, равным ‘01’, для предложения RMC NMEA, ‘02’, ‘03’, ‘04’, ‘05’, ‘06’ для предложения GSA NMEA, ‘11’ для предложения AMC и ‘12’, ‘13’, ‘14’, ‘15’, ‘16’ для предложения ASA.

2. Полученные данные о последнем **местоположении** ~~меете~~ хранятся в EF с идентификатором ‘2F2F’ и записями, описанными в ~~таблице 49~~ **таблице 1**, в безопасном трансивере ГНСС с учетом того, что безопасный трансивер ГНСС получает данные NMEA с частотой не менее 1 Гц из приемника ГНСС через интерфейс данных ГНСС.

3. Безопасный трансивер ГНСС передает ответ в безопасный трансивер БУ с помощью ответного сообщения APDU в порядке защищенного обмена сообщениями в режиме только аутентификации, как описано в ~~приложении 11~~, части **11.5 подраздела 11**.

4. Безопасный трансивер БУ проверяет аутентичность и целостность полученного ответа. В случае положительного результата данные о местоположении передаются в процессор БУ через интерфейс данных ГНСС.

5. Процессор БУ проверяет полученные данные, извлекая информацию (например, широту, долготу, время) из предложения RMC NMEA. Предложение RMC NMEA включает эту информацию в том случае, если данное **неаутофицированное** местоположение действительно. Если данное **неаутофицированное** местоположение недействительно, то ~~данные о нем остаются недоступными и не могут использоваться для регистрации местоположения транспортного средства. Если местоположение действительно, процессор БУ также извлекает значения HDOP из предложений GSA NMEA и вычисляет среднее минимальное значение по имеющимся спутниковым системам (т. е. когда данное местоположение зафиксировано).~~

6. Процессор БУ **также извлекает информацию (например, широту, долготу, время) из предложения AMC. Предложение AMC включает эту информацию в том случае, если местоположение, заслуживающее доверия, недействительно или если сигнал GNSS был подвергнут воздействию помех. Если позиция действительна, то процессор БУ также извлекает значения HDOP из предложений ASA и вычисляет минимальное значение по доступным спутниковым системам (т. е. когда доступно соответствующее фиксированное положение), сохраняет полученную и обработанную информацию, такую как широта, долгота, время и скорость в БУ в формате, определенном в Словаре данных приложения 1 в виде геокоординат вместе со значением HDOP, вычисленным как минимальное из значений HDOP, собранных по доступным системам GNSS.**

GNS_23a БУ также записывает время RTC БУ и максимальную разницу между истинным временем и, по мере необходимости, временем RTC БУ, используя команды ISO/IEC 7816-4:2013 SELECT (выбрать) и WRITE RECORD(S) (произвести запись(и)) в режиме безопасного обмена сообщениями только для аутентификации, как описано в части 11.5 подраздела 11 с идентификатором файла '2F30' и номером RECORD равным '01' для параметров VuRtcTime и '02' для MaximalTimeDifference.

4.2.3 Структура команды Read Record (считывание записи)

В настоящем разделе подробно описана структура команды Read Record. Кроме того, дополнительно обеспечивается защищенный обмен сообщениями (в режиме только аутентификации), как описано в ~~приложении~~ подразделе 11 «Общие механизмы безопасности».

GNS_24 Эта команда поддерживает защищенный обмен сообщениями в режиме только аутентификации, см. ~~приложение~~ подраздел 11.

GNS_25 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'0Ch'	Открытая экспонента ключа RSA
INS	1	'B2h'	Считывание записи
P1	1	'XXh'	Номер записи ('00' относится к текущей записи)
P2	1	'04h'	Считывание записи с номером записи, указанным в P1
Le	1	'XXh'	Ожидаемая длина записи. Число байтов, подлежащих считыванию

GNS_26 Запись, указанная в P1, становится текущей записью.

Байт	Длина	Значение	Описание
#1-#X	X	'XX..XXh'	Считанные данные
ME	2	'XXXXh'	Характеристики состояния (SW1,SW2)

- Если команда проходит успешно, то безопасный трансивер ГНСС выдает '9000'.
- Если текущий файл не имеет доступа к записям, то безопасный трансивер ГНСС выдает '6981'.
- Если команда используется с P1 = '00', но текущего EF нет, то безопасный трансивер ГНСС выдает '6986' (команда не допускается).
- Если текущий файл не найден, то безопасный трансивер ГНСС выдает '6A83'.
- Если внешнее устройство ГНСС обнаружило взлом, то оно выдает характеристику статуса '6690'.

GNS_27 ~~Безопасный трансивер ГНСС поддерживает следующие команды тахографа второго поколения, указанные в приложении подраздел 2:~~

Команда	Ссылка
Выбрать	Приложение подраздел 2 добавления, глава 3.5.1
Считывание данных	Приложение подраздел 2 добавления, глава 3.5.2
Получить запрос	Приложение подраздел 2 добавления, глава 3.5.4
PSO: Проверка сертификата	Приложение подраздел 2 добавления, глава 3.5.7

Команда	Ссылка
Внешняя аутентификация	Приложение подраздел 2 добавления , глава 3.5.9
Общая аутентификация	Приложение подраздел 2 добавления , глава 3.5.10
MSE:SET	Приложение подраздел 2 добавления , глава 3.5.11

4.2.4 Структура команды Read Record (считывание записи)

В данном разделе подробно описана структура команды Read Record. Кроме того, дополнительно обеспечивается защищенный обмен сообщениями (в режиме только аутентификации), как описано в ~~приложении~~ подразделе 11 «Общие механизмы безопасности».

GNS_26a Эта команда поддерживает защищенный обмен сообщениями в режиме только аутентификации, см. подраздел 11.

GNS_26b Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'0Ch'	Запрос на защищенный обмен сообщениями
INS	1	'D2h'	Произвести запись
P1	1	'XXh'	Номер записи ('00' относится к текущей записи)
P2	1	'04h'	Считать запись с номером записи, указанным в P1
Данные	X	'XXh'	Данные

GNS_26c Запись, указанная в P1, становится текущей записью.

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики состояния (SW1, SW2)

- Если команда проходит успешно, то безопасный трансивер ГНСС выдает '9000'.
- Если текущий файл не имеет доступа к записям, то безопасный трансивер ГНСС выдает '6981'.
- Если команда используется с P1 = '00', но текущего EF нет, то безопасный трансивер ГНСС выдает '6986' (команда не проходит).
- Если текущий файл не найден, то безопасный трансивер ГНСС выдает '6A83'.
- Если внешнее устройство ГНСС обнаружило взлом, то оно выдает характеристику статуса '6690'.

4.2.5 Другие команды

GNS_27 Безопасный трансивер ГНСС поддерживает следующие команды тахографа второго поколения, указанные в подразделе 2 добавления:

Команда	Ссылка
Выбрать	Подраздел 2 добавления, глава 3.5.1
Считать данные	Подраздел 2 добавления, глава 3.5.2
Получить запрос	Подраздел 2 добавления, глава 3.5.4
PSO: Проверить сертификат	Подраздел 2 добавления, глава 3.5.7
Произвести внешнюю аутентификацию	Подраздел 2 добавления, глава 3.5.9
Произвести общую аутентификацию	Подраздел 2 добавления, глава 3.5.10
MSE:SET	Подраздел 2 добавления, глава 3.5.11

4.3 Соединение, взаимная аутентификация и согласование сеансовых ключей между внешним устройством ГНСС и бортовым устройством

Соединение, взаимная аутентификация и согласование сеансовых ключей между внешним устройством ГНСС и бортовым устройством описаны в ~~приложении~~ подразделе 11. Общие механизмы защиты, глава 11.

4.4 Обработка ошибок

В настоящем разделе описывается, каким образом обрабатываются возможные условия ошибок внешним устройством ГНСС и как они записываются в БУ.

4.4.1 Ошибка связи с внешним устройством ГНСС

GNS_28 Если БУ не может связаться с соединенным с ним внешним устройством ГНСС в течение более чем 20 минут подряд, то БУ генерирует и регистрирует событие типа EventFaultType со значением enum ~~‘53’H~~ **‘0E’H Ошибка связи с внешним устройством ГНСС** и указанием метки времени по отношению к текущему времени. Это событие генерируется только в случае выполнения двух следующих условий: а) смарт-тахограф не находится в режиме калибровки и б) транспортное средство движется. В данном контексте ошибка связи инициируется в том случае, когда безопасный трансивер БУ не получает ответное сообщение на направленный ему запрос, как описано в ~~5.2~~ **4.2**.

4.4.2 Нарушение физической целостности внешнего устройства ГНСС

GNS_29 Если внешнее устройство ГНСС взломано, безопасный трансивер ГНСС ~~перекрывает доступ к криптографическим материалам стирает всю свою память, включая криптографические материалы.~~ Как описано в GNS_25 и GNS_26, БУ обнаруживает факт взлома, если статус ответа ~~‘6690’~~. Затем БУ генерирует событие, ~~как оно определено в требовании 85 добавления 1С и подразделе 1 тина (EventFaultType в случаеenum ‘55’H–‘19’H «обнаружения взлома ГНСС»).~~ **как оно определено в требовании 85 добавления 1С и подразделе 1 тина (EventFaultType в случаеenum ‘55’H–‘19’H «обнаружения взлома ГНСС»).** В качестве альтернативы внешнее устройство ГНСС может не отвечать на запросы БУ без защищенного обмена сообщениями и со статусом **‘6A88’** на любой внешний запрос.

4.4.3 Отсутствие информации со стороны приемника ГНСС о местоположении

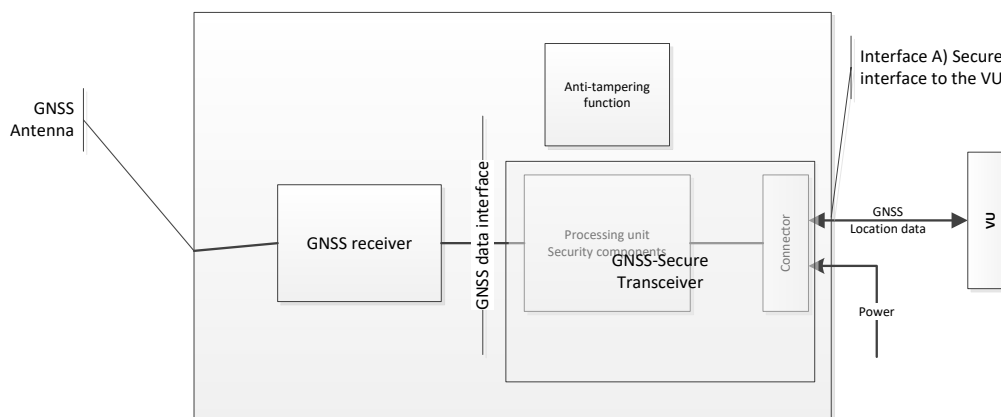
GNS_30 Если безопасный трансивер ГНСС не получает данные из приемника ГНСС ~~в течение более чем 3 часов подряд~~, то этот безопасный трансивер ГНСС генерирует ответное сообщение на команду READ RECORD с номером RECORD, равным **‘01’**, и 12-байтовым полем данных, установленным на 0xFF. По получении ответного сообщения с таким значением поля данных БУ генерирует и регистрирует ~~событие типа EventFaultType enum ‘52’H Ошибка внешнего~~ **‘0D’H факт отсутствия информации со стороны приемника ГНСС о местоположении, как оно определено в требовании 81 добавления 1С и подраздела 1 добавления (EventFaultType) с указанием времени, равным текущему значению времени, только если выполнены два следующих условия:** а) ~~«умный» тахограф не находится в режиме калибровки~~ и б) ~~транспортное средство движется.~~

4.4.4 Истекший срок действия сертификата внешнего устройства ГНСС

GNS_31 Если БУ обнаруживает, что сертификат EGF, используемый для взаимной аутентификации, больше не действителен, БУ генерирует и регистрирует событие в виде попытки нарушения безопасности, **как оно определено в требовании 85 добавления 1С и подраздела 1**

(EventFaultType: истечение срока действия сертификата внешнего устройства ГНСС) регистрирует событие неисправности устройства управления оборудованием записи типа EventFaultType enum '56' и '1B' и истечение срока действия сертификата устройства ГНСС с временной меткой, соответствующей текущему времени. Тем не менее БУ все еще продолжает использовать полученные данные ГНСС о местоположении.

Рис. 64
Схема внешнего устройства ГНСС



5. Бортовое устройство без внешнего устройства ГНСС

5.1 Конфигурация

В данной конфигурации приемник ГНСС встроен в бортовое устройство, как это отображено на рисунке 144.

GNS_32 В целях передачи данных о местоположении, DOP и спутниковых данных Приемник ГНСС работает как рация и передает предложения NMEA или похожие на NMEA в процессор БУ, который действует в качестве приемника и принимает их с частотой 1/10 Гц или более в случае предопределенного набора предложений NMEA, в который входят, как минимум, предложения, RMC, и GSA, AMC и ASA. В качестве альтернативного варианта процессор БУ и внутренний приемник GNSS могут использовать другие форматы данных для обмена информацией, содержащейся в предложениях NMEA или похожих на NMEA, которые указаны в GNS_4, GNS_4a и GNS_5.

GNS_33 К БУ подсоединяется внешняя антенна ГНСС, установленная на транспортном средстве, или внутренняя антенна ГНСС.

5.2 Ошибка в обработке передачи информации от приемника ГНСС в БУ

GNS_34 Процессор БУ проверяет полученные данные, извлекая информацию (например, широту, долготу, время) из предложения RMC NMEA и предложения AMC.

GNS_35 Предложение RMC NMEA включает эту информацию в том случае, если данное неаутентифицированное местоположение действительно. Если данное неаутентифицированное местоположение недействительно, то данные о нем остаются недоступными и не могут использоваться для регистрации местоположения транспортного средства. Если

неаутентифицированное местоположение действительно, то процессор БУ также извлекает значения HDOP из GSA NMEA.

GNS_36 Процессор БУ также извлекает информацию (например, широту, долготу, время) из предложения AMC. Предложение AMC включает эту информацию в том случае, если в соответствии с GNS_4a данное неаутентифицированное местоположение действительно. Если это неаутентифицированное местоположение действительно, то процессор БУ также извлекает значения HDOP из предложений ASA NMEA.

5.3 Передача информации из БУ в приемник ГНСС

GNS_37 Процессор БУ передает приемнику ГНСС время RTC БУ и максимальную разницу между истинным временем и временем RTC БУ в соответствии с GNS_3f и GNS_3g.

5.4 Обработка ошибок

5.4.2.1 Отсутствие информации от приемника ГНСС о местоположении

GNS_384 БУ генерирует и регистрирует событие отсутствия информации о местоположении от приемника ГНСС, как определено в требовании 81 добавления 1С и подраздела 1 (EventFaultType) Если БУ не получает данные от приемника ГНСС более 3 часов подряд, БУ генерирует и регистрирует событие типа EventFaultType enum 'S1'Н Internal'0D'Н ~~Отсутствие информации о местоположении от приемника ГНСС с меткой времени, равной текущему значению времени, только если выполнены следующие два условия: а) смарт-тахограф не находится в режиме калибровки и б) транспортное средство движется.~~

6. Обработка и регистрация данных о местоположении с помощью БУГНСС ~~Нестыковка во времени~~

Этот раздел относится к конфигурации смарт-тахографа как с внешним устройством ГНСС, так и без него. Если БУ обнаруживает несоответствие более чем на 1 минуту между временем функции измерения времени бортового устройства и временем приемника ГНСС, БУ регистрирует событие типа EventFaultType enum '0B'Н ~~Нестыковка во времени (ГНСС и внутренних часов БУ). Данное событие регистрируется вместе со значением внутренних часов бортового устройства и отображается вместе с автоматической корректировкой времени. После возникновения события, связанного с противоречивой информацией о времени, БУ не будет проверять несоответствия времени в течение следующих 12 часов. Данное событие не отображается в тех случаях, когда приемник ГНСС не обнаруживает действительного сигнала ГНСС в течение последних 30 дней. Однако если информация о местоположении из приемника ГНСС появляется снова, производится автоматическая корректировка времени.~~

GNS_39 Данные о местоположении должны храниться в БУ вместе с меткой, указывающей на то, было ли данное местоположение аутентифицировано. Когда данные о местоположении надлежит записывать в БУ, применяются следующие правила:

а) Если и аутентифицированное и стандартное местоположения действительно и согласованы, то стандартное положение и его точность записываются в БУ, а метка устанавливается в положение «аутентифицировано».

b) Если оба положения — аутентифицированное и стандартное — действительны, но не соответствуют друг другу, то БУ сохраняет аутентифицированное положение и его точность, а метка устанавливается в положение «аутентифицирован».

c) Если аутентифицированное положение действительно, а стандартное положение недействительно, то БУ записывает аутентифицированное положение и его точность, а метка устанавливается в положение «аутентифицировано».

d) Если стандартное положение действительно, а аутентифицированное положение недействительно, то БУ записывает стандартное положение и его точность, а метка устанавливается в положение «не аутентифицировано».

Аутентифицированное и стандартное местоположения считаются согласованными, как показано на рисунке 7, в том случае, если аутентифицированное местоположение по горизонтали можно найти внутри окружности с центром, расположенным в стандартном местоположении по горизонтали, радиус которой представляет собой результат округления значения R_H , рассчитанного по нижеследующей формуле, до ближайшего большего целого числа:

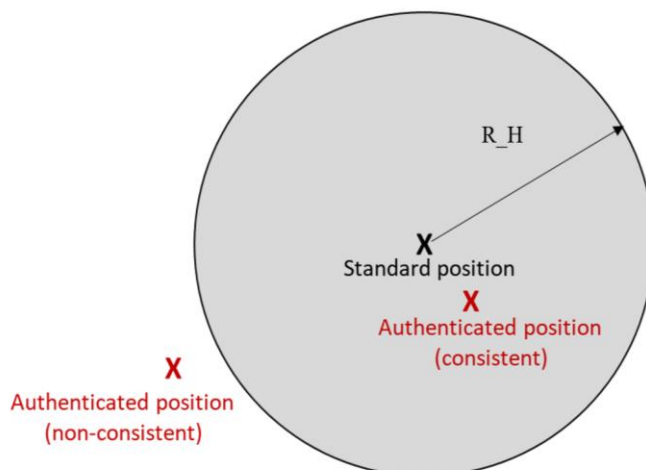
$$R_H = 1,74 \cdot \sigma_{UERE} \cdot HDOP,$$

где:

- R_H — относительный радиус окружности, описанной вокруг расчетного местоположения по горизонтали, в метрах. Это — показатель, который используется для проверки соответствия между стандартными и аутентифицированными местоположениями;
- σ_{UERE} — стандартная эквивалентная погрешность измерения дальности пользователем (UERE), которая моделирует все ошибки измерения для целевого применения, включая городские условия. Используется постоянное значение $UERE = 10$ метров;
- $HDOP$ — снижение точности по горизонтали, рассчитанное приемником ГНСС;
- $\sigma_{UERE} \cdot HDOP$ — оценка среднеквадратичной ошибки по горизонтали.

Рисунок 7

Последовательные аутентифицированные и стандартные (неаутентифицированные) местоположения



GNS_40 Когда значение Status (статус) в принятом предложении АМС установлено на 'J' или 'O', или 'F' в соответствии с требованием

GNS_4a, БУ должен генерировать и регистрировать событие аномалии GNSS, как определено в требовании 88a добавления 1С и подраздела 1 (EventFaultType). Бортовое устройство может выполнять дополнительные проверки перед сохранением события аномалии ГНСС после получения настройки 'J' или 'O'.

7. Нестыковка во времени ГНСС

GNS_41 Если БУ обнаруживает расхождение в показаниях времени между функцией измерения времени бортового устройства и показаниях времени, полученных по несущим сигналам ГНСС, оно генерирует и регистрирует событие нестыковки во времени, как оно определено в требовании 86 добавления 1С и подраздела 1 этого добавления (EventFaultType).

8. Противоречивые данные о движении транспортного средства

GNS_4235 БУ инициирует и регистрирует событие «противоречивые данные о движении транспортного средства» ~~(см. в соответствии с требованием 84 добавления 1С в настоящем приложении)~~ с указанием времени, ~~равного текущему значению времени,~~ в том случае, если данные о движении, вычисляемые по датчику движения, противоречат данным о движении, вычисляемым по внутреннему приемнику ГНСС или внешнему устройству ГНСС, **а равно по другому(им) независимому(ым) источнику(ам) движения, как указано в требовании 26 добавления 1С.**

Событие «противоречивые данные о движении транспортного средства» инициируется в случае возникновения одного из следующих условий срабатывания:

Условие срабатывания 1:

~~Для выявления таких противоречий~~ При наличии информации о местоположении от приемника ГНСС и при включенном зажигании транспортного средства, используется усеченное медианное среднее значение разности скоростей между этими источниками, как указано ниже:

- максимум каждые 10 секунд вычисляется абсолютное значение разницы между скоростью транспортного средства, оцениваемой по ГНСС, и скоростью, оцениваемой по датчику движения;
- все вычисляемые значения во временном окне, содержащие последние пять минут движения, используются для вычисления **усеченного медианного среднего** значения;
- **усеченное медианное среднее** значение вычисляется как среднее от 80 % остальных показаний после исключения наибольших абсолютных значений.

Событие, связанное с противоречивыми данными о движении транспортного средства, инициируется в том случае, если **усеченное медианное среднее** значение превышает 10 км/ч в течение пяти последовательных минут движения транспортного средства. ~~Для более надежного обнаружения манипуляций с тахографом возможно факультативное применение других независимых источников обнаружения движения транспортного средства.~~ (Примечание: **Усеченное медианное среднее** значение за последние 5 минут применяется в порядке снижения риска, обусловленного посторонними и мгновенными значениями).

Для расчета усеченного среднего значения транспортное средство считается движущимся, если, как минимум, одно значение скорости транспортного средства, выданное либо датчиком движения, либо приемником GNSS, не равно нулю. Это событие не должно инициироваться в следующих условиях: а) во время переправы на пароме/поезде, б) когда информация о положении от приемника GNSS недоступна и в) в режиме калибровки.

Условие срабатывания 2:

Событие, связанное с противоречивыми данными о движении транспортного средства, инициируется также в том случае, если верно следующее условие:

$$GnssDistance > [OdometerDifference \times OdometerToleranceFactor + \text{Minimum}(SlipDistanceUpperlimit; (OdometerDifference \times SlipFactor)) + GnssTolerance + FerryTrainDistance],$$

где:

- *GnssDistance* — расстояние между нынешним положением транспортного средства и предыдущим, полученным в том и другом случае из действительных аутентифицированных сообщений о местоположении без учета высоты;
- *OdometerDifference* — разница между текущим показанием счетчика пробега и показанием счетчика пробега, соответствующим предыдущему достоверному аутентифицированному сообщению о местоположении;
- *OdometerToleranceFactor* равен 1.1 (наихудший допустимый коэффициент для всех допусков показаний счетчика пробега транспортного средства);
- *GnssTolerance* — допустимое отклонение, равно 1 км (наихудший случай допустимого отклонения GNSS);
- *Minimum (SlipDistanceUpperLimit* — верхний предел расстояния проскальзывания; $(OdometerDifference * SlipFactor)$) — минимальное значением между:
 - *SlipDistanceUpperLimit* (верхний предел расстояния проскальзывания), который равен 10 км (верхний предел расстояния проскальзывания, вызванного эффектом скольжения при торможении);
 - и $OdometerDifference * SlipFactor$ (разница в показаниях счетчика пробега и коэффициент проскальзывания), в котором *SlipFactor* равен 0,2 (максимальное влияние эффекта скольжения в процессе торможения),
 - Расстояние *FerryTrainDistance* рассчитывается следующим образом: $FerryTrainDistance = 200 \text{ км/ч} * t_{FerryTrain}$, где *tFerryTrain* — общая продолжительность перевозки в часах на железнодорожных паромах в рассматриваемом интервале времени. Продолжительность паромной/железнодорожной перевозки определяется как разница во времени между временной меткой ее окончания и временной меткой ее начала.

Предыдущие проверки выполняются через каждые 15 минут, если имеются необходимые данные о местоположении, в противном случае — сразу после получения данных о местоположении.

В случае этого условия срабатывания:

- дата и время начала события должны соответствовать дате и времени получения предыдущего сообщения о местоположении;
- дата и время окончания события должны соответствовать дате и времени, когда проверяемое условие снова становится ложным.

Условие срабатывания 3:

Бортовое устройство обнаруживает несоответствие, суть которого состоит в том, что датчик движения не обнаруживает никакого движения, а независимый источник движения обнаруживает движение в течение определенного периода времени. Условия регистрации несоответствия, а также период обнаружения несоответствия устанавливаются изготовителем бортового устройства транспортного средства, хотя это несоответствие обнаруживается не более чем через три часа.

Подраздел 13

Интерфейс ИТС

Содержание

	<i>Стр.</i>
1. Введение	541
1.1 Сфера охвата	541
1.2 Акронимы и определения	541
2. Стандарты, на которые сделаны ссылки	541
3. Принципы работы интерфейса ИТС	542
3.1 Технология связи	542
3.2 Доступные функции	542
3.3 Доступ через интерфейс ИТС	543
3.4 Доступные данные и необходимость согласия водителя	545
4. Перечень данных, доступных через интерфейс ИТС, и классификация личных/ неличных данных	545
2. Сфера охвата	548
 2.1 Сокращения, определения и обозначения	548
3. Ссылки на регламенты и стандарты	549
4. Принципы работы интерфейса	549
 4.1 Предварительные условия передачи данных через интерфейс ИТС	549
 4.1.1 Данные, передаваемые через интерфейс ИТС	550
 4.1.2 Содержание данных	550
 4.1.3 Приложения ИТС	550
 4.2 Технология связи	550
 4.3 Получение доступа при помощи ПИН кода	551
 4.4 Формат сообщения	552
 4.5 Согласие водителя	557
 4.6 Извлечение стандартных данных	557
 4.7 Извлечение личных данных	557
 4.8 Извлечение данных о событиях и неисправностях	558

1. Введение

1.1 Сфера охвата

ITS_01 В настоящем ~~приложении подразделе добавления~~ изложены базовые принципы связи ~~дизайн и процедуры реализации~~ через посредство интерфейса тахографа с интеллектуальными транспортными системами (ИТС) ~~в соответствии с требованиями статьи 10 Регламента (ЕС) № 165/2014 (регламент).~~

ITS_02 Интерфейс ИТС должен позволять внешним устройствам получать данные от тахографа, использовать функции тахографа, а также предоставлять тахографу соответствующие данные.

Для этой цели могут использоваться и другие интерфейсы тахографа (например, шина CAN).

В этом подразделе не уточняется:

- каким образом производится сбор и обработка данных в тахографе, передаваемых через интерфейс ИТС;
- форма отображения собранных данных в приложениях, установленных на внешнем устройстве;
- требования к безопасности ИТС в дополнение к тому, что обеспечивает система Bluetooth®;
- протоколы Bluetooth®, используемые интерфейсом ИТС.

1.2 Акронимы и определения

В настоящем приложении используются следующие сокращения и определения:

ГНСС	Глобальная навигационная спутниковая система
ИТС	Интеллектуальная транспортная система
ВОС	Взаимосвязь открытых систем
БУ	Бортовое устройство
Блок ИТС	внешнее устройство или приложение, использующее интерфейс БУ ИТС

2. Стандарты, на которые сделаны ссылки

ITS_03 Данный подраздел добавления, содержит ссылки на все или некоторые части следующих правил и стандартов и использует их в качестве основы. В положениях настоящего подраздела содержатся ссылки на соответствующие стандарты или на содержащиеся в них соответствующие положения. В случае любого противоречия преимущественную силу имеют положения настоящего приложения.

Стандарты, на которые сделаны ссылки в данном подразделе, указаны ниже:

- Bluetooth®. Основная версия 4.2;
- ISO 16844 — 7: Транспорт дорожный. Системы тахографов. Часть 7: Параметры;
- ISO/IEC 7498-1:1994 Информационные технологии — Взаимосвязь открытых систем — Базовая справочная модель, Базовая модель.

3. Принципы работы интерфейса ИТС

ITS_04 БУ отвечает за обновление и поддержку данных тахографа, передаваемых через интерфейс ИТС, без какого бы то ни было взаимодействия в этом процессе интерфейса ИТС.

3.1 Технология связи

ITS_05 Связь через интерфейс ИТС осуществляется через интерфейс Bluetooth® и должна быть совместимой с системой «Bluetooth® Low Energy» в соответствии с версией Bluetooth 5.0 или более новой.

ITS_06 Связь между БУ и устройством ИТС устанавливается после завершения процесса сопряжения Bluetooth®.

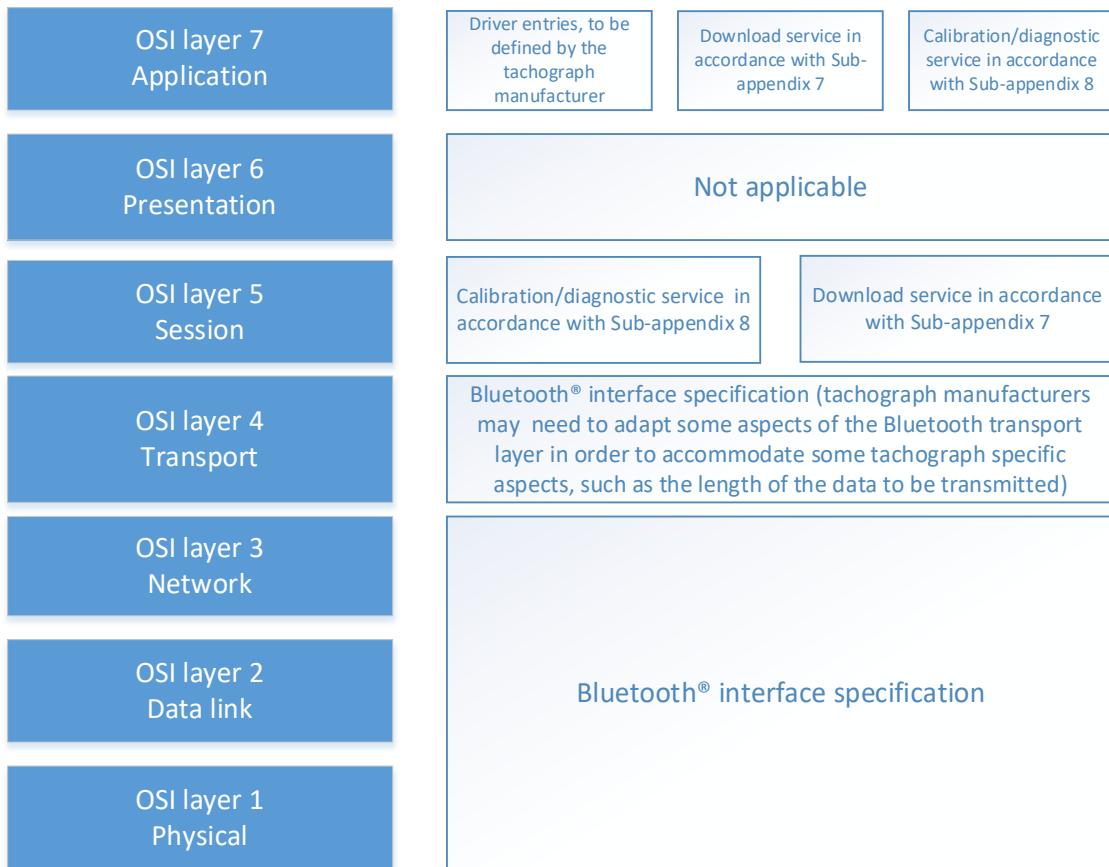
ITS_07 Между БУ и устройством ИТС устанавливается защищенная и зашифрованная связь в соответствии с механизмами спецификации Bluetooth®. В данном подразделе не указываются механизмы шифрования или какие-либо другие механизмы защиты в дополнение к тем, которые обеспечиваются по линии Bluetooth®.

ITS_08 Bluetooth® использует модель «сервер/клиент» для управления передачей данных между соответствующими устройствами, в случае которых БУ является «сервером», а устройство ИТС — «клиентом».

3.2 Доступные функции

ITS_09 Данные, которые должны передаваться через интерфейс ИТС в соответствии с пунктом 4, должны быть доступны через служебные сервисы, указанные в подразделе 7 и подразделе 8 добавления. Кроме того, БУ предоставляет блоку ИТС возможность использовать функции, необходимые для ручного ввода данных в соответствии с требованием 61 добавления 1С, и, в факультативном порядке, для ввода других данных в режиме реального времени.

Разделение системы связи через интерфейс ИТС в соответствии с уровнями модели сетевой модели OSI



ITS_10 Если интерфейс загрузки используется через передний разъем, то БУ не обеспечивает сервисные услуги по загрузке, указанные в подразделе 7, через соединение ITS Bluetooth®.

ITS_11 Если интерфейс калибровки используется через передний разъем, то БУ не обеспечивает сервисные услуги по калибровке, указанные в подразделе 8, через соединение ITS Bluetooth®.

3.3 Доступ через интерфейс ИТС

ITS_12 Интерфейс ИТС обеспечивает беспроводной доступ ко всем услугам, указанным в подразделе 7 и подразделе 8, вместо кабельного соединения с подключением к переднему соединителю для калибровки и загрузки, указанному в подразделе 6.

ITS_13 БУ обеспечивает доступ пользователя к интерфейсу ИТС в соответствии с комбинацией действительных карточек тахографа, вставленных в БУ, как указано в таблице 1.

Доступ к интерфейсу ИТС		Считывающее устройство водителя				
		Карточка не введена	Карточка водителя	Карточка контролера	Карточка мастерской	Карточка предприятия
Считывающее устройство второго водителя	Карточка не вставлена	Недоступна	Доступна	Доступна	Доступна	Доступна
	Карточка водителя	Доступна	Доступна	Доступна	Доступна	Доступна
	Карточка контролера	Доступна	Доступна	Доступна	Недоступна	Недоступна
	Карточка мастерской	Доступна	Доступна	Недоступна	Доступна	Недоступна
	Карточка предприятия	Доступна	Доступна	Недоступна	Недоступна	Доступна

Таблица 1 — Доступность интерфейса ИТС в зависимости от типа карточки, вставленной в тахограф

ITS_14 После успешного сопряжения ITS с Bluetooth® БУ передает функцию соединения ITS Bluetooth® для конкретной карточки, вставленной в тахограф, в соответствии с таблицей 2:

Назначение соединения ITS–Bluetooth®		Считывающее устройство водителя				
		Карточка не вставлена	Карточка водителя	Карточка контролера	Карточка мастерской	Карточка предприятия
Считывающее устройство второго водителя	Карточка не вставлена	Недоступна	Карточка водителя	Карточка контролера	Карточка мастерской	Карточка предприятия
	Карточка водителя	Карточка водителя	Карточка водителя (**)	Карточка контролера	Карточка мастерской	Карточка предприятия
	Карточка контролера	Карточка контролера	Карточка контролера	Плата управления (*)	Недоступна	Недоступна
	Карточка мастерской	Карточка мастерской	Карточка мастерской	Недоступна	Карточка мастерской (*)	Недоступна
	Карточка предприятия	Карточка предприятия	Карточка предприятия	Недоступна	Недоступна	Карточка предприятия (*)

Таблица 2 — Доступность интерфейса ИТС в зависимости от типа карточки, вставленной в тахограф

(*) Функция соединения ITS-Bluetooth® задается карточке тахографа в считывающем устройстве водителя БУ.

(**) Пользователь выбирает карточку (вставленную в считывающее устройство водителя или второго водителя), которой задается соединение ITS-Bluetooth®.

ITS_15 Если карточка тахографа извлекается, то БУ прерывает соединение ITS-Bluetooth®, которое было задано этой карточке.

ITS_16 БУ поддерживает подключение ИТС, как минимум, к одному устройству ИТС, но может поддерживать подключение и к нескольким устройствам ИТС одновременно.

ITS_17 Права доступа к данным и сервисам, доступным через интерфейс ИТС, должны соответствовать требованиям 12 и 13 добавления 1С, в дополнение к согласию водителя, предусмотренному в разделе 3.4 данного подраздела.

3.4 Доступные данные и необходимость согласия водителя

- ITS_18** Все данные тахографа, доступные по линии сервисов, указанных в пункте 3.3, классифицируются как личные или неличные для водителя, второго водителя или их обоих.
- ITS_19** Через интерфейс ИТС должен быть доступен, как минимум, перечень данных, отнесенных в разделе 4 к категории обязательных.
- ITS_20** Данные в разделе 4, которые классифицируются как «личные», должны быть доступны только с согласия водителя, поэтому допускается, что персональные данные могут быть извлечены из сети транспортного средства, за исключением случая, указанного в требовании ITS_25, когда согласие водителя не требуется.
- ITS_21** Данные, дополнительные к тем, которые сведены воедино в пункте 4 и считаются обязательными, могут быть доступны через интерфейс ИТС. Дополнительные данные, не включенные в пункт 4, классифицируются изготовителем БУ как «личные» или «неличные», при том что согласие водителя испрашивается на те данные, которые были классифицированы как личные, за исключением случая, указанного в требовании ITS_25, когда согласие водителя не требуется.
- ITS_22** В случае введения карточки водителя, неизвестной бортовому устройству, владельцу карточки выдается запрос тахографа на подтверждение своего согласия на передачу личных данных, выводимых через интерфейс ИТС, в соответствии с требованием 61 добавления 1С.
- ITS_23** Статус согласия (подтверждено/не подтверждено) записывается в блоке памяти тахографа.
- ITS_24** Если водителей несколько, то доступ к личным данным через интерфейс ИТС будет открыт только для тех водителей, которые дали свое согласие. Например, в случае ситуации с экипажем, если свое согласие дал только водитель, то личные данные, относящиеся ко второму водителю, будут недоступны.
- ITS_25** Когда БУ находится в режиме управления, предприятия или калибровки, права доступа через интерфейс ИТС регламентируются требованиями 12 и 13 добавления 1С, поэтому согласие водителя не требуется.

4. Перечень данных, доступных через интерфейс ИТС, и классификация личных/неличных данных

Название данных	Формат данных	Источник	Классификация данных (личные/не личные)		Согласие на доступность данных	Доступность
			водитель	второй водитель		
VehicleIdentificationNumber (идентификационный номер транспортного средства)	Добавление 8	БУ	не личные	не личные	согласие не требуется	обязательно
CalibrationDate	ISO 16844-7	БУ	не личные	не личные	согласие не требуется	обязательно
TachographVehicleSpeed	ISO 16844-7	БУ	личные	Н/П	согласие водителя	обязательно
Driver1WorkingState	ISO 16844-7	БУ	личные	Н/П	согласие водителя	обязательно
Driver2WorkingState	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	обязательно
DriveRecognize	ISO 16844-7	БУ	не личные	не личные	согласие не требуется	обязательно
Driver1TimeRelatedStates	ISO 16844-7	БУ	личные	Н/П	согласие водителя	обязательно

Название данных	Формат данных	Источник	Классификация данных (личные/не личные)		Согласие на доступность данных	Доступность
			водитель	второй водитель		
Driver2TimeRelatedStates	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	обязательно
DriverCardDriver1	ISO 16844-7	БУ	личные	Н/П	согласие водителя	обязательно
DriverCardDriver2	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	обязательно
OverSpeed	ISO 16844-7	БУ	личные	Н/П	согласие водителя	обязательно
TimeDate	Подраздел 8 добавления	БУ	не личные	не личные	согласие не требуется	обязательно
HighResolutionTotalVehicleDistance	ISO 16844-7	БУ	не личные	не личные	согласие не требуется	обязательно
HighResolutionTripDistance	ISO 16844-7	БУ	не личные	не личные	согласие не требуется	обязательно
ServiceComponentIdentification	ISO 16844-7	БУ	не личные	не личные	согласие не требуется	обязательно
ServiceDelayCalendarTimeBased	ISO 16844-7	БУ	не личные	не личные	согласие не требуется	обязательно
Driver1Identification	ISO 16844-7	Карточка водителя	личные	Н/П	согласие водителя	обязательно
Driver2Identification	ISO 16844-7	Карточка водителя	Н/П	личные	согласие второго водителя	обязательно
NextCalibrationDate	Подраздел 8 добавления	БУ	не личные	не личные	согласие не требуется	обязательно
Driver1ContinuousDrivingTime	ISO 16844-7	БУ	личные	Н/П	согласие водителя	обязательно
Driver2ContinuousDrivingTime	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	обязательно
Driver1CumulativeBreakTime	ISO 16844-7	БУ	личные	Н/П	согласие водителя	обязательно
Driver2CumulativeBreakTime	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	обязательно
Driver1CurrentDurationOfSelectedActivity	ISO 16844-7	БУ	личные	Н/П	согласие водителя	обязательно
Driver2CurrentDurationOfSelectedActivity	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	обязательно
SpeedAuthorised	Подраздел 8	БУ	не личные	не личные	согласие не требуется	обязательно
TachographCardSlot1	ISO 16844-7	БУ	не личные	Н/П	согласие не требуется	обязательно
TachographCardSlot2	ISO 16844-7	БУ	Н/П	не личные	согласие не требуется	обязательно
Driver1Name	ISO 16844-7	Карточка водителя	личные	Н/П	согласие водителя	обязательно
Driver2Name	ISO 16844-7	Карточка водителя	Н/П	личные	согласие второго водителя	обязательно
OutOfScopeCondition	ISO 16844-7	БУ	не личные	не личные	согласие не требуется	обязательно
ModeOfOperation	ISO 16844-7	БУ	не личные	не личные	согласие не требуется	обязательно
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	ISO 16844-7	БУ	личные	Н/П	согласие водителя	обязательно
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	обязательно
EngineSpeed	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
RegisteringMemberState	Подраздел 8	БУ	не личные	не личные	согласие не требуется	обязательно
VehicleRegistrationNumber	Подраздел 8	БУ	не личные	не личные	согласие не требуется	обязательно
Driver1EndOfLastDailyRestPeriod	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2EndOfLastDailyRestPeriod	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1EndOfLastWeeklyRestPeriod	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2EndOfLastWeeklyRestPeriod	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1EndOfSecondLastWeeklyRestPeriod	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2EndOfSecondLastWeeklyRestPeriod	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно

Название данных	Формат данных	Источник	Классификация данных (личные/не личные)		Согласие на доступность данных	Доступность
			водитель	второй водитель		
Driver1TimeLastLoadUnloadOperation	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2TimeLastLoadUnloadOperation	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1CurrentDailyDrivingTime	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2CurrentDailyDrivingTime	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1CurrentWeeklyDrivingTime	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2CurrentWeeklyDrivingTime	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1TimeLeftUntilNewDailyRestPeriod	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2TimeLeftUntilNewDailyRestPeriod	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1CardExpiryDate	ISO 16844-7	Карточка водителя	личные	Н/П	согласие водителя	факультативно
Driver2CardExpiryDate	ISO 16844-7	Карточка водителя	Н/П	личные	согласие второго водителя	факультативно
Driver1CardNextMandatoryDownloadDate	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2CardNextMandatoryDownloadDate	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
TachographNextMandatoryDownloadDate	ISO 16844-7	БУ	не личные	не личные	согласие не требуется	факультативно
Driver1TimeLeftUntilNew WeeklyRestPeriod	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2TimeLeftUntilNew WeeklyRestPeriod	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1NumberOfTimes9hDailyDrivingTimes Exceeded	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2NumberOfTimes9hDailyDrivingTimes Exceeded	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1CumulativeUninterruptedRestTime	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2CumulativeUninterruptedRestTime	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1MinimumDailyRest	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2MinimumDailyRest	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1MinimumWeeklyRest	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2MinimumWeeklyRest	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1MaximumDailyPeriod	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2MaximumDailyPeriod	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1MaximumDailyDrivingTime	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2MaximumDailyDrivingTime	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1NumberOfUsedReducedDailyRestPeriods	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2NumberOfUsedReducedDailyRestPeriods	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
Driver1RemainingCurrentDrivingTime	ISO 16844-7	БУ	личные	Н/П	согласие водителя	факультативно
Driver2RemainingCurrentDrivingTime	ISO 16844-7	БУ	Н/П	личные	согласие второго водителя	факультативно
VehiclePosition	Подраздел 8 добавления	БУ	личные	личные	согласие водителя и второго водителя	обязательно
ByDefaultLoadType	Подраздел 8 добавления	БУ	личные	личные	согласие водителя и второго водителя	обязательно

В Правилах уточняется, что тахографы транспортных средств могут быть оснащены стандартизированными интерфейсами, позволяющими использовать данные, записанные или выдаваемые тахографами, в оперативном режиме на внешних устройствах, при соблюдении следующих условий:

- а) — интерфейс не влияет на подлинность и целостность данных тахографа;

б) — интерфейс соответствует подробным положениям статьи 11 регламента **настоящего подраздела**;

е) — внешнее устройство, соединенное с интерфейсом, имеет доступ к личным данным, включая данные геопозиционирования, только при условии получения поддающегося проверке согласия водителя, с которым связаны эти данные.

2. Сфера охвата

Область применения настоящего приложения **подраздела** пояснить, как приложения на внешних устройствах через подключение Bluetooth® могут получать данные (данные) тахографа.

Данные, доступные через этот интерфейс, описаны в приложении 1 к настоящему документу. Данный интерфейс не препятствует реализации других интерфейсов (например, через шину CAN) для передачи данных БУ в другие процессоры транспортного средства.

— В данном подразделе добавления указываются:

— *Данные*, передаваемые через интерфейс ИТС

— Характеристики Bluetooth® для передачи данных

— Процедуры запроса и загрузки и последовательность операций

— Механизм соединения тахографа и внешнего устройства

— Механизм предоставления согласия водителя

— В качестве пояснения, в настоящем приложении не указывается следующее:

— сбор данных и управление ими в БУ (это рассматривается в других частях регламента **настоящего Соглашения** или является функцией дизайна изделия);

— форма отображения собранных данных в приложениях, установленных на внешнем устройстве;

— положения о безопасности данных сверх того, что обеспечивает Bluetooth® (например, шифрование) в отношении содержания *данных* (которые должны быть указаны в другом месте в рамках Правил [приложение 10 **подраздел 11** Общие механизмы безопасности]);

— протоколы Bluetooth®, используемые интерфейсом ИТС.

2.1 Сокращения, определения и обозначения

В настоящем приложении **подразделе** используются следующие сокращения и определения:

Передача данных — обмен информацией/данными между основным устройством (т. е. тахографом) и внешним устройством через интерфейс ИТС при помощи Bluetooth®.

Данные — Наборы данных в соответствии с определением в приложении 1.

Правила — Регламент (ЕС) № 165/2014 Европейского парламента и Совета от 4 февраля 2014 года о тахографе на автомобильном транспорте, отменяющее Постановление Совета (ЕЭС) № 561/2006 Европейского парламента и Совета о гармонизации некоторых социальных законов, касающихся автомобильного транспорта.

BR — Базовый тариф

РДС — Ускоренная передача данных

ГНСС — Глобальная навигационная спутниковая система

IRK	Ключ разрешения при опознавании
ITS	Интеллектуальная транспортная система
LE	Энергия низкого уровня
PIN	Персональный идентификационный номер
PUC	Персональный код разблокировки
SID	Идентификатор функции
ЭСС	Профиль последовательного порта
SSP	Защищенное простое соединение
TRTP	Параметр запроса передачи данных
TREP	Параметр запроса передачи данных
VU (БУ)	Бортовое устройство

3. Ссылки на регламенты и стандарты

Данное добавление **Данный подраздел** содержит ссылки на все или некоторые части следующих правил и стандартов и использует их в качестве основы. В положениях настоящего приложения **подраздела** указываются конкретные стандарты или конкретные их условия. В случае любого противоречия преимущественную силу имеют положения настоящего приложения **подраздела**.

Регламенты и **стандарты**, на которые даются ссылки в настоящем приложении **подразделе**:

Регламент (ЕС) № 165/2014 Европейского парламента и Совета от 4 февраля 2014 года о тахографах дорожных транспортных средств, отменяющий Регламент Совета (ЕЭС) № 3821/85 о записывающем оборудовании в дорожном транспорте и вносящий поправки в Регламент (ЕС) № 561/2006 Европейского парламента и Совета о гармонизации соответствующего социального законодательства, связанного с дорожным транспортом.

Регламент (ЕС) № 561/2006 Европейского парламента и Совета от 15 марта 2006 года о гармонизации соответствующего социального законодательства, связанного с дорожным транспортом, вносящий поправки в Регламенты Совета (ЕЭС) № 3821/85 и (ЕС) № 2135/98 и отменяющий Регламент Совета (ЕЭС) № 3820/85.

- ISO 16844-4: Дорожные транспортные средства. Системы тахографов. Часть 4: интерфейс CAN
- ISO 16844-7: Транспортные средства дорожные. Системы тахографов. Часть 7: Параметры
- Bluetooth®. Профиль последовательного порта V1.2
- Bluetooth®. Основная версия 4.2
- Протокол NMEA 0183 V4.1

4. Принципы работы интерфейса

4.1 Предварительные условия передачи данных через интерфейс ITS

БУ отвечает за обновление и поддержку данных тахографа, передаваемых через интерфейс ITS, без какого бы то ни было участия в этом процессе со стороны интерфейса ITS. Средства, которыми это достигается, являются внутренними средствами БУ, описанными в других частях регламента **настоящего Соглашения** и не указанными в настоящем приложении **подразделе**.

4.1.1 — Данные, передаваемые через интерфейс ИТС

БУ отвечает за обновление данных, передаваемых через интерфейс ИТС с частотой, определяемой процедурами БУ, без участия интерфейса ИТС. Данные БУ используются в качестве основы наполнения и обновления данных, а средства, которыми это достигается, описываются в других частях Регламента **настоящего Соглашения**, или, если такой спецификации нет, являются функцией дизайна изделия и в настоящем приложении подразделе добавления не обуславливаются.

4.1.2 — Содержание данных

Содержание ~~данных~~ соответствует представленному в приложении 1 настоящего приложения ~~подраздела~~.

4.1.3 — Приложения ИТС

Приложения ИТС используют данные, предоставляемые через интерфейс ИТС, например, для оптимизации управления действиями водителя при условии соблюдения регламента **положений настоящего Соглашения**, обнаружения возможных неисправностей тахографа или использования данных ГНСС. Спецификация приложений в настоящее приложение **настоящий подраздел** не входит.

Договаривающиеся стороны могут устанавливать ограничения на передачу данных приложениями ИТС; эти ограничения не должны влиять на данные, предоставляемые через интерфейс ИТС в соответствии с пунктом 4.1.1. Договаривающиеся стороны соблюдают действующее на их территориях законодательство о защите данных в части, касающейся сбора, хранения, обработки и использования личных данных с использованием ИТС.

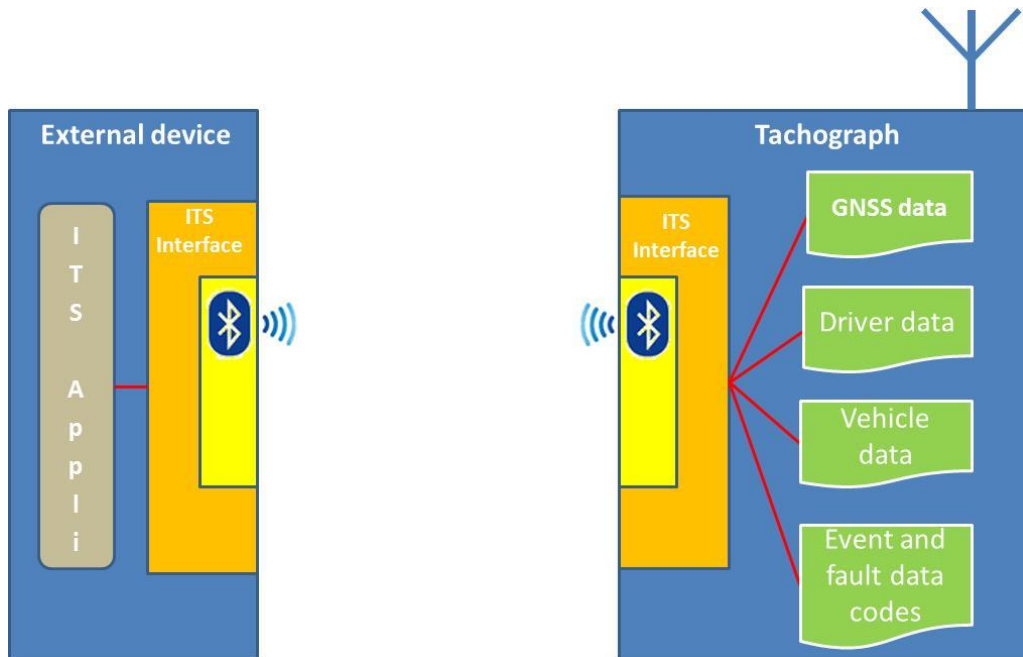
4.2 — Технология связи

Обмен ~~данными~~ через интерфейс ИТС происходит при помощи интерфейса Bluetooth®, совместимость которого обеспечивается через версию 4.2 или новее. Bluetooth® действует в нелицензированном промышленном, научном и медицинском диапазоне частот (ISM) от 2,4 до 2,485 ГГц. Bluetooth® 4.2 обеспечивает усиленные механизмы конфиденциальности и защиты и увеличивает скорость и надежность передачи данных. Для целей настоящей спецификации это рация Bluetooth® 2 го класса, используемая в радиусе до 10 метров. Более подробная информация о Bluetooth® 4.2 опубликована здесь: www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications_ga=1.215147412.2083380574.1435305676).

Передача данных осуществляется с помощью оборудования связи после завершения процесса соединения с санкционированным оборудованием. Поскольку для контроля, когда и куда устройства могут передавать данные, Bluetooth® использует модель ведущего/ведомого, тахограф играет роль ведущего, а внешнее устройство — ведомого.

Когда внешнее устройство впервые оказывается в радиусе действия БУ, может быть инициирован процесс соединения Bluetooth® (см. также приложение 2). Устройства обмениваются своими адресами, названиями и характеристиками и общим секретным ключом, что позволяет им связываться при дальнейших соединениях в будущем. После завершения данного этапа устанавливается доверительный статус применительно к данному внешнему устройству, вследствие чего оно может инициировать запросы на загрузку данных с тахографа. Установка механизмов шифрования, помимо предлагаемых Bluetooth®, не предусматривается. Однако если нужны дополнительные механизмы защиты, они обеспечиваются в соответствии с приложением 10 **подразделом 11 «Общие механизмы безопасности»**.

Общий принцип передачи данных представлен на следующем рисунке.



SPP (профиль последовательного порта) Bluetooth® используется для передачи данных из БУ на внешнее устройство.

4.3 Получение доступа при помощи ПИН-кода

По соображениям безопасности БУ **предусматривает** систему получения доступа по ПИН-коду, отдельно от соединения через Bluetooth. Каждое БУ также способно генерировать ПИН-коды для целей аутентификации, состоящие хотя бы из 4 цифр. Всякий раз, когда внешнее устройство соединяется с БУ, оно должно ввести правильный ПИН-код, прежде чем получит какие-либо данные.

При успешном вводе ПИН-кода устройство вносится в белый список. В белом списке хранится не менее 64 устройств, соединяемых с соответствующим БУ.

Если три раза подряд попытка ввода ПИН-кода не удалась, устройство временно вносится в черный список. Пока оно находится в черном списке, любые новые попытки устройства отклоняются. Если попытка ввода верного ПИН-кода снова оказалась неудачной три раза подряд, период запрета, наложенного на устройство, соответственно увеличивается (см. таблицу 1). При вводе верного ПИН-кода продолжительность запрета и число попыток ввода обнуляются. Рис. 1 в приложении 2 представляет собой диаграмму последовательности действий при попытке ввода ПИН-кода.

Таблица 150

Продолжительность запрета в зависимости от числа неудачных попыток ввода правильного ПИН-кода подряд

<i>Количество последовательных отказов</i>	<i>Продолжительность запрета</i>
3	30 секунд
6	5 минут
9	1 час
12	24 часа
15	Постоянно

Если попытка ввода ПИН-кода оказалась неудачной пятнадцать раз подряд (5 × 3), устройство ИТС вносится в черный список навсегда. Этот запрет на него снимается только при вводе верного кода PUC.

Код PUC состоит из 8 цифр; его предоставляет изготовитель вместе с БУ. Если попытка ввода ПИН-кода оказалась неудачной пятнадцать раз подряд (5 × 3), устройство ИТС вносится в черный список навсегда.

Хотя изготовитель может **предлагать** вариант непосредственной замены ПИН-кода в БУ, код PUC не меняется. Если есть возможность замены ПИН-кода, текущий ПИН-код вводится непосредственно в БУ.

Кроме того, любые устройства, внесенные в белый список, сохраняются там до тех пор, пока их вручную не удалит пользователь (например, через интерфейс пользователя и интерфейс «человек-машина» БУ или другие средства). Таким образом утерянные или похищенные устройства ИТС можно исключить из белого списка. К тому же, устройство ИТС, покидающее радиус связи Bluetooth более чем на 24 часа, автоматически исключается из белого списка БУ и при установлении повторной связи должно будет снова ввести верный ПИН-код.

Формат сообщений между интерфейсом БУ и БУ оставлен на усмотрение изготовителя. Однако изготовитель должен следить за тем, чтобы формат сообщений между устройством ИТС и интерфейсом БУ соблюдался (см. спецификации ASN.1).

Так, любые запросы данных подвергаются соответствующей проверке реквизитов запрашивающего устройства до начала обработки. Рис. 1 в приложении 2 отображает диаграмму последовательности действий при попытке ввода ПИН-кода. Любое устройство, внесенное в черный список, получает автоматический отказ, а устройство, не внесенное ни в черный, ни в белый списки, получает запрос на ПИН-код, который оно должно предоставить, прежде чем снова отправить запрос на данные.

4.4 Формат сообщения

Все сообщения, которыми обмениваются устройство ИТС и БУ, форматируются в соответствии с трехкомпонентной структурой: Заголовок, состоящий из байта адреса приемника (TGT), байта адреса источника (SRC) и в некоторых случаях также байта длины сообщения (LEN).

Поле данных, состоящее из байта идентификатора функции (SID) и меняющегося числа байтов данных (не более 255).

Байт контрольной суммы представляет собой 1-битную сумму по модулю 256 всех байтов сообщения, за исключением самой контрольной суммы.

Порядок байтов в сообщении обратный

Таблица 2-51

Общий формат сообщения

Заголовок			Поле данных				Контрольная сумма	
TGT	SRC	LEN	SID	TRTP	CS	CM	ДАнные	CS
3 байта			Макс. 255 байтов				1 байт	

Заголовок

TGT и SRC: ИД устройств приема (TGT) и источника (SRC) сообщения. ИД интерфейса БУ по умолчанию «4EE». Этот ИД изменению не подлежит. Для первого сообщения сеанса связи устройство ИТС по умолчанию использует ИД «A0». Затем интерфейс БУ присваивает уникальный идентификатор устройству ИТС и передает для дальнейшего обмена сообщениями во время сеанса.

Байт LEN учитывает только часть «DATA» в поле данных (см. таблицу 2), а первые 4 байта остаются неявными.

Интерфейс БУ подтверждает подлинность отправителя сообщения, проводя перекрестную проверку собственного IDList через данные Bluetooth и проверяя устройство ИТС, указанное со своим ИД, которое в настоящий момент находится в радиусе связи Bluetooth.

Поле данных

Помимо SID, поле данных также содержит другие параметры: параметр запроса на передачу данных (TRTP) и байты счетчика.

Если данные, которые необходимо **передать**, слишком длинные **бóльшие по объему** и не помещаются в одно сообщение, они разбиваются на несколько подсообщений. Каждое подсообщение имеет одинаковый заголовок и SID, но содержит 2 байтовый счетчик, счетчик текущего сообщения (СС) и счетчик максимального числа сообщений (СМ), для указания номера подсообщения. Чтобы обеспечить возможность обнаружения ошибок и отмены передачи, принимающее устройство подтверждает получение каждого подсообщения. Принимающее устройство может принять подсообщение, запросить его повторную передачу, выдать отправляющему устройству команду начать передачу заново или отменить ее.

Если СС и СМ не используются, им присваивается значение 0xFF.

Например, такое сообщение

ЗАГОЛОВОК	SID	TRTP	СС	СМ	ДАнные	CS
3 байта	Длиной более 255 байтов					1 байт

Передается в таком виде:

ЗАГОЛОВОК	SID	TRTP	01	n	ДАнные	CS
3 байта	255 байтов					1 байт

ЗАГОЛОВОК	SID	TRTP	02	n	ДАнные	CS
3 байта	255 байтов					1 байт

ЗАГОЛОВОК	SID	TRTP	N	N	ДАнные	CS
3 байта	Макс. 255 байтов					1 байт

В таблице 3 представлены сообщения, которыми могут обмениваться БУ и устройство ИТС. Содержание каждого параметра представлено в шестнадцатеричном виде. Для ясности в таблице СС и СМ не отображаются; см. полный формат выше.

Таблица 3 52 Подробное содержание сообщения

	Заголовок		ДАнные			Контрольная сумма
Сообщение	TGT	SRC	LEN	SID	ДАнные	
RequestPIN	ITSID	EE	00	01	FF	
SendITSID	ITSID	EE	01	02	FF ITSID	
SendPIN	EE	ITSID	04	03	FF 4*ЦЕЛОЕ ЧИСЛО (0..9)	
PairingResult	ITSID	EE	01	04	FF БУЛЕВО ЗНАЧЕНИЕ (Т/Ф)	

	Заголовок		ДАННЫЕ			Контрольная сумма
<i>Сообщение</i>	TGT	SRC	LEN	SID	ДАННЫЕ	
<i>SendPUC</i>	EE	ITSID	08	05	FF	8*ЦЕЛОЕ ЧИСЛО (0..9)
<i>BanLiftingResult</i>	ITSID	EE	01	06	FF	БУЛЕВО ЗНАЧЕНИЕ (Т/Е)
<i>RequestRejected</i>	ITSID	EE	08	07	FF	Время
<i>RequestData</i>						
<i>standardTachData</i>	EE	ITSID	01	08	01	
<i>personalTachData</i>	EE	ITSID	01	08	02	
<i>gnssData</i>	EE	ITSID	01	08	03	
<i>standardEventData</i>	EE	ITSID	01	08	04	
<i>personalEventData</i>	EE	ITSID	01	08	05	
<i>standardFaultData</i>	EE	ITSID	01	08	06	
<i>manufacturerData</i>	EE	ITSID	01	08	07	
<i>RequestAccepted</i>	ITSID	EE	Len	09	TREP	Данные
<i>DataUnavailable</i>						
Данные отсутствуют	ITSID	EE	02	0A	TREP	10
Личные данные не передаются	ITSID	EE	02	0A	TREP	11
<i>Отрицательный ответ</i>						
Общее отклонение запроса	ITSID	EE	02	0B	SID Req	10
Услуга не поддерживается	ITSID	EE	02	0B	SID Req	11
Подфункция не поддерживается	ITSID	EE	02	0B	SID Req	12
Неверная длина сообщения	ITSID	EE	02	0B	SID Req	13
Недопустимые условия или ошибка очередности	ITSID	EE	02	0B	SID Req	22
Запрос вне диапазона	ITSID	EE	02	0B	SID Req	31
Ответ ожидается	ITSID	EE	02	0B	SID Req	78
Несоответствие ITSID	ITSID	EE	02	0B	SID Req	FC
ITSID не найден	ITSID	EE	02	0B	SID Req	FB

RequestPIN (SID 01)

Сообщение выдает интерфейс БУ, если устройство ИТС, не включенное в черный или белый списки, направляет запрос о передаче данных.

SendITSID (SID-02)

Данное сообщение выдает интерфейс БУ, если запрос направляет новое устройство. Это устройство использует ИД по умолчанию «A0», прежде чем ему присваивается уникальный ИД для сеанса передачи данных.

SendPIN (SID-03)

Сообщение выдается устройством ИТС в целях внесения интерфейса БУ в белый список. Содержание данного сообщения 4 ЦЕЛЫХ ЧИСЛА от 0 до 9.

PairingResult (SID-04)

Данное сообщение выдается интерфейсом БУ с целью сообщить устройству ИТС, что переданный ПИН код верный. Содержание данного сообщения BOOLEAN со значением «True», если ПИН код верный, и «False» в противном случае.

SendPUC (SID-05)

Сообщение выдается устройством ИТС в целях внесения интерфейса БУ в черный список. Содержание данного сообщения 8 ЦЕЛЫХ ЧИСЛА от 0 до 9.

BanLiftingResult (SID-06)

Данное сообщение выдается интерфейсом БУ с целью сообщить устройству ИТС, что переданный ПИН код верный. Содержание данного сообщения BOOLEAN со значением «True», если PUC код верный, и «False» в противном случае.

RequestRejected (SID-07)

Данное сообщение выдается интерфейсом БУ как ответ на любое сообщение устройства ИТС из черного списка, кроме «SendPUC». Сообщение содержит оставшееся время, в течение которого устройство ИТС остается в черном списке, в соответствии с форматом последовательности «Time», как указано в приложении 3.

RequestData (SID-08)

Данное сообщение о доступе к данным выдается устройством ИТС. Тип требуемых данных указывается однобайтовым параметром запроса передачи (TRTP). Возможна передача нескольких типов данных:

- standardTachData (TRTP 01): Данные, доступные с тахографа, классифицируемые как неличные.
- personalTachData (TRTP 02): данные, доступные с тахографа, классифицированные как личные.
- gnssData (TRTP 03): Данные ГНСС, всегда личные.
- standardEventData (TRTP 04): Данные регистрируемых событий, классифицируемые как неличные.
- personalEventData (TRTP 05): записанные данные о событиях, классифицируемые как личные.
- standardEventData (TRTP 04): Данные регистрируемых событий, классифицируемые как неличные.
- manufacturerData (TRTP 07): данные, предоставляемые изготовителем.

Более подробную информацию о содержании каждого типа данных см. в приложении 3 настоящего подраздела.

Более подробную информацию о формате и содержании данных ГНСС см. в приложении подраздела 12.

Более подробную информацию о коде данных событий и неисправностей см. в добавлениях IV и IC.

RequestAccepted (SID-09)

Данное сообщение выдается интерфейсом БУ, если принято сообщение устройства ИТС «RequestData». Данное сообщение содержит 1-байтовое значение TRTP, представляющее собой байт TRTP соответствующего сообщения RequestData, и все данные запрошенного типа.

DataUnavailable (SID-0A)

Данное сообщение выдается интерфейсом БУ, если по какой-либо причине запрашиваемых данных нет, чтобы их можно было передать устройству ИТС, включенному в белый список. Сообщение содержит 1-байтовое значение TRTP, представляющее собой TRTP запрашиваемых данных, и 1-байтовый код ошибки, указанный в таблице 3. Существуют следующие коды:

- **Данных нет (10):** Интерфейс БУ по неуказанным причинам не может получить доступ к данным БУ.
- **Личные данные не передаются (11):** Устройство ИТС пытается получить личные данные, обмен которыми не предусмотрен.

NegativeAnswer (SID-0B)

Данные сообщения выдаются интерфейсом БУ, если запрос невозможно выполнить по любой другой причине, не связанной с отсутствием данных. Такие сообщения обычно передаются в результате неверного формата запроса (длина, SID, ITSID...), но не только. TRTP в поле данных содержит SID запроса. Поле данных содержит код, указывающий на причину отрицательного ответа. Существуют следующие коды:

- **Общее отклонение запроса (код: 10)**

Действие не может быть выполнено по причине, не указанной ни ниже, ни в разделе (Ввести номер раздела *DataUnavailable*).

- **Услуга не поддерживается (код: 11)**

Не опознан SID запроса.

- **Подфункция не поддерживается (код: 12)**

Не опознан TRTP запроса. Например, значения могут отсутствовать или быть неприемлемыми.

- **Неверная длина сообщения (код: 13).**

Неверная длина полученного сообщения (несоответствие между байтом LEN и фактической длиной сообщения).

- **Недопустимые условия или ошибка очередности (код: 22).**

Требуемая функция не активирована либо неверная очередность запросов.

- **Запрос вне диапазона (код: 33).**

Значение параметра запроса (поле данных) недействительно.

- **Ожидается ответ (код: 78).**

Запрошенная операция не может быть завершена своевременно; БУ не готов к приему нового запроса.

- **Несоответствие ITSID (код: FB).**

SRC ITSID не соответствует связанному устройству после сравнения с данными по Bluetooth.

- **ITSID не найден (код: FC).**

SRC ITSID не связан ни с каким устройством.

Строки от 1 до 72 (**FormatMessageModule**) кода ASN.1 в приложении 3 указывают формат сообщений, как описано в таблице 3. Более подробная информация о содержании сообщений представлена ниже.

4.5 — Согласие водителя

Все имеющиеся данные классифицируются как стандартные или личные. Личные данные доступны только в том случае, если водитель дал свое согласие, что его личные данные из тахографа могут покинуть сеть транспортного средства и быть переданы приложениям третьих сторон.

Согласие водителя дается при первом вводе соответствующей карточки водителя или мастеркей, в настоящее время неизвестной для бортового устройства, в связи с чем держателю карточки предлагается дать свое согласие на вывод личных данных, связанных с тахографом, через факультативный интерфейс ИТС. (см. также приложение 1С **добавление 1С**, пункт 3.6.2).

Статус согласия (подтверждено/не подтверждено) записывается в блоке памяти тахографа.

Если водителей несколько, то доступ к личным данным через интерфейс ИТС будет открыт только для тех водителей, которые дали свое согласие. Например, если есть два водителя транспортного средства, и если согласие на обмен своими личными данными дал только первый водитель, то данные второго водителя не передаются.

4.6 — Извлечение стандартных данных

Рисунок 3 приложения 2 представляет собой диаграммы последовательности действительного запроса устройства ИТС на доступ к стандартным данным. Если устройство ИТС должным образом внесено в белый список и не запрашивает личные данные, дополнительная проверка не требуется. Диаграммы касаются надлежащей уже проделанной процедуры, представленной на рисунке 2 приложения 2. Их можно приравнять к серому разделу *REQUEST TREATMENT* на рисунке 2.

Среди имеющихся данных стандартными считаются следующие:

- standardTachData (TRTP 01)
- StandardEventData (TRTP 04)
- standardFaultData (TRTP 06)

4.7 — Извлечение личных данных

Рис. 4 в приложении 2 представляет собой диаграмму последовательности действий обработки запроса на личные данные. Как уже указывалось, интерфейс БУ передает личные данные, только если водитель дал явное согласие на эту передачу (см. также 4.5). В противном случае запрос должен быть автоматически отклонен.

Среди имеющихся данных личными считаются следующие:

- personalTachData (TRTP 02)
- gnssData (TRTP 03)
- personalEventData (TRTP 05)
- manufacturerData (TRTP 07)

4.8 ~~Извлечение данных о событиях и неисправностях~~

~~Устройства ИТС способны запрашивать данные о событиях со списком всех непредвиденных событий. Такие данные считаются стандартными или личными; см. приложение 3. Содержание каждого события в соответствии с документацией в приложении 1 настоящего приложения.~~

ПРИЛОЖЕНИЕ 1

- 1) ~~ПЕРЕЧЕНЬ ДАННЫХ, ДОСТУПНЫХ ЧЕРЕЗ ИНТЕРФЕЙС ИТС~~**
- 2) ~~ПОСТОЯННЫЕ ДАННЫЕ ГНСС, ДОСТУПНЫЕ ПРИ УСЛОВИИ СОГЛАСИЯ ВОДИТЕЛЯ~~**

См. подраздел 12 добавления ГНСС

3) КОДЫ СОБЫТИЙ, ДОСТУПНЫХ БЕЗ СОГЛАСИЯ ВОДИТЕЛЯ

Data	Source	Data classification (personal/not personal)
VehicleIdentificationNumber	Vehicle Unit	not personal
CalibrationDate	Vehicle Unit	not personal
TachographVehicleSpeed speed instant t	Vehicle Unit	personal
Driver1WorkingState Selector driver	Vehicle Unit	personal
Driver2WorkingState	Vehicle Unit	personal
DriveRecognize Speed Threshold detected	Vehicle Unit	not personal
Driver1TimeRelatedStates Weekly day time	Driver Card	personal
Driver2TimeRelatedStates	Driver Card	personal
DriverCardDriver1	Vehicle Unit	not personal
DriverCardDriver2	Vehicle unit	not personal
OverSpeed	Vehicle Unit	personal
TimeDate	Vehicle Unit	not personal
HighResolutionTotalVehicleDistance	Vehicle Unit	not personal
ServiceComponentIdentification	Vehicle Unit	not personal
ServiceDelayCalendarTimeBased	Vehicle Unit	not personal
Driver1Identification	Driver Card	personal
Driver2Identification	Driver Card	personal
NextCalibrationDate	Vehicle Unit	not personal
Driver1ContinuousDrivingTime	Driver Card	personal
Driver2ContinuousDrivingTime	Driver Card	personal
Driver1CumulativeBreakTime	Driver Card	personal
Driver2CumulativeBreakTime	Driver Card	personal
Driver1CurrentDurationOfSelectedActivity	Driver Card	personal
Driver2CurrentDurationOfSelectedActivity	Driver Card	personal
SpeedAuthorised	Vehicle Unit	not personal
TachographCardSlot1	Driver Card	not personal
TachographCardSlot2	Driver Card	not personal
Driver1Name	Driver Card	personal
Driver2Name	Driver Card	personal
OutOfScopeCondition	Vehicle Unit	not personal
ModeOfOperation	Vehicle Unit	not personal
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
EngineSpeed	Vehicle Unit	personal
RegisteringMemberState	Vehicle Unit	not personal
VehicleRegistrationNumber	Vehicle Unit	not personal
Driver1EndOfLastDailyRestPeriod	Driver Card	personal
Driver2EndOfLastDailyRestPeriod	Driver Card	personal
Driver1EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver1EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver1CurrentDailyDrivingTime	Driver Card	personal
Driver2CurrentDailyDrivingTime	Driver Card	personal
Driver1CurrentWeeklyDrivingTime	Driver Card	personal
Driver2CurrentWeeklyDrivingTime	Driver Card	personal
Driver1TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver1CardExpiryDate	Driver Card	personal
Driver2CardExpiryDate	Driver Card	personal
Driver1CardNextMandatoryDownloadDate	Driver Card	personal
Driver2CardNextMandatoryDownloadDate	Driver Card	personal
TachographNextMandatoryDownloadDate	Vehicle Unit	not personal
Driver1TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Driver Card	personal
Driver2NumberOfTimes9hDailyDrivingTimesExceeded	Driver Card	personal
Driver1CumulativeUninterruptedRestTime	Driver Card	personal
Driver2CumulativeUninterruptedRestTime	Driver Card	personal
Driver1MinimumDailyRest	Driver Card	personal
Driver2MinimumDailyRest	Driver Card	personal
Driver1MinimumWeeklyRest	Driver Card	personal
Driver2MinimumWeeklyRest	Driver Card	personal
Driver1MaximumDailyPeriod	Driver Card	personal
Driver2MaximumDailyPeriod	Driver Card	personal
Driver1MaximumDailyDrivingTime	Driver Card	personal
Driver2MaximumDailyDrivingTime	Driver Card	personal
Driver1NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver2NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver1RemainingCurrentDrivingTime	Driver Card	personal
Driver2RemainingCurrentDrivingTime	Driver Card	personal
GnssPosition	Vehicle Unit	personal

<i>Событие</i>	<i>Правила хранения</i>	<i>Данные по каждому событию, подлежащему регистрации</i>
Ввод недействительной карточки	—	—дата и время события —тип карточки (карточек), номер, государство-эмитент Договаривающаяся сторона и поколение карточки, создавшей событие —число аналогичных событий за указанный день
Несовместимость карточек	—10 самых последних событий	—дата и время начала события —дата и время завершения события —тип карточки (карточек), номер, государство-эмитент Договаривающаяся сторона — эмитент и поколение карточки, создавшей событие несовместимости
Неправильное завершение последнего сеанса использования карточки	—10 самых последних событий	—дата и время ввода карточки —тип карточки (карточек), номер, государство-эмитент Договаривающаяся сторона — эмитент и поколение карточки —последняя дата сеанса использования, записанная на карточке: —дата и время ввода карточки —VRN, Договаривающаяся сторона регистрации и генерирование БУ
Прекращение электронитания (2)	—самое длительное событие за каждый из 10 последних дней —5 самых длительных событий за последние 365 дней	—дата и время начала события —дата и время завершения события —тип карточки (карточек), номер и государство-член, выдавшее Договаривающаяся сторона , выдавшая любую карточку, вставленную в начале и/или конце события, и ее поколение —число аналогичных событий за указанный день
Ошибка связи со средством удаленной связи	—самое длительное событие за каждый из 10 последних дней —5 самых длительных событий за последние 365 дней	—дата и время начала события —дата и время завершения события —тип карточки (карточек), номер и государство-член, выдавшее Договаривающаяся сторона , выдавшая любую карточку, вставленную в начале и/или конце события, и ее поколение —число аналогичных событий за указанный день

<i>Событие</i>	<i>Правила хранения</i>	<i>Данные по каждому событию, подлежащему регистрации</i>
Отсутствие информации о местоположении из приемника ГНСС	—самое длительное событие за каждый из 10 последних дней —5 самых длительных событий за последние 365 дней	—дата и время начала события —дата и время завершения события —тип карточки (карточек), номер и государство-член, выдавшее Договаривающая сторона, выдавшая любую карточку, вставленную в начале и/или конце события, и ее поколение —число аналогичных событий за указанный день
Ошибка связи со средством удаленной связи	самое длительное событие за каждый из 10 последних дней 5 самых длительных событий за последние 365 дней	—дата и время начала события —дата и время завершения события —тип карточки (карточек), номер и государство-член, выдавшее Договаривающая сторона, выдавшая любую карточку, вставленную в начале и/или конце события, и ее поколение —число аналогичных событий за указанный день
Ошибкачные данные о движении	—самое длительное событие за каждый из 10 последних дней —5 самых длительных событий за последние 365 дней	—дата и время начала события —дата и время завершения события —тип карточки (карточек), номер и государство-член, выдавшее Договаривающая сторона, выдавшая любую карточку, вставленную в начале и/или конце события, и ее поколение —число аналогичных событий за указанный день
Противоречивые данные о движении транспортного средства	—самое длительное событие за каждый из 10 последних дней —5 самых длительных событий за последние 365 дней	—дата и время начала события —дата и время завершения события —тип карточки (карточек), номер и государство-член, выдавшее Договаривающая сторона, выдавшая любую карточку, вставленную в начале и/или конце события, и ее поколение —число аналогичных событий за указанный день
Попытка нарушения системы защиты	—10 самых последних событий по типу события	—дата и время начала события —дата и время завершения события (в случае применимости) —тип карточки (карточек), номер и государство-член, выдавшее Договаривающая сторона, выдавшая любую карточку, вставленную в начале и/или конце события, и ее поколение —тип события

<i>Событие</i>	<i>Правила хранения</i>	<i>Данные по каждому событию, подлежащему регистрации</i>
Нестыковка во времени	—самое длительное событие за каждый из 10 последних дней —5 самых длительных событий за последние 365 дней	—записывающее оборудование контрольное устройство дата и время —Дата и время ГНСС —тип карточки (карточек), номер и государство-член, выдавшее Договаривающаяся сторона, выдавшая любую карточку, вставленную в начале и/или конце события, и ее поколения —число аналогичных событий за указанный день

4) КОДЫ СОБЫТИЙ, ДОСТУПНЫХ БЕЗ СОГЛАСИЯ ВОДИТЕЛЯ

<i>Событие</i>	<i>Правила хранения</i>	<i>Данные по каждому событию, подлежащему регистрации</i>
Управление без соответствующей карточки	—самое длительное событие за каждый из 10 последних дней —5 самых длительных событий за последние 365 дней	—дата и время начала события —дата и время завершения события —тип карточки (карточек), номер и государство-член, выдавшее Договаривающаяся сторона, выдавшая любую карточку, вставленную в начале и/или конце события, и ее поколение —число аналогичных событий за указанный день
Ввод карточки во время управления	—самое длительное событие за каждый из 10 последних дней	—дата и время события —тип карточки (карточек), номер, государство-член, выдавшее Договаривающаяся сторона, выдавшая карточку, и ее поколение —число аналогичных событий за указанный день
Превышение скорости	—наиболее серьезное событие за последние 10 дней (т. е. случай регистрации самой высокой средней скорости) —5 самых длительных событий за последние 365 дней —первое событие, наступившее после последней калибровки	—дата и время начала события —дата и время завершения события —максимальная скорость, измеренная во время события —среднеарифметическая скорость, измеренная во время события —тип карточки (карточек), номер, государство-член, выдавшее Договаривающаяся сторона, выдавшая и поколение карточки, создавшей событие (в случае применимости) —число аналогичных событий за указанный день

5) КОДЫ ДАННЫХ О НЕИСПРАВНОСТЯХ, ДОСТУПНЫХ БЕЗ СОГЛАСИЯ ВОДИТЕЛЯ

<i>Неисправность</i>	<i>Правила хранения</i>	<i>Данные по каждой неисправности, подлежащие регистрации</i>
Неисправность карточки	—10 самых последних неисправностей карточки водителя	—дата и время начала неисправности —дата и время завершения неисправности —тип карточки (карточек), номер, государство-член, выдавшее Договаривающаяся сторона, выдавшая карточку, и ее поколение
Неисправность контрольного устройства	—10 самых последних неисправностей по типу события —первая неисправность после ее последней калибровки.	—дата и время начала неисправности —дата и время завершения неисправности —тип неисправности —тип карточки (карточек), номер и государство-член, выдавшее Договаривающаяся сторона, выдавшая любую карточку, вставленную в начале и/или конце неисправности, и ее поколение

Данное уведомление отображается в случае возникновения любых из перечисленных ниже неисправностей, за исключением режима калибровки:

- внутренние неполадки в БУ;
- неисправность принтера;
- неисправность дисплея;
- ошибка при загрузке;
- неисправность датчика;
- неисправность приемника ГНСС или внешнего устройства ГНСС;
- неисправность средства удаленной связи;
- **неисправность интерфейса ИТС (в случае применимости).**

6) СОБЫТИЯ И НЕИСПРАВНОСТИ, СВЯЗАННЫЕ С КОНКРЕТНЫМ ИЗГОТОВИТЕЛЕМ, БЕЗ СОГЛАСИЯ ВОДИТЕЛЯ

<i>Событие или неисправность</i>	<i>Правила хранения</i>	<i>Данные по каждому событию, подлежащие регистрации</i>
Определяется изготовителем	Определяется изготовителем	Определяется изготовителем

ПРИЛОЖЕНИЕ 2

ДИАГРАММЫ ПОСЛЕДОВАТЕЛЬНОСТИ ДЕЙСТВИЙ В СЛУЧАЕ ОБМЕНА СООБЩЕНИЯМИ С УСТРОЙСТВОМ ИТС

Рис. 1-18

Диаграмма последовательности действий в случае попытки ввода ПИН-кода

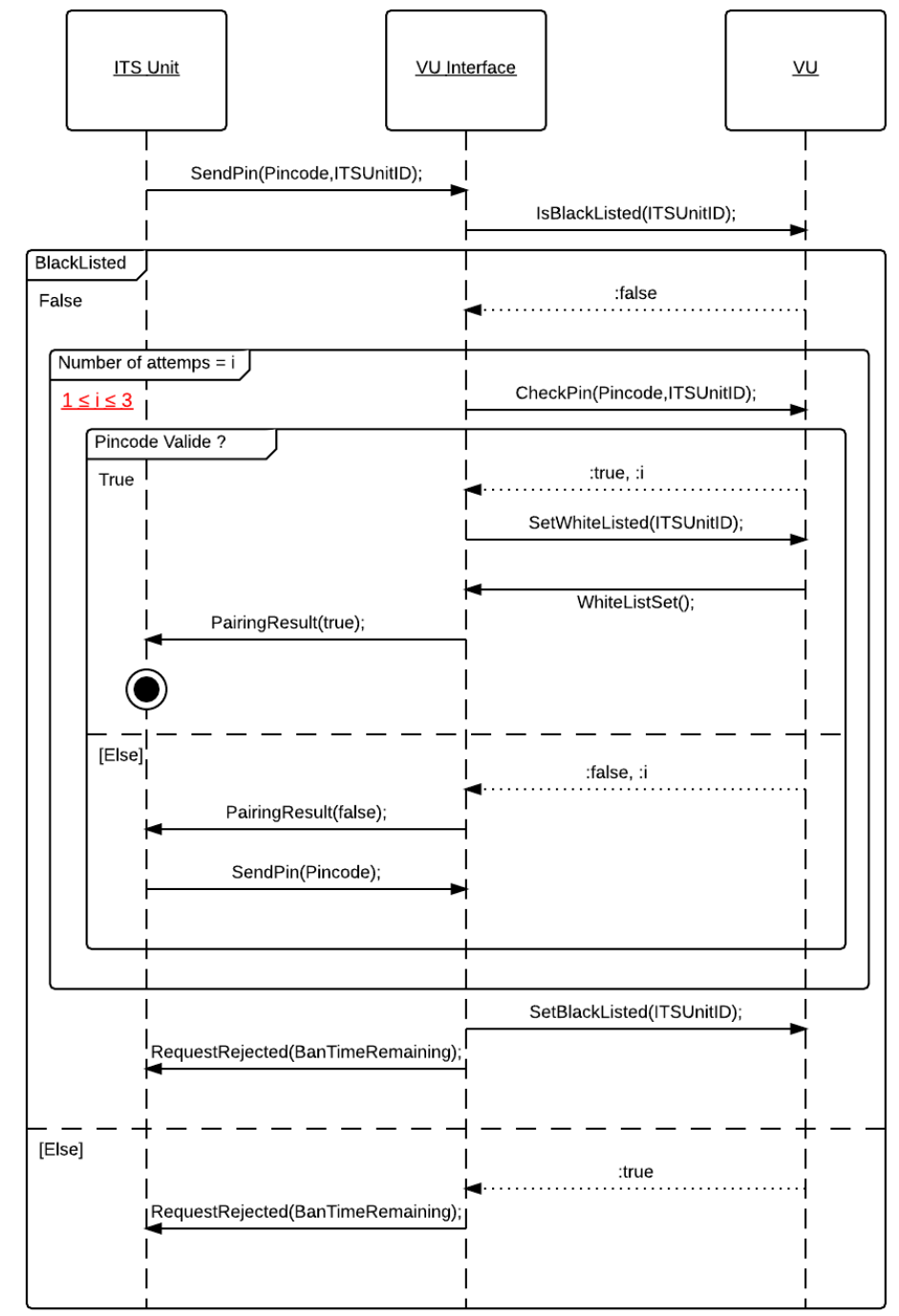


Рис. 2-19
Диаграмма последовательности действий в случае проверки полномочий устройства ИТС

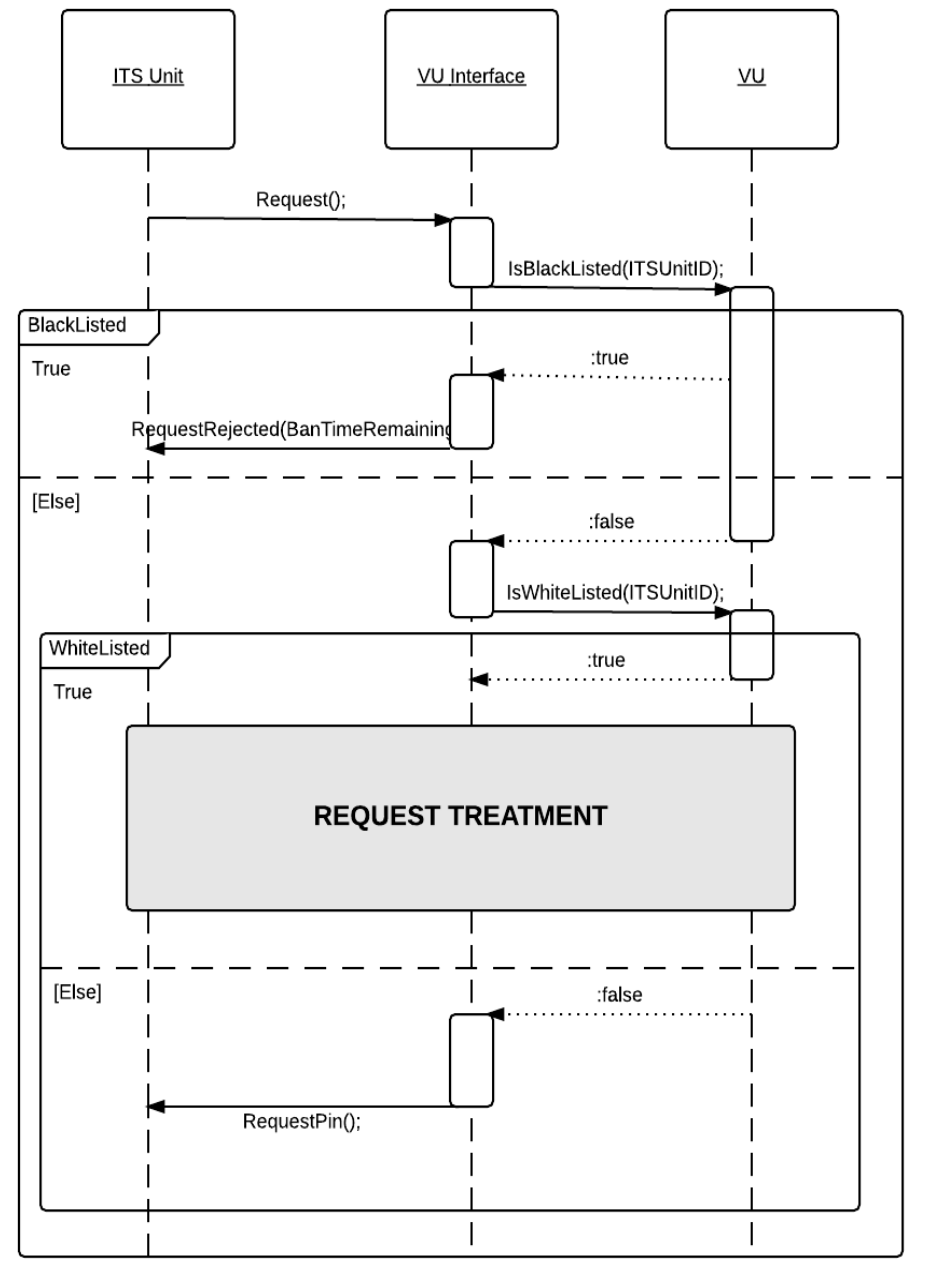


Рис. 3 20

Диаграмма последовательности действий в случае обработки запроса на данные, классифицируемые как неличные (после ввода правильного ПИН-кода)

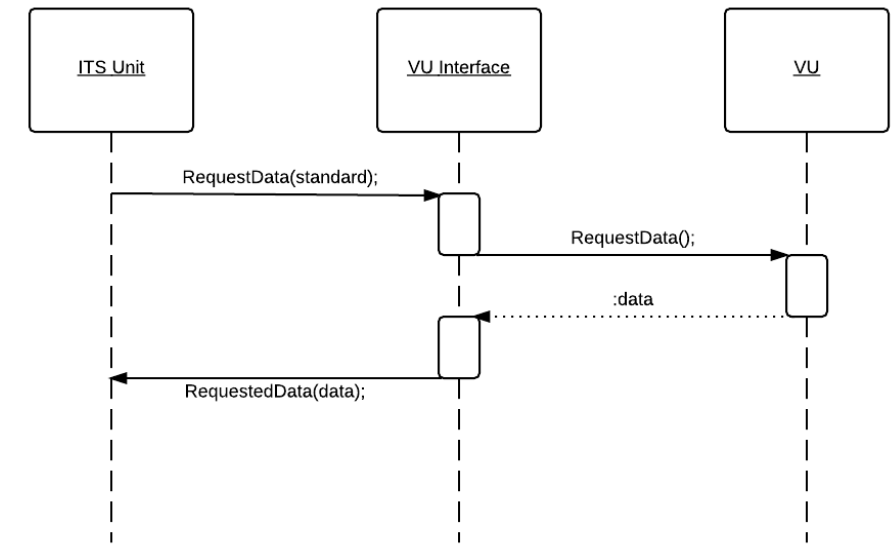


Рис. 4 21

Диаграмма последовательности действий в случае обработки запроса на данные, классифицируемые как не личные (после ввода правильного ПИН-кода)

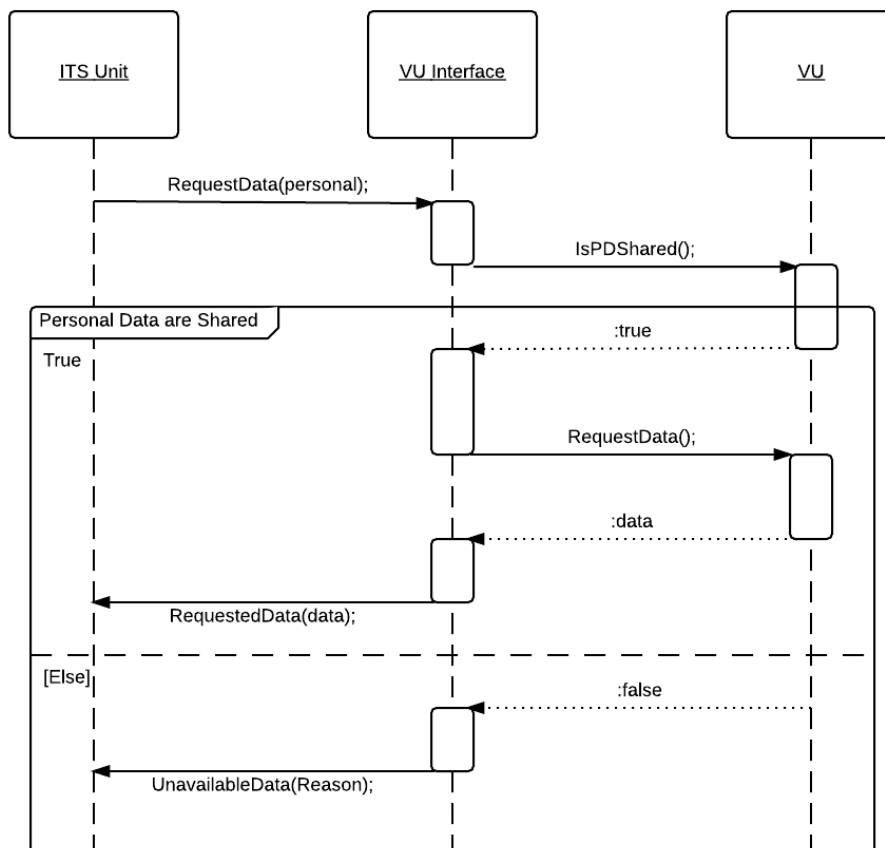
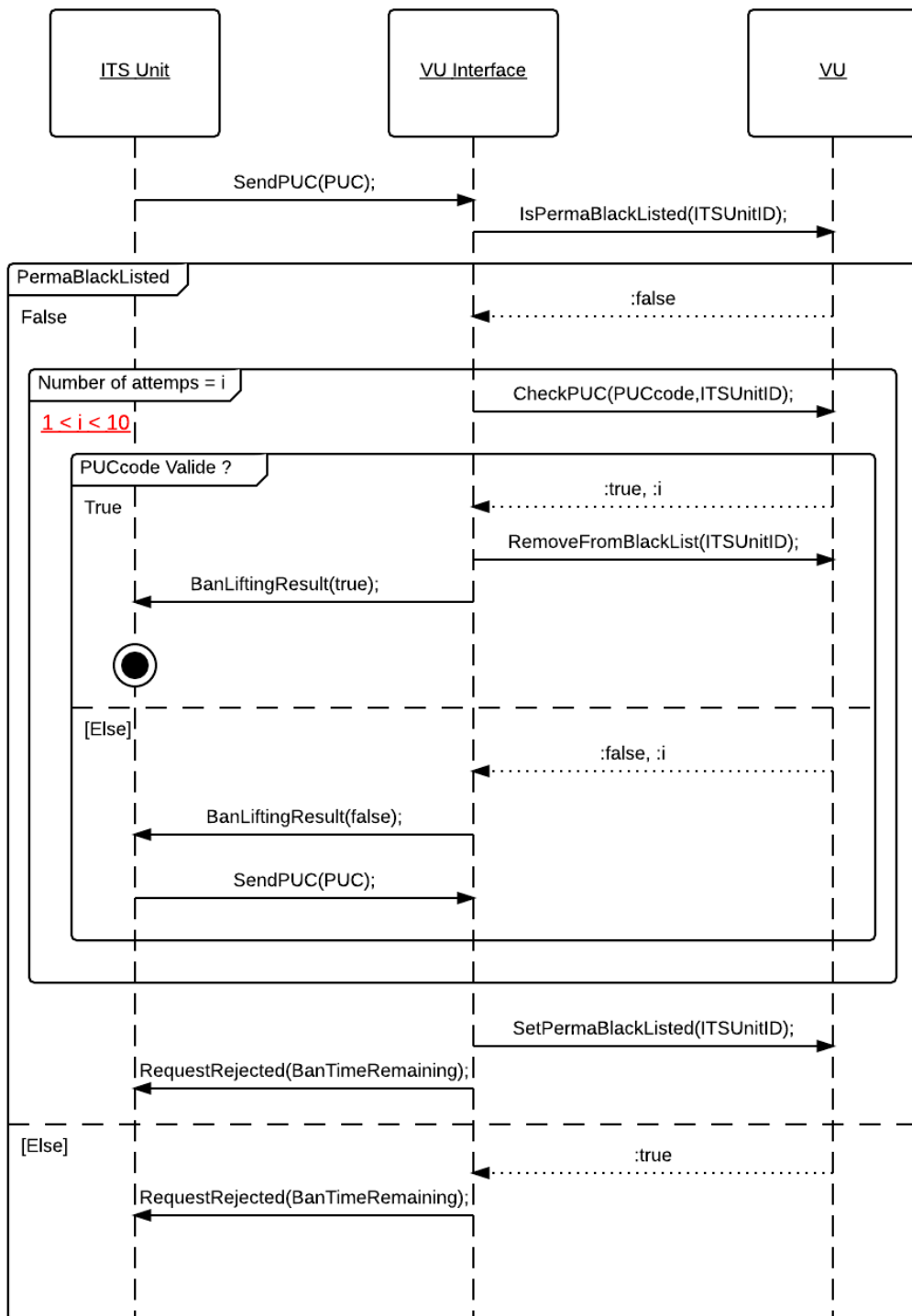


Рис. 5-22
Диаграмма последовательности действий в случае попытки подтверждения PUC кода



ПРИЛОЖЕНИЕ 3

SPÉCIFICATIONS ASN.1

~~FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN~~

~~EXPORTS ;~~

~~IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult FROM PINPUCDataFieldsModule
RequestAccepted, RequestData, DataUnavailable FROM
RequestDataFieldsModule
SendITSID, NegativeAnswer FROM OtherDataFieldsModule ;~~

```
-----
CompleteMessage ::= SEQUENCE {
    header Header,
    data DataField,
    checksum Checksum
}
-----
```

~~-----
HEADER TYPES
-----~~

```
-----
Header ::= SEQUENCE {
    tgt IDList,
    src IDList,
    len BIT STRING (1..255)
}
-----
```

```
-----
vuID BIT STRING ::= 'EE'H
IDList ::= CHOICE {
    vu BIT STRING (vuID),
    itsUnits SEQUENCE OF BIT STRING,
        -- Default hex Value:A0, redefined after first message exchange --
        -- Each ID will be linked to the Bluetooth ID of the device --
    ...
}
-----
```

~~-----
DATAFIELDS TYPES
-----~~

```
-----
DataField ::= SEQUENCE {
    sid BIT STRING,
    PDT BIT STRING,
    subMBytes SubMessageBytes,
    dataField Content,
    ...
}
-----
```

```
-----
SubMessageBytes ::= SEQUENCE {
    currentSubM BIT STRING,
    totalSubM BIT STRING
}
-----
```

```
-----
Content ::= CHOICE {
    requestPIN RequestPIN,
    sendITSID SendITSID,
    sendPin SendPIN,
    pairRsIt PairingResult,
    sendPUC SendPUC,
}
-----
```

```
banlift BanLiftingResult,  
requestRejected RequestRejected,  
requestData RequestData,  
requestOK RequestAccepted,  
dataUnavailable DataUnavailable,  
negAns NegativeAnswer
```

```
}
```

```
-----  
CHECKSUM TYPES  
-----
```

```
Checksum ::= SEQUENCE{
```

```
SHA2 checksum
```

```
}
```

```
END
```

```

PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult ;
IMPORTS ;
-----
-----Utils-----
-----
-----
PUC ::= SEQUENCE (SIZE(8)) OF
INTEGER (SIZE(0..9))
-----
PIN ::= SEQUENCE (SIZE(4)) OF
INTEGER (SIZE(0..9))
-----
-----
-----Messages From ITS Unit-----
-----
SendPIN {PIN:pin} ::= SEQUENCE {
sid BIT STRING ('03'H),
pin PIN (pin)
}
-----
SendPUC {PUC:puc} ::= SEQUENCE {
sid BIT STRING ('05'H),
puc PUC (puc)
}
-----
-----Messages From VU-----
-----
PairingResult ::= SEQUENCE{
sid BIT STRING ('04'H),
result BOOLEAN
}
-----
RequestPIN {MType:receivedRequest} ::= SEQUENCE{
sid BIT STRING ('01'H)
}
-----
RequestRejected ::= SEQUENCE{
sid BIT STRING ('07'H),
banTimeRemaining GeneralizedTime, PermaBan == 1k years }
-----
BanLiftingResult ::= SEQUENCE{
sid BIT STRING ('06'H),
result BOOLEAN
}
-----
END

```

```

RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS RequestAccepted, RequestData, DataUnavailable ;
IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule ;

-----
----- From ITS Unit -----
-----
RequestData ::= SEQUENCE{
sid BIT STRING ('08'H),
requestedData DataTypeCode,
...
}

----- From VU -----
-----
RequestAccepted ::= SEQUENCE{
sid BIT STRING ('09'H),
trtp DataTypeCode,
dataSheet CHOICE{
standardData StandardTachDataContent,
personalData PersonalTachDataContent,
gnss GNSSDataContent,
standardEvent StandardEventContent,
personalEvent PersonalEventContent,
standardFault StandardFaultContent,
manufacturerdata ManufacturerDataContent,
...
}
}

DataTypeCode ::= CHOICE{
standardTachData BIT STRING ('01'H),
personalTachData BIT STRING ('02'H),
gnssData BIT STRING ('03'H),
standardEventData BIT STRING ('04'H),
personalEventData BIT STRING ('05'H),
standardFaultData BIT STRING ('06'H),
manufacturerData BIT STRING ('07'H),
...
}

DataUnavailable ::= SEQUENCE{
sid BIT STRING ('0A'H),
trtp DataTypeCode,
reason UnavailableDataCodes
}

UnavailableDataCodes ::= CHOICE{
noDataAvailable BIT STRING ('10'H),
personalDataNotShared BIT STRING ('11'H),
...
}

----- Complete Tachograph Data -----
-----
The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document-----

Time ::= SEQUENCE{
seconds INTEGER (0..59.75), increment: 0.25s
}

```

```

minutes INTEGER (0..59), increment: 1min
hours INTEGER (0..23), increment: 1h
day INTEGER (0.25.. 31.75), increment: 0.25d
month INTEGER (1..12), increment: 1month
year INTEGER (1985..2235), increment: 1year
locMinOffset INTEGER (-59..59), increment: 1min
locHourOffset INTEGER (-23..23) increment: 1h
 }

Date ::= SEQUENCE{
 month INTEGER (1..12), increment: 1month
 day INTEGER (0.25.. 31.75), increment: 0.25d
 year INTEGER (1985..2235) increment: 1year
 }
DriverName ::=SEQUENCE{
 codePageSurname UTF8String, See ISO/CEI 8859
 surname UTF8String,
 codePageFirstname UTF8String, See ISO/CEI 8859
 firstname UTF8String,
 }

-----
Message Content
-----
-----
StandardTachDataContent ::= SEQUENCE{
 trtp DataTypeCode (DataTypeCode.&standardTachData),
 personal BOOLEAN (FALSE),
 data StandardTachyDataSheet,
 }
PersonalTachDataContent ::= SEQUENCE{
 trtp DataTypeCode (DataTypeCode.&personalTachData),
 personal BOOLEAN (TRUE),
 data PersonalTachyDataSheet
 }
GNSSDataContent ::= SEQUENCE{
 trtp DataTypeCode (DataTypeCode.&gnssData),
 personal BOOLEAN (TRUE),
 data GNSSDataSheet
 }
StandardEventContent ::= SEQUENCE{
 trtp DataTypeCode (DataTypeCode.&standardEventData),
 personal BOOLEAN (FALSE),
 data StandardEventDataSheet
 }
PersonalEventContent ::= SEQUENCE{
 trtp DataTypeCode (DataTypeCode.&personalEventData),
 personal BOOLEAN (TRUE),
 data PersonalEventDataSheet
 }
StandardFaultContent ::= SEQUENCE{
 trtp DataTypeCode (DataTypeCode.&standardFaultData),
 personal BOOLEAN (FALSE),
 data StandardFault

```

```

}
}
ManufacturerDataContent ::= SEQUENCE{
  trtp_DataTypeCode (DataTypeCode.&manufacturerData),
  personal BOOLEAN (TRUE),
  ...
}
}
-----
DATA SHEETS
-----
Data sheet format follows ISO 16844-7.
StandardTachyDataSheet ::= SEQUENCE{
  vin UTF8String (SIZE(17)),
  calibrationDate Date,
  driveRecognize INTEGER (2 UNION 12),
  driverCardDriver1 INTEGER (2 UNION 12),
  driverCardDriver2 INTEGER (2 UNION 12),
  timeDate Time,
  highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment: 5m--
  serviceComponentIdentification INTEGER (0..255),
  serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week--
  nextCalibrationDate Date,
  speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
  tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
  tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
  outOfScopeCondition INTEGER(2 UNION 12),
  modeOfOperation INTEGER (0..4...), --Maximum 250--
  registeringMemberState UTF8String, vehicleRegistrationNumber SEQUENCE {
    codePageVRN INTEGER (0..255),
    vrn OCTET STRING (SIZE(13)),
  },
  tachographNextMandatoryDownloadDate Date,
  ...
}
PersonalTachyDataSheet ::= SEQUENCE{
  tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
  driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002 UNION
1012...),
  driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002 UNION
1012...),
  driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION 1002
UNION
1012 UNION 1102 UNION 1112 UNION 10002 UNION 10012 UNION
10102 UNION 10112 UNION 11002 UNION 11012...),
  driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION 1002
UNION
1012 UNION 1102 UNION 1112 UNION 10002 UNION 10012 UNION
10102 UNION 10112 UNION 11002 UNION 11012...),
  overSpeed INTEGER (2 UNION 12),
  driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS FROM TACHO
REGULATION--
  driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS FROM TACHO
REGULATION--
  driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
  driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--

```

```

----- driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --increment:
1min--
----- driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --increment:
1min--
----- driver1Name DriverName,
----- driver2Name DriverName,
----- driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255), --
increment: 1min--
----- driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255), --
increment: 1min--
----- engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
----- driver1EndOfLastDailyRestPeriod Time,
----- driver2EndOfLastDailyRestPeriod Time,
----- driver1EndOfLastWeeklyRestPeriod Time,
----- driver2EndOfLastWeeklyRestPeriod Time,
----- driver1EndOfSecondLastWeeklyRestPeriod Time,
----- driver2EndOfSecondLastWeeklyRestPeriod Time,
----- driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min--
----- driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min--
----- driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment: 1min--
----- driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment: 1min--
----- driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --increment: 1min--
-
----- driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --increment: 1min--
-
----- driver1CardExpiryDate Date,
----- driver2CardExpiryDate Date,
----- driver1CardNextMandatoryDownloadDate Date,
----- driver2CardNextMandatoryDownloadDate Date,
----- driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --increment:
1min--
----- driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --increment:
1min--
----- driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
----- driver2NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
----- driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --increment: 1min--
-
----- driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --increment: 1min--
-
----- driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
----- driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
----- driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
----- driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
----- driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
----- driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
----- driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
----- driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
----- driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
----- driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
----- driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment: 1min--
----- driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment: 1min--
----- ...
----- }
----- GNSSDataSheet ::= SEQUENCE {
----- gnssPosition GeoCoordinates
----- --See Appendix 1 for definition of GeoCoordinates--
----- }
-----
----- StandardEventDataSheet ::= SEQUENCE{

```

```

events SEQUENCE OF StandardEvent
}
PersonalEventDataSheet ::= SEQUENCE{
events SEQUENCE OF PersonalEvent
}
END
EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ALL ;
IMPORTS NationAlpha FROM Annex Appendix1 ; -- See Annex Appendix 1 for more
information about NationAlpha
SecurityBreachEvent ::= SEQUENCE{
See Appendix 1B for more information
}
RecordingEquipmentFaultType ::= SEQUENCE{
See Appendix 1B for more information
}
StandardEvent ::= CHOICE{
insertionInvalidCard InsertionOfANonValidCard,
cardConflict CardConflict,
timeOverlap TimeOverlap,
previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
overSpeeding OverSpeeding,
powerSupplyInterruption PowerSupplyInterruption,
comErrorWithRemoteFacility
CommunicationErrorWithTheRemoteCommunicationFacility,
absenceGNSSPosition AbsenceOfPositionInformationFromGNSSReceiver,
positionDataError PositionDataError,
motionDataError MotionDataError,
vehicleMotionConflict VehicleMotionConflict,
securityBreachAttempt SecurityBreachAttempt,
timeConflict TimeConflict,
...
}
PersonalEvent ::= CHOICE{
lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
cardInsertionWhileDriving CardInsertionWhileDriving,
overSpeeding OverSpeeding,
...
}
StandardFault ::= CHOICE{
cardFault CardFault,
recordingEquipmentFault RecordingEquipmentFault,
...
}
-----
EVENTS LIST
-----
InsertionOfANonValidCard ::= SEQUENCE{
beginDate GeneralizedTime,
endDate GeneralizedTime,
carsdType SEQUENCE OF UTF8String,
cardsNumber SEQUENCE OF INTEGER,

```



```

_____ issuingMemberState SEQUENCE OF NationAlpha,
_____ cardsGeneration SEQUENCE OF INTEGER
_____ }
_____
_____ CardConflict ::= SEQUENCE{
_____ beginDate GeneralizedTime,
_____ endDate GeneralizedTime,
_____ carsdType SEQUENCE OF UTF8String,
_____ cardsNumber SEQUENCE OF INTEGER,
_____ issuingMemberState SEQUENCE OF NationAlpha,
_____ cardsGeneration SEQUENCE OF INTEGER
_____ }
_____
_____ TimeOverlap ::=SEQUENCE{
_____ beginDate GeneralizedTime,
_____ endDate GeneralizedTime,
_____ carsdType SEQUENCE OF UTF8String,
_____ cardsNumber SEQUENCE OF INTEGER,
_____ issuingMemberState SEQUENCE OF NationAlpha,
_____ cardsGeneration SEQUENCE OF INTEGER,
_____ numberSimilarEvent INTEGER
_____ }
_____
_____ DrivingWithoutAnAppropriateCard ::= SEQUENCE{
_____ beginDate GeneralizedTime,
_____ endDate GeneralizedTime,
_____ carsdType SEQUENCE OF UTF8String,
_____ cardsNumber SEQUENCE OF INTEGER,
_____ issuingMemberState SEQUENCE OF NationAlpha,
_____ cardsGeneration SEQUENCE OF INTEGER,
_____ numberOfSimilarEvent INTEGER
_____ }
_____
_____ CardInsertionWhileDriving ::= SEQUENCE{
_____ date GeneralizedTime,
_____ carsdType SEQUENCE OF UTF8String,
_____ cardsNumber SEQUENCE OF INTEGER,
_____ issuingMemberState SEQUENCE OF NationAlpha,
_____ numberOfSimilarEvents INTEGER
_____ }
_____
_____ LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
_____ beginDate GeneralizedTime,
_____ endDate GeneralizedTime,
_____ carsdType SEQUENCE OF UTF8String,
_____ cardsNumber SEQUENCE OF INTEGER,
_____ issuingMemberState SEQUENCE OF NationAlpha,
_____ cardsGeneration SEQUENCE OF INTEGER,
_____ oldSession SEQUENCE{
_____ beginDate GeneralizedTime,
_____ endDate GeneralizedTime,
_____ vrn UTF8String,
_____ issuingMemberState NationAlpha,
_____ cardsGeneration INTEGER,
_____ }
_____ }
_____
_____ OverSpeeding ::=SEQUENCE{
_____ beginDate GeneralizedTime,

```

```

_____ endDate GeneralizedTime,
_____ maximumSpeed INTEGER,
_____ averageSpeed INTEGER,
_____ cardType UTF8String,
_____ cardNumber INTEGER,
_____ issuingMemberState NationAlpha,
_____ cardGeneration INTEGER,
_____ numberOfSimilarEvents INTEGER
_____ }
_____
_____ PowerSupplyInterruption ::= SEQUENCE{
_____ beginDate GeneralizedTime,
_____ endDate GeneralizedTime,
_____ cardsType SEQUENCE OF UTF8String,
_____ cardsNumber SEQUENCE OF INTEGER,
_____ issuingMemberState SEQUENCE OF NationAlpha,
_____ cardsGeneration SEQUENCE OF INTEGER,
_____ numberOfSimilarEvent INTEGER
_____ }
_____
_____ CommunicationErrorWithTheRemoteCommunicationFacility ::= SEQUENCE{
_____ beginDate GeneralizedTime,
_____ endDate GeneralizedTime,
_____ cardsType SEQUENCE OF UTF8String,
_____ cardsNumber SEQUENCE OF INTEGER,
_____ issuingMemberState SEQUENCE OF NationAlpha,
_____ cardsGeneration SEQUENCE OF INTEGER,
_____ numberOfSimilarEvent INTEGER
_____ }
_____
_____ AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
_____ beginDate GeneralizedTime,
_____ endDate GeneralizedTime,
_____ cardsType SEQUENCE OF UTF8String,
_____ cardsNumber SEQUENCE OF INTEGER,
_____ issuingMemberState SEQUENCE OF NationAlpha,
_____ cardsGeneration SEQUENCE OF INTEGER,
_____ numberOfSimilarEvent INTEGER
_____ }
_____
_____ PositionDataError ::= SEQUENCE{
_____ beginDate GeneralizedTime,
_____ endDate GeneralizedTime,
_____ cardsType SEQUENCE OF UTF8String,
_____ cardsNumber SEQUENCE OF INTEGER,
_____ issuingMemberState SEQUENCE OF NationAlpha,
_____ cardsGeneration SEQUENCE OF INTEGER,
_____ numberOfSimilarEvent INTEGER
_____ }
_____
_____ MotionDataError ::= SEQUENCE{
_____ beginDate GeneralizedTime,
_____ endDate GeneralizedTime,
_____ cardsType SEQUENCE OF UTF8String,
_____ cardsNumber SEQUENCE OF INTEGER,
_____ issuingMemberState SEQUENCE OF NationAlpha,
_____ cardsGeneration SEQUENCE OF INTEGER,
_____ numberOfSimilarEvent INTEGER
_____ }
_____

```

```

VehicleMotionConflict ::= SEQUENCE{
    beginDate GeneralizedTime,
    endDate GeneralizedTime,
    carsdType SEQUENCE OF UTF8String,
    cardsNumber SEQUENCE OF INTEGER,
    issuingMemberState SEQUENCE OF NationAlpha,
    cardsGeneration SEQUENCE OF INTEGER,
    numberOfSimilarEvent INTEGER
}

```

```

SecurityBreachAttempt ::= SEQUENCE{
    beginDate GeneralizedTime,
    endDate GeneralizedTime
    carsdType SEQUENCE OF UTF8String,
    cardsNumber SEQUENCE OF INTEGER,
    issuingMemberState SEQUENCE OF NationAlpha,
    cardsGeneration SEQUENCE OF INTEGER,
    numberOfSimilarEvent INTEGER,

```

```

SecurityBreachAttempt ::= SEQUENCE{
    beginDate GeneralizedTime,
    endDate GeneralizedTime OPTIONAL,
    carsdType SEQUENCE OF UTF8String,
    cardsNumber SEQUENCE OF INTEGER,
    issuingMemberState SEQUENCE OF NationAlpha,
    numberOfSimilarEvent INTEGER,
    typeOfEvent SecurityBreachEvent
}

```

```

TimeConflict ::= SEQUENCE{
    beginDate GeneralizedTime,
    endDate GeneralizedTime,
    carsdType SEQUENCE OF UTF8String,
    cardsNumber SEQUENCE OF INTEGER,
    issuingMemberState SEQUENCE OF NationAlpha,
    cardsGeneration SEQUENCE OF INTEGER,
    numberOfSimilarEvent INTEGER
}

```

FAULTS LIST

```

CardFault ::= SEQUENCE{
    beginDate GeneralizedTime,
    endDate GeneralizedTime,
    carsdType SEQUENCE OF UTF8String,
    cardsNumber SEQUENCE OF INTEGER,
    issuingMemberState SEQUENCE OF NationAlpha,
    cardsGeneration SEQUENCE OF INTEGER,
}

```

```
RecordingEquipmentFault ::= SEQUENCE{  
beginDate GeneralizedTime,  
endDate GeneralizedTime,  
faultType RecordingEquipmentFaultType,  
cardsType SEQUENCE OF UTF8String,  
cardsNumber SEQUENCE OF INTEGER,  
issuingMemberState SEQUENCE OF NationAlpha,  
cardsGeneration SEQUENCE OF INTEGER,  
}  
END
```

Подраздел 14

Функция удаленной связи

Содержание

	<i>Стр.</i>
1. Введение	583
2. Область применения	584
3. Акронимы, определения и обозначения	585
4. Эксплуатационные сценарии	587
4.1 Обзор	587
4.1.1 Предварительные условия передачи данных через интерфейс DSRC 5,8 ГГц	588
4.1.2 Схема 1a: с помощью ручного наведения или временно установленной на обочине аппаратуры удаленной связи раннего обнаружения	589
4.1.3 Схема 1b: с помощью установленного на транспортном средстве и направленного считывающего устройства удаленной связи раннего обнаружения (REDCR)	590
4.2 Безопасность/целостность	590
5. Конструктивные характеристики и протоколы системы удаленной связи	591
5.1 Конструктивные характеристики	591
5.2 Рабочий процесс	594
5.2.1 Операции	594
5.2.2 Интерпретация данных, полученных по системе связи DSRC	596
5.3 Параметры физического интерфейса DSRC удаленной связи	596
5.3.1 Ограничения, обусловленные расположением	596
5.3.2 Параметры нисходящих и восходящих потоков данных	596
5.3.3 Конструктивные особенности антенны	601
5.4 Требования, предусмотренные протоколом DSRC к RTM	601
5.4.1 Обзор	601
5.4.2 Команды	603
5.4.3 Последовательность команд запроса	604
5.4.4 Структуры данных	605
5.4.5 Элементы RtmData, выполняемые действия и определения	606
5.4.6 Механизм передачи данных	616
5.4.7 Детальное описание операций DSRC	616
5.4.8 Детальное описание операции по проверке DSRC	624
5.5 Поддержка Директивы 2015/71/ЕС (текст удален) Зарезервировано для использования в будущем	627
5.6 Механизмы передачи Передача данных между DSRC_VU и БУ	627
5.6.1 Физическое соединение и интерфейсы	627
5.6.2 Протокол приложения	628

5.7	Обработка ошибок	629
5.7.1	Регистрация и передача данных в DSRC-VU	629
5.7.2	Ошибки беспроводной связи	630
6.	Испытания при вводе в эксплуатацию и периодических проверках функции удаленной связи	631
6.1	Общие положения	631
6.2	ЕСНО	631
6.3	Испытания на подтверждение защищенности содержания данных	632
Приложение	633

1. Введение

В настоящем ~~приложении подразделе~~ отобразены проект и процедуры реализации системы удаленной связи (далее — связь) ~~в соответствии с требованиями статьи 9 Регламента (ЕС) № 165/2014 (далее — Регламент).~~

~~DSC_1~~ ~~Регламент (ЕС) № 165/2014 определяет, что~~ **DSC_1** Тахограф оснащается функцией удаленной связи, позволяющей представителям компетентных контрольных органов считывать информацию с тахографов проезжающих транспортных средств с помощью соответствующего оборудования удаленного мониторинга (считывающего устройства удаленной связи раннего обнаружения [REDCR]), в частности, оборудования мониторинга, обеспечивающего беспроводное соединение с помощью интерфейса выделенной связи ближнего действия CEN 5,8 ГГц (DSRC).

Важно иметь в виду, что цель данной функции — выполнять роль предварительного фильтра для выявления транспортных средств в целях проведения более тщательной проверки и тот факт, что процедуры официальной проверки она не заменяет ~~и, как указано в положениях Регламента (ЕС) № 165/2014. См. положение 9 в преамбуле данного регламента, в котором говорится, что система дистанционной связи.~~ Система удаленной связи между тахографом и контрольными органами для целей проверок на дорогах способствует проведению в соответствующих случаях таких целевых проверок на дорогах.

DSC_2 Обмен данными должен осуществляться с использованием системы связи, которая представляет собой беспроводное взаимодействие по беспроводной связи DSRC на частоте 5,8 ГГц, соответствующей данному ~~приложению подразделу~~ и проверенной на соответствие требуемым параметрам EN 300 674-1, {Электромагнитная совместимость и вопросы радиоспектра (ERM); Телематика автомобильного транспорта и дорожного движения (RTTT); Оборудование передачи данных по выделенной связи ближнего действия (DSRC) (500 кбит/с/250 кбит/с), работающее в диапазоне частот, отведенных для промышленных, научных и медицинских целей (ISM) 5,8 ГГц; Часть 1: Общие характеристики и методы проверок контрольных устройств на дорогах (ПКУ) и бортовых устройств (БУ)}.

DSC_3 Коммуникация с устройством связи устанавливается только в том случае, если запрос выдается устройством компетентного контрольного органа с помощью соответствующего требованиям радиокommunikационного оборудования (считывающего устройства удаленной связи раннего обнаружения (REDCR)).

DSC_4 Для обеспечения целостности данных они должны быть защищены.

DSC_5 Доступ к передаваемым данным предоставляется только компетентным контрольным органам, ~~уполномоченным совершать проверки на предмет нарушений Регламента (ЕС) № 561/2016 и Регламента (ЕС) № 165/2014,~~ и мастерским в той степени, в какой это необходимо для проверки правильного функционирования тахографа.

DSC_6 Данные, обмен которыми происходит во время связи, ограничиваются теми данными, которые необходимы для целевых проверок транспортных средств на дорогах, в случае которых предполагается вероятность манипуляции с тахографом или злоупотребление им.

DSC_7 Целостность и безопасность данных обеспечивается путем защиты данных в бортовом устройстве (БУ) и передачи только содержащихся в нем защищенных данных и данных, касающихся безопасности (см. 4.4.4 5.4.4), при помощи беспроводного средства удаленной связи DSRC, работающей на частоте 5,8 ГГц; это означает, что понять данные, передаваемые по этой связи, и проверить их аутентичность могут только

уполномоченные представители компетентных контрольных органов.
См. ~~приложение~~ **подраздел 11** «Общие механизмы безопасности».

- DSC_8 *Эти данные* содержат временную метку последнего обновления.
- DSC_9 Содержание данных по безопасности известны только компетентным контрольным органам и сторонам, которым предоставляется эта информация, находится под их контролем и не регулируется положениями в области *связи*, представляющей собой предмет настоящего ~~приложения~~ **подраздела**, за исключением того, что данная *связь* предусматривает возможность передачи пакета защищенных данных с каждым пакетом обычных данных.
- DSC_10 Ту же самую архитектуру и то же оборудование можно использовать для разработки других концепций данных (таких как взвешивание на борту), используя в этих целях ту же архитектуру, которая упомянута здесь.
- DSC_11 ~~Для уточнения в соответствии с положениями Регламента (ЕС) № 165/2014 (7-й статьи) данные о~~ **Данные** о личности водителя по этой системе *связи* не передаются.

2. Область применения

Область применения настоящего ~~приложения~~ **подраздела** — указать, каким образом представители компетентных контрольных органов пользуются беспроводной связью DSRC 5,8 ГГц для удаленного получения данных (*Данные*) с выбранного транспортного средства, если есть подозрения по поводу того, что оно, возможно, нарушает ~~Регламент (ЕС) № 165/2014~~, настоящее **Соглашение** и что в этой связи необходимо рассмотреть вопрос о необходимости его остановки в целях дальнейшей проверки.

~~Регламент (ЕС) № 165/2014 требует, чтобы собираемые Данные, подлежащие сбору, ограничиваются данными или имеют отношение к данным, которые указывают на возможное нарушение, или связанные с ними данные, как указано в статье 9 Регламента (ЕС) № 165/2014.~~

В случае такого сценария время связи ограничено, поскольку данный вид связи носит целевой характер и действует на ближнем расстоянии. Кроме того, компетентные контрольные органы могут использовать такую же связь для удаленного мониторинга тахографов (RTM) и в других целях (таких, как проверка максимального веса и габаритов большегрузных транспортных средств ~~определенные в Директиве 2015/719/ЕС~~), с учетом того факта, что по усмотрению компетентных контрольных органов такие операции могут носить разовый или последовательный характер.

В данном ~~приложении~~ **подразделе** уточняются такие вопросы, как:

- оборудование, процедуры и протоколы связи, подлежащие использованию в целях *коммуникации*;
- стандарты и правила, которым должно соответствовать радиооборудование;
- передача *данных* в *коммуникационное* оборудование;
- процедуры запроса и загрузки и последовательность операций;
- данные, подлежащие передаче;
- возможное толкование *данных*, передаваемых в пределах системы *коммуникации*;
- положения, регламентирующие данные, имеющие отношение к системе *коммуникации*;

- наличие *данных* для компетентных контрольных органов;
- способы, с помощью которых *считывающее устройство системы коммуникации удаленной связи раннего обнаружения* может запрашивать разные системы данных о грузах и автомобильном парке.

В порядке уточнения в настоящем ~~приложении~~ **подразделе** не указывается следующее:

осуществление и управление системой сбора *данных* в БУ (~~которые должны являться проектной функцией продукта, если в Регламенте (ЕС) № 165/2014 не указано иное~~)

- форма представления собранных данных сотруднику компетентных контрольных органов или критерии, используемые компетентными контрольными органами в целях принятия решения о том, какое транспортное средство следует остановить (~~что является проектной функцией данного продукта, если в Регламенте (ЕС) № 165/2014 не указано иное, или директивным решением компетентных контрольных органов~~). Уточнение: *система коммуникации* позволяет только собирать *данные* для компетентных контрольных органов, с тем чтобы они могли принимать обоснованные решения;
- положения, регламентирующие безопасность данных (например, шифрование), в части содержания *данных* (что уточняется в ~~приложении~~ **подразделе** 11 «Общие механизмы безопасности»);
- подробное описание любых концепций данных, кроме RTM, которые можно получать с помощью такой же архитектуры и оборудования;
- детальные данные по поводу поведения и управления системой взаимосвязи между БУ и DSRC-VU или поведения на уровне DSRC-VU (кроме случаев, когда необходимо представить *данные* по требованию REDCR).

3. Акронимы, определения и обозначения

В настоящем ~~приложении~~ **подразделе** используются следующие акронимы и определения:

Антенна	Электрический прибор, преобразующий электрическую энергию в радиоволны и наоборот, используемый вместе с радиопередатчиком или радиоприемником. На практике радиопередатчик подает электрические колебательные сигналы на соответствующей радиочастоте и поступающие на разъемы антенны, которая излучает эту электроэнергию в виде электромагнитной волны (радиоволны). В режиме приема антенна перехватывает часть энергии электромагнитной волны, которая создает на уровне разъемов весьма незначительное напряжение, передаваемое на приемник в целях его усиления.
Коммуникация	Обмен информацией/данными между DSRC-REDCR и DSRC-VU в соответствии с разделом 0 в целях синхронизации, позволяющей получить передаваемые данные.
Данные	защищенные данные определенного формата (см. 5.4.4), запрашиваемые DSRC-REDCR и передаваемые DSRC-VU на DSRC-REDCR на частоте 5,8 ГГц, как указано в разделе 5 ниже.
Регламент (ЕС) № 165/2014	Регламент (ЕС) № 165/2014 Европейского парламента и Совета от 4 февраля 2014 г. о тахографах дорожных транспортных средств, отменяющий Регламент Совета (ЕЭС) № 3821/85 о записывающем оборудовании на дорожном транспорте и вносящий поправки в Регламент (ЕС) № 561/2006 Европейского

парламента и Совета о гармонизации социального законодательства, связанного с дорожным транспортом.

АИД	идентификатор приложения
BLE	система «Bluetooth» с низким энергопотреблением
БСТ	радионавигационная служба с использованием радиомаяков
CIWD	ввод карточки во время управления
КПР	циклический контроль избыточности
DSC (n)	идентификатор требования конкретного приложения DSRC
DSRC	выделенная связь ближнего действия
DSRC-REDCR	REDCR — считывающее устройство удаленной связи раннего обнаружения.
DSRC-VU.	DSRC — бортовое устройство. Это — «дистанционное устройство раннего обнаружения», определенное в приложении добавлении 1С .
DWVC	управление без действительной карточки
EID	идентификатор элемента
LLC	управление логической связью
LPDU	блок данных протокола LLC
OWS	бортовая система взвешивания
PDU	блок данных протокола
REDCR	считывающее устройство удаленной связи раннего обнаружения. Это — «оборудование, представляющее собой считывающее устройство удаленной связи раннего обнаружения», определенное в приложении добавлении 1С .
RTM	удаленный мониторинг тахографа
SM-REDCR	защитный модуль — считывающее устройство удаленной связи раннего обнаружения
TARV	приложения телеинформатики для регулируемых транспортных средств (серия стандартов ISO 15638)
VU (БУ)	бортовое устройство
VUPM	блок памяти бортового устройства
VUSM	модуль защиты бортового устройства
VST	таблица обслуживания транспортного средства
WIM	взвешивание в пути
WOB	взвешивание на борту

Спецификация, определенная в настоящем ~~приложении~~ **подразделе**, относится ко всем следующим правилам и стандартам или их частям или разработана на их основе. В положениях настоящего ~~приложения~~ **подраздела** указываются конкретные стандарты или предусмотренные ими конкретные условия. В случае противоречия преимущественную силу имеют положения настоящего подраздела. Если в настоящем ~~приложении~~ **подразделе** нет никаких конкретных указаний, то в случае любых противоречий преимущественную силу имеет ERC 70-03 (и испытания по соответствующим параметрам EN 300 674-1)¹⁵, а затем в порядке убывания и в

¹⁵ С учетом развития научно-технического прогресса в случаях, когда отсутствует ссылка на какой-либо стандарт ISO, но есть только ссылка на региональный стандарт,

зависимости от предпочтения¹⁶ — EN 12795, EN 12253, EN 12834 и EN 13372, 6.2, 6.3, 6.4 и 7.1.

Регламенты и Стандарты, на которые даются ссылки в настоящем **приложении подразделе**:

~~Регламент (ЕС) № 165/2014 Европейского парламента и Совета от 4 февраля 2014 года о тахографах на автомобильном транспорте, отменяющий Регламент Совета (ЕЭС) № 3821/85 о записывающем оборудовании на автомобильном транспорте и внесение поправок Регламент (ЕС) № 561/2006 Европейского парламента и Совета от 15 марта 2006 г. о согласовании соответствующего социального законодательства, связанного с дорожным транспортом, вносящий поправки в Регламенты Совета (ЕЭС) № 3821/85 и (ЕС) № 2135/98 и отменяющий Регламент Совета (ЕС) № 3820/85 (текст применим в ЕЭП).~~

1. ERC 70-03 СЕРТ: Рекомендация ECC 70-03: Использование устройств ближнего действия (SRD)
2. ISO 15638 Интеллектуальные транспортные системы. Рамочные принципы приложений телеинформатики на базе сотрудничества для регламентированных коммерческих грузовых транспортных средств (TARV).
3. EN 300 674-1 Электромагнитная совместимость и вопросы радиоспектра (ERM); Телематика автомобильного транспорта и дорожного движения (RTTT); Оборудование для передачи данных по выделенной связи ближнего действия (DSRC) (500 кбит/с / 250 кбит/с), работающее в диапазоне частот, отведенных для промышленных научных и медицинских целей (ISM) 5,8 ГГц; Часть 1: Общие характеристики и методы проверок контрольных устройств на дорогах (ПКУ) и бортовых устройств (БУ)}.
4. EN 12253 Телеинформатика дорожного транспорта и дорожного движения. Выделенная связь ближнего действия. Физический уровень с использованием микроволн с частотой 5,8 ГГц.
5. EN 12795 Телеинформатика дорожного транспорта и дорожного движения. Выделенная связь ближнего действия. Уровень канала передачи данных: доступ к носителям и управление логической связью.
6. EN 12834: Телеинформатика дорожного транспорта и дорожного движения. Выделенная связь ближнего действия — прикладной уровень.
7. EN 13372: Телеинформатика дорожного транспорта и дорожного движения. Выделенная связь ближнего действия. Характеристики приложений RTTT.
8. ISO 14906: Система электронного взимания платы за проезд. Определение интерфейса приложения для выделенной связи ближнего действия.

4. Эксплуатационные сценарии

4.1 Обзор

~~Регламент (ЕС) № 165/2014 предусматривает конкретные и контролируемые Поддерживаемые сценарии, в соответствии с которыми следует использовать систему коммуникации.~~

Описание схемы коммуникации 1: проверка на дорогах с использованием беспроводной связи ближнего действия и считывающего устройства удаленной связи

компетентные органы Договаривающихся сторон могут использовать другие технические правила, но не хуже тех, которые предусмотрены в применяемых стандартах.

¹⁶ Переход на стандарт ISO планируется осуществить в течение пяти лет.

раннего обнаружения, инициирующего физические проверки на дорогах (по принципу «ведущий — ведомый»).

«Схема считывающего устройства 1a: с помощью ручного наведения или временно установленной на обочине аппаратуры удаленной связи раннего обнаружения.

Схема считывающего устройства 1b: с помощью установленного на транспортном средстве и направленного считывающего устройства удаленной связи раннего обнаружения (REDCR)».

4.1.1 Предварительные условия передачи данных через интерфейс DSRC 5,8 ГГц

ПРИМЕЧАНИЕ: Для того чтобы лучше понять контекст предварительных условий, считывающее устройство представлено на рисунке 14.3 ниже.

4.1.1.1 Данные, хранящиеся в БУ

DSC_12 БУ отвечает через каждые 60 секунд за обновление и поддержку данных, хранящихся в БУ, без какого бы то ни было участия интерфейса функции связи DSRC. Методы, которыми это достигается, определяются самим БУ, как указано в Регламенте (ЕС) № 165/2014, приложение 1С, разделе 3.19 **добавления 1С**, «Удаленная связь для целевых придорожных проверок», и в настоящем **приложении подразделе** не уточняются.

4.1.1.2 Данные, передаваемые на устройство DSRC-VU

DSC_13 БУ отвечает за обновление данных тахографа DSRC (*данные*) каждый раз, когда хранящиеся в БУ данные обновляются с интервалом, указанным в пункте 4.1.1.1 (DSC_12), без какого бы то ни было воздействия функции связи DSRC.

DSC_14 Данные БУ используются в качестве основы наполнения и обновления *данных*, а средства, которыми это достигается, описываются в **приложении добавлении 1С**, раздел 3.19 «Удаленная связь для целевых проверок на дорогах», или, если такой спецификации нет, являются проектной функцией изделия и в настоящем **приложении подразделе** не уточняются. Схему связи между устройством DSRC-VU и БУ см. раздел 5.6.

4.1.1.3 Содержание данных

DSC_15 Содержание и формат *данных* таковы, что после расшифровки они отображаются в структуре, форме и формате, описанных в пункте 5.4.4 настоящего **подраздела** (структуры данных).

4.1.1.4 Представление данных

DSC_16 *Данные*, которые часто обновляются в соответствии с процедурами, определенными в пункте 4.1.1.1, защищаются до передачи в *DSRC-VU* и выдаются в виде соответствующего концептуального значения защищенных данных для временного хранения в *DSRC-VU* в качестве текущей версии *данных*. Эти данные передаются из *VUSM* на функцию DSRC *VUPM*. *VUSM* и *VUPM* являются функциями и необязательно физическими объектами. Форма создания физического объекта в целях выполнения данных функций обусловлена проектными особенностями продукта, если в Регламенте (ЕС) № 165/2014 **добавлении 1С** не указано иное.

4.1.1.5 Данные по безопасности

DSC_17 Данные по безопасности (*DSRCsecurityData*), включающие в себя данные, необходимые REDCR для выполнения своей функции по расшифровке ~~данных~~, выдаются, как указано в ~~приложении~~ **подразделе 11 добавления** «Общие механизмы безопасности», ~~в виде значения данных~~ для временного хранения в *DSRC-VU* в качестве текущей версии *DSRCsecurityData*, в форме, указанной в **разделе 5.4.4** настоящего ~~приложения~~ **подраздела добавления**.

4.1.1.6 Данные VUPM, доступные для передачи через интерфейс DSRC

DSC_18 Данные, всегда доступные в блоке функции DSRC VUPM в целях немедленной передачи по требованию REDCR, представлены в разделе 5.4.4 в части подробных спецификаций модуля ASN.1.

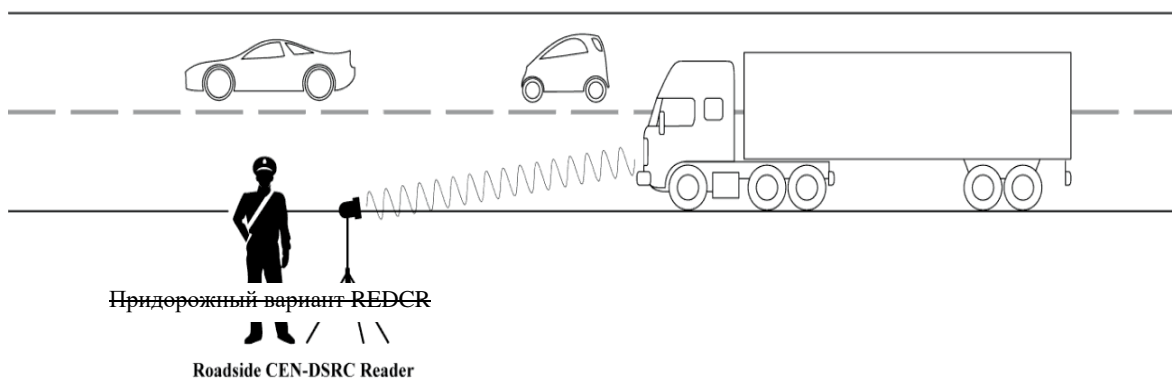
Общий обзор схемы коммуникации 1

Эта схема относится к примеру использования, когда какой-либо представитель компетентных контрольных органов пользуется в целях удаленной связи ближнего действия считывающим устройством удаленной связи раннего обнаружения (интерфейсы DSRC 5,8 ГГц, применяемые в соответствии с ERC 70-03 и тестируемые по соответствующим параметрам EN 300 674-1, как описано в разделе 0) (*REDCR*), в порядке удаленной идентификации соответствующего транспортного средства, ~~которое, возможно, нарушает Регламент (ЕС) № 165/2014~~. После идентификации представитель компетентных контрольных органов, контролирующий ход проверки, принимает решение на предмет необходимости остановить данное транспортное средство.

4.1.2 Схема 1a: с помощью ручного наведения или временно установленной на обочине аппаратуры удаленной связи раннего обнаружения

В данном случае представитель компетентных контрольных органов находится на обочине и направляет ручное устройство REDCR на треноге или аналогичное переносное устройство с обочины в направлении центральной части лобового стекла проверяемого транспортного средства. Проверка осуществляется с использованием интерфейса DSRC 5,8 ГГц в соответствии с ERC 70-03, результаты которой определяются на основании соответствующих параметров EN 300 674-1, как описано в разделе 5. См. рисунок 14.1 (вариант использования 1).

Рис. 14.1
Контроль на дорогах с помощью DSRC 5,8 ГГц
Use case 1

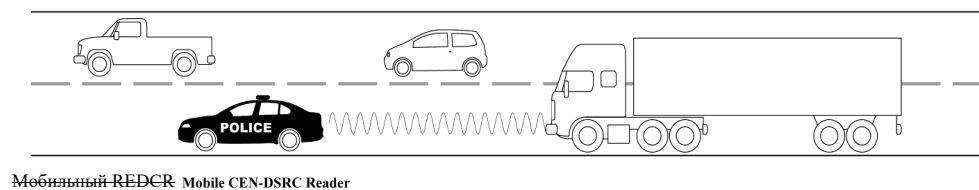


4.1.3. Схема 1b: с помощью установленного на транспортном средстве и направленного считывающего устройства удаленной связи раннего обнаружения (REDCR)

В данном случае представитель компетентных контрольных органов находится в движущемся транспортном средстве и направляет ручное переносное устройство REDCR со своего транспортного средства в сторону центральной части лобового стекла проверяемого транспортного средства, или же устройство REDCR установлено внутри транспортного средства или на нем таким образом, чтобы оно было направлено на центр лобового стекла проверяемого транспортного средства, когда транспортное средство со считывающим устройством удаленного действия раннего обнаружения находится в заданном положении относительно проверяемого транспортного средства (например, непосредственно перед ним в потоке машин). Проверка осуществляется с использованием интерфейса DSRC 5,8 ГГц в соответствии с ERC 70-03, результаты которой выясняются на основании соответствующих параметров EN 300 674-1, как описано в разделе 5. См. рис. 14.2. (Пример использования 2).

Рис. 14.2
Контроль на дорогах с использованием DSRC 5,8 ГГц

Use case 2



4.2 Безопасность/целостность

Для целей контроля подлинности и целостности загруженных данных с помощью системы удаленной связи защищенные данные проверяются и расшифровываются в соответствии с ~~приложением~~ **подразделом 11** «Общие механизмы безопасности».

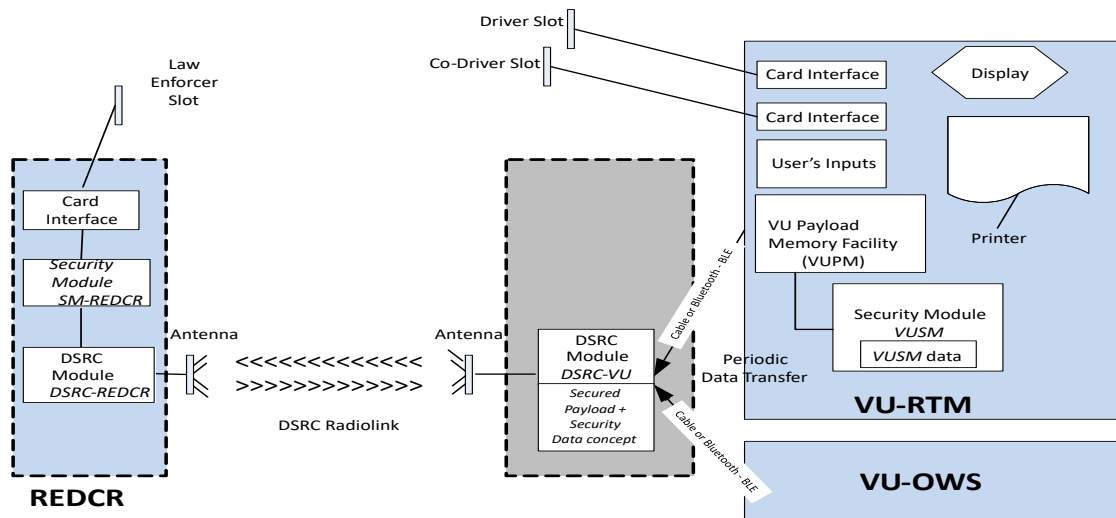
5. Конструктивные характеристики и протоколы системы удаленной связи

5.1 Конструктивные характеристики

Система функции удаленной связи в смарт-тахографе показана на рис. 14.3.

Рис. 14.3

Схема функции удаленной связи



DSC_19 В БУ встроены следующие функции:

- модуль безопасности (*VUSM*). Данная функция БУ отвечает за защиту данных, которые подлежат передаче с DSRC-VU представителю компетентных контрольных органов с помощью системы удаленной связи.
- Защищенные данные хранятся в блоке памяти VUSM. С интервалами, указанными в 4.1.1.1 (DSC_12), БУ шифрует и наполняет данные RTM (которые включают в себя значения содержащихся данных и данных по безопасности, представленных ниже в настоящем **приложении подразделе**), хранящиеся в блоке памяти DSRC-VU. Работа модуля безопасности представлена в **приложении подразделе 11** «Общие механизмы безопасности» и не входит в область применения настоящего **приложения подраздела**), за исключением того, что в этом случае необходимо направлять обновленные данные устройству связи БУ каждый раз, когда меняются данные VUSM.
- Коммуникация между БУ и DSRC-VU может быть проводной или беспроводной с использованием системы «Bluetooth Low Energy» (BLE), а физическое расположение DSRC-VU может представлять собой единое целое с антенной или лобовым стеклом транспортного средства, быть внутри БУ или находиться где-то между ними.
- DSRC-VU обеспечивается надежным источником питания в любой момент времени. Способы обеспечения питания определяются на уровне проектного решения.
- Память DSRC-VU должна быть энергонезависимой, с тем чтобы данные на DSRC-VU сохранялись даже в том случае, когда зажигание транспортного средства выключено.
- Если связь между БУ и DSRC-VU осуществляется через систему BLE, а источник питания — неподзаряжаемая батарея, то источник питания DSRC-VU заменяется при каждой регулярной проверке, а изготовитель оборудования DSRC-VU обязан проследить, чтобы питание было достаточным на весь период

между двумя регулярными проверками и чтобы в течение этого периода любое устройство REDCR могло получить доступ к данным без сбоев или перерывов.

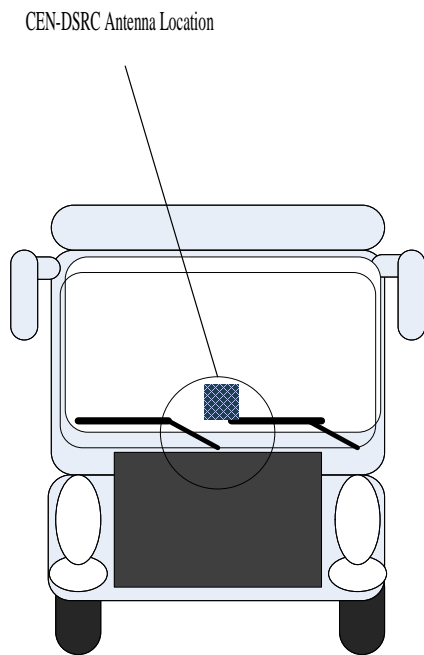
- Блок памяти данных БУ RTM (*VUPM*). Данная функция БУ отвечает за выдачу и обновление *данных*. Содержание *данных* тахографа (TachographPayload) определяется ниже в пунктах 5.4.4/5.4.5 и обновляется с интервалом, указанным в пункте 4.1.1.1 (DSC_12).
 - DSRC-VU. Это - функция, встроенная в антенну или соединенная с ней и обеспечивающая связь с БУ через проводное или беспроводное подключение (BLE), в котором хранятся текущие данные (*данные VUPM*) и осуществляется обработка ответов на запросы при помощи DSRC 5,8 ГГц. Отсоединение устройства DSRC или помехи в работе функций устройства DSRC при нормальной эксплуатации транспортного средства считаются нарушением ~~Регламента (ЕС) № 165/2014~~ **настоящего Соглашения**.
 - Модуль безопасности (REDCR) (*SM-REDCR*) — это функция, используемая для расшифровки и проверки целостности данных, сгружаемых с БУ. Средства, которыми это достигается, представлены в ~~приложении~~ **подразделе 11** «Общие механизмы безопасности» и в настоящем ~~приложении~~ **подразделе** не обсуждаются.
 - Функция DSRC (REDCR) (*DSRC-REDCR*) включает в себя трансивер 5,8 ГГц, а также встроенные программы и другое программное обеспечение, которое управляет *системой коммуникации* с DSRC-VU в соответствии с настоящим ~~приложением~~ **подразделом**.
 - *DSRC-REDCR* запрашивает *DSRC-VU* проверяемого транспортного средства и получает *данные* (текущие *данные VUPM* проверяемого транспортного средства) через посредство соединений и процессов DSRC и хранит полученные данные в своем модуле *SM-REDCR*.
 - Антенна DSRC-VU должна быть расположена в таком месте, в котором обеспечивается оптимальная связь DSRC между транспортным средством и антенной придорожного считывающего устройства (~~как правило, в или рядом,~~ когда само считывающее устройство установлено на расстоянии 15 метров перед транспортным средством и на высоте 2 метра с ориентацией на центр ветрового стекла по горизонтали и вертикали ~~транспортного средства ...)~~ ~~любового —стекла~~. На транспортных средствах малой грузоподъемности устройство может устанавливаться на уровне, **соответствующем** верхней части ветрового стекла. **Для всех остальных транспортных средств антенна DSRC должна быть установлена либо рядом с нижней, либо рядом с верхней частью ветрового стекла.**
 - Перед антенной или вблизи нее не должно быть никаких металлических предметов (например, именных табличек, наклеек, отражающих элементов из фольги (тонировка), противосолнечных козырьков и стеклоочистителей ветрового стекла в неподвижном состоянии), которые могут создать помехи связи.
 - Антенну устанавливают так, чтобы ее осевое направление было примерно параллельно поверхности дороги.
- DSC_20 Антенна и система коммуникации должны работать в пределах значений ERC 70-03, проверенных на соответствие предусмотренным параметрам стандарта EN 300 674-1, как описано в разделе 45. Антенна и система коммуникации могут быть оснащены функцией снижения риска беспроводных помех, как описано в докладе ECC 228, например с помощью коммуникационных фильтров CEN DSRC 5,8 ГГц.
- DSC_21 Антенна DSRC соединена с устройством DSRC-VU непосредственно в модуле, установленном на ветровом стекле или поблизости, или с помощью отдельного кабеля таким образом, чтобы затруднить попытки противозаконного отключения. Отключение или попытки осложнить

работу антенны являются нарушением ~~Регламента (ЕС) № 165/2014 настоящего Соглашения~~. Намеренная маскировка или иное неблагоприятное воздействие на работу антенны считается нарушением ~~Регламента (ЕС) № 165/2014~~ **настоящего Соглашения**.

- DSC_22 Фактор формы антенны не определен и зависит от коммерческого решения в той степени, в которой установленное устройство DSRC-VU соответствует требованиям раздела 5 ниже. Антенна устанавливается, как указано в DSC_19 и на рисунке 14.4 (овальная линия), и эффективно ~~поддерживает~~ варианты использования, отображенные в пунктах ~~3.1.2 и 3.1.3~~ **4.1.2 и 4.1.3**.

Рис. 14.4

Пример расположения антенны DSRC 5.8 ГГц на ветровом стекле регламентируемых транспортных средств



Фактор формы *REDCR* и антенны может варьироваться в зависимости от обстоятельств, связанных со считывающим устройством (установлено на треноге, ручное, установлено на транспортном средстве и проч.), и метода его использования представителем компетентных контрольных органов.

Функция отображения и/или уведомления используется в целях направления результатов функции удаленной связи представителю компетентных контрольных органов. Отображение возможно на экране, в распечатанном виде, в виде аудиосигнала или в разных сочетаниях этих форм. Форма отображения и/или уведомления зависит от требований представителей компетентных контрольных органов и конструктивных характеристик изделия и в данном ~~приложении~~ **подразделе** не обсуждается.

- DSC_23 Дизайн и фактор формы *REDCR* являются функцией коммерческого проекта, соответствующего требованиям ERC 70-03, и проектных и эксплуатационных спецификаций, указанных в настоящем ~~приложении~~ **подразделе** (раздел 5.3.2), что обеспечивает максимальную рыночную гибкость при проектировании и поставке этого оборудования, позволяющего охватить конкретные сценарии проверки со стороны любого конкретного компетентного контрольного органа.

- DSC_24 Дизайн и фактор формы *DSRC-VU* и его расположение внутри или снаружи БУ являются функцией коммерческого проекта,

соответствующего требованиям ERC 70-03, а равно проектных и эксплуатационных спецификаций, указанных в настоящем ~~приложении~~ **подразделе** (раздел 5.3.2) и в данном положении (5.1).

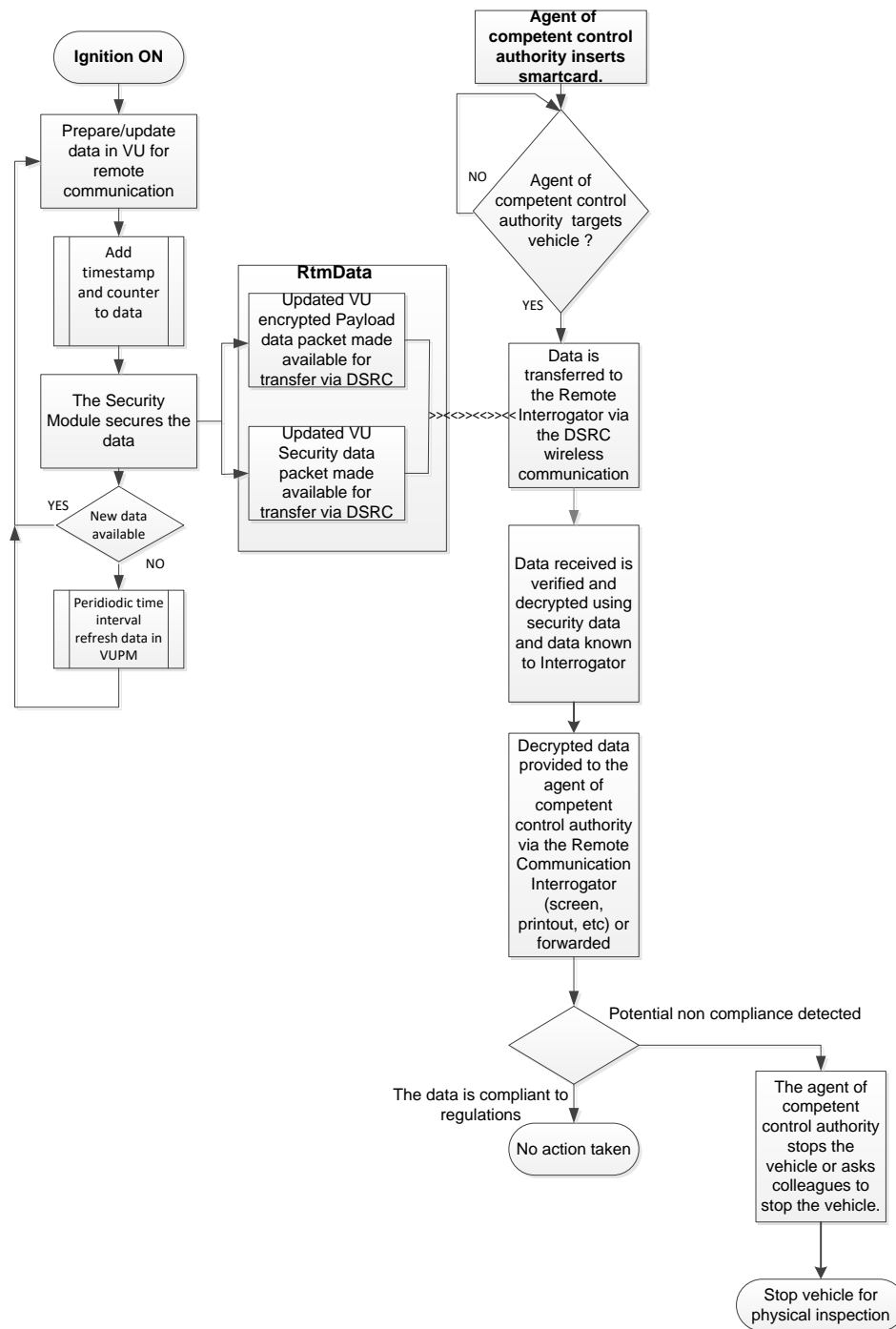
DSC_25 Вместе с тем *DSRC-VU* в принципе способно на приемлемом уровне принимать значения данных из другой программируемой аппаратуры «интеллектуального» транспортного средства с помощью соответствующего соединения и протоколов открытого промышленного стандарта (например, в случае оборудования для соответствующего соединения и протоколов открытого промышленного стандарта (например, в случае оборудования для взвешивания на борту), если данные определяются уникальными и известными идентификаторами приложений/названиями файлов и если ~~Европейской комиссией~~ **лаборатории, компетентной в вопросах испытаний на эксплуатационную совместимость**, предоставляется доступ к инструкциям по использованию таких протоколов, а изготовителям соответствующего оборудования этот доступ предоставляется на безвозмездной основе.

~~5.24.2~~ **Рабочий процесс**

~~5.2.15.4~~ **Операции**

Рабочая схема операций представлена на рисунке 14.5.

Рис. 14.5
Рабочий процесс функции удаленной связи



Этапы этого процесса описаны ниже:

а) в процессе эксплуатации транспортного средства (зажигание «Вкл.») тахограф передает данные на устройство БУ. Соответствующая функция БУ готовит *данные* для функции удаленной связи (в зашифрованном виде) и обновляет *данные VUPM*, хранящиеся в памяти *DSRC-VU* (как указано в пунктах 4.1.1.1–4.1.1.2). Собранные данные форматируются в соответствии с пунктами 5.4.4–5.4.5 ниже;

б) каждый раз, когда *данные* обновляются, обновляется и временная метка, указанная в данных по безопасности;

в) функция *VUSM* обеспечивает защиту данных в соответствии с процедурами, указанными в ~~приложении~~ **подразделе 11**;

d) каждый раз, когда *Данные* обновляются (см. 4.1.1.1-4.1.1.2), они передаются в *DSRC-VU*, где они заменяют любые прежние данные с целью обеспечить доступность обновленных текущих данных (*Данные*) на случай проверки *REDCR*. В процессе передачи *Данных* из БУ в *DSRC-VU* их можно будет идентифицировать по названию файла «*RTMData*» или по идентификаторам «*ApplicationID*» и «*Attribute*»;

e) если представитель компетентных контрольных органов намерен проверить какое-либо транспортное средство и снять с него данные, он сначала вводит свою смарт-карточку в *REDCR* с целью активировать функцию *Коммуникация* и тем самым позволяет *SM-REDCR* проверить ее подлинность и расшифровать данные;

f) затем этот представитель компетентного контрольного органа проводит целевую проверку соответствующего транспортного средства и запрашивает данные с помощью системы удаленной связи. *REDCR* открывает сеанс связи через интерфейс *DSRC 5,8 ГГц* с *DSRC-VU* проверяемого транспортного средства и запрашивает необходимые данные. Данные передаются в *REDCR* по системе беспроводной связи в качестве атрибута *DSRC* с помощью приложения *GET*, как указано в пункте 5.4. Атрибут содержит значения зашифрованных нужных данных и данные по безопасности *DSRC*;

g) эти данные анализируются аппаратурой *REDCR* и передаются представителю компетентного контрольного органа;

h) представитель компетентного контрольного органа использует эти данные в целях аргументированного принятия решения по поводу того, следует ли остановить данное транспортное средство для тщательной проверки или попросить другого представителя компетентного контрольного органа остановить указанное транспортное средство.

5.2.2 Интерпретация данных, полученных по системе связи *DSRC*

DSC_26 Данные, полученные через интерфейс *5,8 ГГц*, имеют тот же смысл и ту же суть, которые определены в пунктах 5.4.4 и 5.4.5 ниже, и понимаются как таковые только в связи целями, которые в них определены. В соответствии с положениями Регламента (ЕС) № 165/2014 действующего законодательства в каждой Договаривающейся стороне эти *Данные* используются только для предоставления соответствующей информации компетентному контрольному органу с целью помочь ему установить, какое транспортное средство следует задержать для физического осмотра, и впоследствии уничтожить эту информацию в соответствии со статьей 9 Регламента (ЕС) № 165/2014 с действующим законодательства в каждой Договаривающейся стороне.

5.3 Параметры физического интерфейса *DSRC* удаленной связи

5.3.1 Ограничения, обусловленные расположением

DSC_27 Удаленный запрос на проверку транспортных средств при помощи интерфейса *DSRC 5,8 ГГц* не должен применяться в радиусе 200 метров от действующего портала *DSRC 5,8 ГГц*.

5.3.2 Параметры нисходящих и восходящих потоков данных

DSC_28 Оборудование, используемое для удаленного мониторинга тахографов, соответствует стандарту *ERC70-03* и эксплуатируется в соответствии с этим стандартом и параметрами, отраженными ниже в таблицах 14.1 и 14.2.

DSC_29 Кроме того, в целях обеспечения совместимости с эксплуатационными параметрами других стандартизированных систем *DSRC 5,8 ГГц*, оборудование, используемое для удаленного мониторинга тахографов, должно соответствовать параметрам *EN 12253* и *EN 13372*.

В частности:

Таблица 14.1

Параметры нисходящей линии связи

Позиция №	Параметр	Значение(я)	Примечание
D1	Несущие частоты нисходящей линии связи	Существует четыре альтернативных варианта, которые может использовать REDCR: 5,7975 ГГц 5,8025 ГГц 5,8075 ГГц 5,8125 ГГц	В пределах ERC 70-03 Несущие частоты могут быть выбраны исполнителем придорожной системы и не обязательно должны быть известны в DSRC-VU (В соответствии с EN 12253, EN 13372)
D1a(*)	Устойчивость носителя Частоты	В пределах ± 5 млн. ⁻¹	(В соответствии с EN 12253)
D2(*)	RSU(REDCR) Маска спектрального предела передатчика	В соответствии с ERC 70-03 REDCR должен соответствовать классу В,С согласно EN 12253 Никаких других конкретных требований в данном приложении добавлении	Параметр, используемый для контроля помех между близко расположенными средствами удаленного мониторинга, как определено в EN 12253 и EN 13372)
D3	OBU(DSRC-VU) Минимальный диапазон частот	5,795–5,815 ГГц	(В соответствии с EN 12253)
D4(*)(**)	Максимальное значение E.I.R.P.	В соответствии с ERC 70-03 (без лицензии) и в рамках национального регулирования Максимум +33 дБм	(В соответствии с EN 12253)
D4a	Угловая маска E.I.R.P.	Согласно заявленной и опубликованной спецификации разработчика средства удаленного мониторинга	(В соответствии с EN 12253, EN 13372)
D5	Поляризация	Левостороннее смещение	(В соответствии с EN 12253)
D5a	Перекрестная поляризация	XPД: Линия визирования: (REDCR) RSU $t \geq 15$ дБ (DSRC-VU) OBU $r \geq 10$ дБ В зоне -3 дБ: (REDCR) RSU $t \geq 10$ дБ (DSRC-VU) OBU $r \geq 6$ дБ	(В соответствии с EN 12253)
D6(*)	Модуляция	Двухуровневая амплитудная модуляция	(В соответствии с EN 12253)
D6a(*)	Индекс модуляции	0.5 ... 0,9	(В соответствии с EN 12253)
D6b	Индикаторная диаграмма	≥ 90 % (время)/ ≥ 85 % (амплитуда)	

Позиция №	Параметр	Значение(я)	Примечание
D7(*)	Кодирование данных	FM0 Бит «1» имеет переходы только в начале и конце битового интервала. Бит «0» имеет дополнительный переход в середине битового интервала по сравнению с битом «1»	(В соответствии с EN 12253)
D8(*)	Битовая скорость	500 кБит/с	(В соответствии с EN 12253)
D8a	Устойчивость битового тактового сигнала	лучше, чем ± 100 млн. ⁻¹	(В соответствии с EN 12253)
D9(*)	Коэффициент битовых ошибок (B.E.R.) в системе связи	$\leq 10^{-6}$, когда падающая мощность на OBU (DSRC-VU) находится в диапазоне, указанном в [D11a–D11b]	(В соответствии с EN 12253)
D10	Сигнал активизации OBU (DSRC-VU)	OBU (DSRC-VU) активизируется при получении любого фрейма с 11 или более октетами (включая преамбулу)	Специальная схема активизации не требуется DSRC-VU может активизироваться при получении фрейма с менее чем 11 октетами (В соответствии с EN 12253)
D10a	Максимальное время запуска	≤ 5 мс	(В соответствии с EN 12253)
D11	Зона коммуникации	Пространственная область, в пределах которой достигается В.Е.Р. в соответствии с D9a	(В соответствии с EN 12253)
D11a(*)	Предел мощности зоны коммуникации (верхний)	-24 дБм	(В соответствии с EN 12253)
D11b(*)	Предел мощности зоны коммуникации (нижний)	Падающая мощность: -43 дБм (визирование) -41 дБм (в пределах -45° — $+45^\circ$, в плоскости, параллельной поверхности дороги, когда DSRC-VU установлено в транспортном средстве (азимут))	(В соответствии с EN 12253) Расширенное требование для горизонтальных углов до $\pm 45^\circ$, в связи со случаями использования, определенными в данном приложении подразделе
D12(*)	Уровень мощности отсечки (DSRC-VU)	-60 дБм	(В соответствии с EN 12253)
D13	Преамбула	Преамбула является обязательной	(В соответствии с EN 12253)
D13a	Длина преамбулы и структура	16 бит \pm 1 бит FM0 кодированные «1» биты	(В соответствии с EN 12253)
D13b	Форма волны преамбулы	Чередующаяся последовательность низкого уровня и высокого уровня с длительностью импульса 2 мкс. Устойчивость D8a	(В соответствии с EN 12253)

Позиция №	Параметр	Значение(я)	Примечание
D13c	Конечные биты	RSU (REDCR) разрешается передавать максимум 8 битов после конечного флага. OBU (DSRC-VU) не обязан учитывать эти дополнительные биты	(В соответствии с EN 12253)

(*) Параметры нисходящих данных, подлежащие проверке на соответствие по результатам теста на соблюдение применимых параметров согласно EN 300 674-1.

(**) Максимальное значение эффективной изотропно излучаемой мощности оборудования, используемого для дистанционного контроля тахографа, должно соответствовать требованиям, установленным на территории данной Договаривающейся стороны.

Таблица 14.2

Параметры восходящей линии связи

Позиция №	Параметр	Значение (значения)	Примечание
U1(*)	Частоты поднесущей	Устройство OBU (DSRC-VU) поддерживает частоты 1,5 МГц и 2,0 МГц RSU (REDCR) поддерживает частоту 1,5 МГц или 2,0 МГц или обе частоты U1-0: 1,5 МГц U1-1: 2,0 МГц	Выбор частоты поднесущей (1,5 МГц или 2,0 МГц) зависит от выбранного профиля EN 13372
U1a(*)	Устойчивость субнесущих частот	В пределах $\pm 0,1$ %	(В соответствии с EN 12253)
U1b	Использование боковых полос	Одинаковые данные с обеих сторон	(В соответствии с EN 12253)
U2(*)	Маска спектрального предела передатчика OBU (DSRC-VU)	В соответствии с EN12253 1) Мощность вне полосы: см. ETSI EN 300674-1 2) Мощность в пределах полосы: [U4a] дБм в диапазоне 500 кГц 3) Передача в любом другом восходящем канале связи: U2(3)-1 = -35 дБм в диапазоне 500 кГц	(В соответствии с EN 12253)
U4a(*)	Максимальное значение E.I.R.P. в одной боковой полосе (визирование)	Два варианта: U4a-0: -14 дБм U4a-1: -21 дБм	Согласно заявленной и опубликованной спецификации разработчика средства удаленного мониторинга
U4b(*)	Максимальное значение E.I.R.P. в одной боковой полосе (35 ⁰)	Два варианта: – Неприменимо – 17 дБм	Согласно заявленной и опубликованной спецификации разработчика средства удаленного мониторинга
U5	Поляризация	Левостороннее смещение	(В соответствии с EN 12253)
U5a	Перекрестная поляризация	XPD: Линия визирования: (REDCR) RSU $r \geq 15$ дБ (DSRC-VU) OBU $r \geq 10$ дБ	(В соответствии с EN 12253)

Позиция №	Параметр	Значение (значения)	Примечание
		При -3 дБ: (REDCR) RSU $r \geq 0$ дБ (DSRC-VU) OBU $t \geq 6$ дБ	
U6	Модуляция поднесущей	2-PSK Кодированные данные синхронизированы с поднесущей: переходы кодированных данных совпадают с переходами поднесущей	(В соответствии с EN 12253)
U6b	Дежурный цикл	Дежурный цикл 50 % $\pm \alpha$, $\alpha \leq 5$ %	(В соответствии с EN 12253)
U6c	Модуляция на несущей	Умножение сигналов модулированной поднесущей и несущей	(В соответствии с EN 12253)
U7(*)	Кодирование данных	NRZI (отсутствие перехода в начале бита «1», переход в начале бита «0», отсутствие перехода внутри бита)	(В соответствии с EN 12253)
U8(*)	Битовая скорость	250 кбит/с	(В соответствии с EN 12253)
U8a	Устойчивость битовых часов	В пределах ± 1000 млн. ⁻¹	(В соответствии с EN 12253)
U9	Коэффициент битовых ошибок (B.E.R.) в системе связи	$\leq 10^6$	(В соответствии с EN 12253)
U11	Зона коммуникации	Пространственная область, в пределах которой DSRC-VU расположен таким образом, что его передачи принимаются REDCR с B.E.R. меньше, чем в случае U9a	(В соответствии с EN 12253)
U12a(*)	Коэффициент преобразования (нижний предел)	1 дБ для каждой боковой полосы Диапазон углов: круговой симметричный между линией визирования и $\pm 35^\circ$ и в пределах -45° — $+45^\circ$ в плоскости, параллельной поверхности дороги, когда DSRC-VU установлено в транспортном средстве (азимут))	Больше установленного диапазона значений горизонтальных углов до $\pm 45^\circ$ в связи со случаями использования, определенными в данном приложении добавлении
U12b(*)	Коэффициент преобразования (верхний предел)	10 дБ для каждой боковой полосы	Меньше установленного диапазона значений для каждой боковой полосы в пределах кругового конуса вокруг линии визирования угол раскрытия 45°

Позиция №	Параметр	Значение (значения)	Примечание
U13	Преамбула	Преамбула является обязательной	(В соответствии с EN 12253)
U13a	Преамбула Длина и структура	32–36 мкс с модулированием только по поднесущей, затем 8 бит NRZI-кодированных битов «0»	(В соответствии с EN 12253)
U13b	Конечные биты	RSU (REDCR) разрешается передавать максимум 8 бит после конечного флажка. RSU (REDCR) не обязан учитывать эти дополнительные биты	(В соответствии с EN 12253)

(*) Параметры восходящих данных, подлежащие проверке на соответствие по результатам теста на соблюдение применимых параметров согласно EN 300 674-1.

5.3.34.3.3 Конструктивные особенности антенны

5.3.3.14.3.3.1 Антенна REDCR

DSC_30 Конструкция антенны *REDCR* зависит от коммерческого проекта; она действует в пределах, указанных в пункте 5.3.2, и адаптирована в порядке оптимизации считывания *DSRC-REDCR* для конкретной цели и с учетом обстоятельств считывания, в которых должно работать устройство REDCR.

5.3.3.24.3.3.2 Антенна БУ

DSC_31 Конструкция антенны *DSRC-VU* зависит от коммерческого проекта; она действует в пределах, указанных в пункте 5.3.2, и адаптирована в целях оптимизации считывания *DSRC-REDCR* для конкретной цели и с учетом обстоятельств считывания, в которых должно работать устройство REDCR.

DSC_32 Антенна БУ крепится на ветровом стекле транспортного средства или рядом с ним, как указано в пункте 5.1 выше.

DSC_33 В испытательной среде в мастерской (см. раздел 6.3) антенна *DSRC-VU*, прикрепленная в соответствии с пунктом 5.1 выше, должна успешно соединяться со стандартным испытательным оборудованием и успешно выполнять требуемую операцию RTM, как указано в настоящем ~~приложении~~ **подразделе**, на расстоянии от 2 до 10 метров, более чем в 99 % времени в расчете на более чем 1000 контрольных запросов в среднем.

5.44.4 Требования, предусмотренные протоколом DSRC к RTM

5.4.14.4.1 Обзор

DSC_34 Протокол операции по загрузке *данных* через интерфейс DSRC 5,8 ГГц предусматривает следующие этапы. В настоящем разделе описана последовательность операций в идеальных условиях без повторных передач или перерывов связи.

ПРИМЕЧАНИЕ: Цель этого этапа инициализации (этап 1) — установить связь между *REDCR* и *DSRC-VU*, находящихся в зоне действия операции DSRC 5,8 ГГц (синхронизация), но еще не установивших связь с *REDCR*, и передавать уведомления о процессах работы приложения.

↪ **Этап 1** Инициализация. *REDCR* передает соответствующий фрейм с «таблицей использования радиомаяков» (BST), в которую входят идентификаторы приложений (AID) в перечне поддерживаемых услуг. В приложении RTM это — просто услуга со

значением AID = 2 (Freight&Fleet). *DSRC-VU* оценивает полученную BST и выдает ответ (см. ниже) с перечнем поддерживаемых приложений в домене «Freight&Fleet», или не отвечает, если никакие приложения не поддерживаются. Если *REDCR* не предлагает AID = 2, то *DSRC-VU* ответ *REDCR* не выдает.

↪ **Этап 2** *DSRC-VU* передает фрейм с запросом выделить частное окно.

↪ **Этап 3** *REDCR* отправляет фрейм с указанием выделенного частного окна.

↪ **Этап 4** *DSRC-VU* использует назначенное частное окно для передачи фрейма с таблицей обслуживания данного транспортного средства (VST). В такой VST представлен перечень всех различных вариантов инстанцирования приложений, которые данное *DSRC-VU* поддерживает в рамках AID = 2. Различные варианты инстанцирования определяются при помощи уникальных EID, каждый из которых ассоциируется со значением параметра контекстной метки приложения с указанием на данное приложение и поддерживаемый стандарт.

↪ **Этап 5** Затем *REDCR* анализирует предложенную VST и либо прерывает связь (RELEASE), так как оно не нуждается ни в чем, что есть в VST (т. е. получает VST из *DSRC-VU*, которое данную операцию RTM не поддерживает), либо, если оно получает соответствующую VST, запускает процесс инстанцирования приложения.

↪ **Этап 6** В этих целях *REDCR* посылает соответствующий фрейм с командой на извлечение данных RTM с указанием на инстанцирование приложения RTM и с идентификатором, соответствующим инстанцированию приложения RTM (как указано *DSRC-VU* в VST), и выделяет соответствующее частное окно.

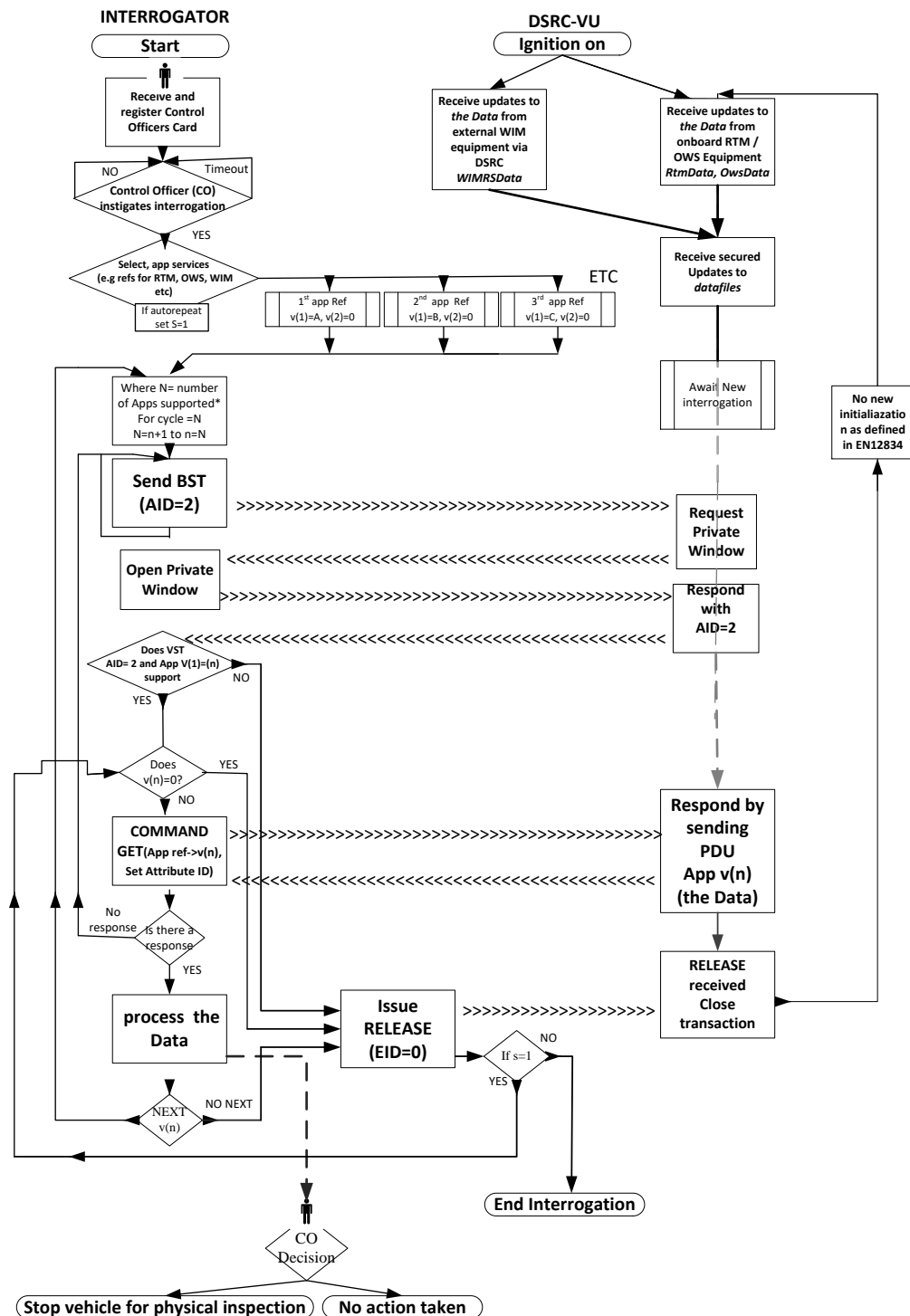
↪ **Этап 7** *DSRC-VU* использует выделенное частное окно для передачи фрейма, в котором содержится адресный идентификатор, соответствующий инстанцированию приложения RTM, как указано в VST, с последующим атрибутом *RtmData* (элемент полезных данных + элемент безопасности).

↪ **Этап 8** Если запросы направлены на несколько услуг, то значение «n» меняется на следующий исходный номер услуги, и процесс повторяется снова.

↪ **Этап 9** *REDCR* подтверждает получение данных, передавая фрейм с командой RELEASE на *DSRC-VU* для прекращения сеанса ИЛИ, если не удалось подтвердить успешное получение LDPU, возвращается на этап 6.

Наглядное описание данного протокола операции отображено на рис. 14.6.

Рис. 14.6
RTM в последовательности процессов DSRC 5,8 ГГц



5.4.24.4.2 Команды

DSC_35 Следующие команды являются единственными функциями, используемыми на этапе операции RTM.

- **INITIALISATION.request:** Команда, выдаваемая REDCR, в форме передачи определения приложений, которые поддерживаются REDCR.
- **INITIALISATION.response:** Ответ DSRC-VU, подтверждающий соединение и содержащий перечень поддерживаемых вариантов приложения с характеристиками и информацией о том, как с ними обращаться (EID).

- **GET.request:** Команда, передаваемая REDCR в DSRC-VU, которая указывает на инстанцирование приложения, подлежащего адресации с помощью определенного EID, полученного в VST, и с указанием DSRC-VU передать выбранный(ые) атрибут(ы) вместе с данными. Цель команды GET — получить данные REDCR из DSRC-VU.
- **GET.response:** Ответ DSRC-VU, в котором содержатся запрашиваемые данные.
- **ACTION.request ECHO:** Команда, указывающая DSRC-VU на отправку данных с DSRC-VU обратно в REDCR. Цель команды ECHO — позволить мастерским или испытательным органам по официальному утверждению типа провести проверку на предмет того, что связь DSRC работает и в доступе к набору удостоверений защиты не нуждается.
- **ACTION.response ECHO:** Ответ DSRC VU на команду ECHO.
- **EVENT_REPORT.request RELEASE:** Команда, указывающая DSRC-VU на завершение операции. Цель команды RELEASE — завершить сеанс с DSRC-VU. По получении команды RELEASE DSRC-VU не отвечает ни на какие другие запросы в ходе данного сеанса связи. Следует иметь в виду, что в соответствии с EN 12834 DSRC-VU дважды не соединяется с одним и тем же контрольным устройством, если оно не находилось за пределами зоны связи в течение 255 секунд или если изменился идентификатор радиомаяка устройства мониторинга.

5.4.34.4.3 Последовательность команд запроса

DSC_36 С точки зрения последовательности команды и ответа эта операция описывается следующим образом:

Последовательность	Передающее устройство	Приемное устройство	Описание	Действие
1	REDCR	> DSRC-VU	Инициализация канала связи — запрос	REDCR передает сообщение BST
2	DSRC-VU	> REDCR	Инициализация канала связи — ответ	Если BST поддерживает AID=2, то DSRC-VU запрашивает частное окно
3	REDCR	> DSRC-VU	Выделяет частное окно	Отправляет фрейм с указанием выделенного частного окна.
4	DSRC-VU	> REDCR	Отправляет VST	Отправляет фрейм с VST
5	REDCR	> DSRC-VU	Отправляет GET.request на получение данных в виде атрибута для конкретного EID	
6	DSRC-VU	> REDCR	Отправляет GET.response с запрошенным атрибутом для конкретного EID	Отправляет атрибут (RTMData, OWSDData....) с данными для конкретного EID
7	REDCR	> DSRC-VU	Отправляет GET.request на данные в виде другого атрибута (если это уместно)	
8	DSRC-VU	> REDCR	Отправляет GET.response с запрошенным атрибутом	Отправляет атрибут с данными для конкретного EID
9	REDCR	> DSRC-VU	Подтверждает успешное получение данных	Отправляет команду RELEASE, которая закрывает операцию
10	DSRC-VU		Закрывает операцию	

Пример последовательности операции и содержания фреймов, участвующих в обмене, представлен в пунктах 5.4.7 и 5.4.8.

5.4.44.4.4 Структуры данных

DSC_37 Семантическая структура *данных*, передаваемых через интерфейс DSRC 5,8 ГГц, соответствует описанию, данному в настоящем ~~приложении~~ **подразделе**. Структура этих данных описана в настоящем пункте.

DSC_38 Информационное наполнение (данные RTM) заключается в конкатенации:

1. Данных EncryptedTachographPayload, представляющих собой зашифрованные данные TachographPayload, описанные в ASN.1 в части 5.4.5. Метод шифрования описан в ~~приложении~~ **подразделе 11**.

2. DSRCSecurityData, как указано в ~~приложении~~ **подразделе 11**.

DSC_39 Данные RTM запарашиваются в виде атрибута RTM = 1 и передаются в «контейнер» RTM = 10.

DSC_40 Контекстная метка RTM определяет поддерживаемый стандарт в серии стандартов TARV (RTM соответствует части 9).

Определение модуля ASN.1 для данных DSRC в приложении RTM определяется следующим образом:

```
TarvRtm {iso(1) standard(0) 15638 part9(9)
version1(1)} АВТОМАТИЧЕСКИЕ МЕТКИ ОПРЕДЕЛЕНИЙ
 ::= BEGIN
IMPORTS
– Импорт атрибутов и элементов данных из EFC, которые используются для RTM
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}
– Импортирует параметры функции из определения интерфейса приложения EFC
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}
– Импортирует параметры функции из определения интерфейса приложения EFC
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report-Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}
– Определения функций RTM:
RTM-InitialiseComm-Request ::= BST
RTM-InitialiseComm-Response ::= VST
RTM-DataRetrieval-Request ::= Get-Request (C КОМПОНЕНТАМИ {заполнить(РАЗМЕР(1)), eid,
accessCredentials ABSENT, iid ABSENT, attrIdList})
RTM-DataRetrieval-Response ::= Get-Response {RtmContainer} (C КОМПОНЕНТАМИ {..., eid, iid ABSENT})
RTM-TerminateComm ::= Event-Report-Request {RtmContainer} (C КОМПОНЕНТАМИ {mode (FALSE), eid (0),
eventType (0)})
RTM-TestComm-Request ::= Action-Request {RtmContainer} (C КОМПОНЕНТАМИ {..., eid (0), ActionType
(15), accessCredentials ABSENT, iid ABSENT})
RTM-TestComm-Response ::= Action-Request {RtmContainer} (C КОМПОНЕНТАМИ {..., eid (0), ActionType
(0), iid ABSENT})
– Определения функций RTM:
RtmData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
encryptedTachographPayload ОКТЕТНАЯ СТРОКА (РАЗМЕР(67)) (ОГРАНИЧЕНИЕ { – рассчитанное шифрование
TachographPayload в соответствии с Приложением подразделом 11 добавления –)},
DSRCSecurityData ОКТЕТНАЯ СТРОКА
}
TachographPayload ::= SEQUENCE {
tp15638VehicleRegistrationPlate LPN – Регистрационный знак транспортного средства в
соответствии со структурой данных из ISO 14906, но для приложения RTM LPN устанавливается в 17 байт
(без определителя длины) в соответствии с EN 1550917.
tp15638SpeedingEvent. БУЛЕВО, – 1= Неравномерность в скорости
(см. Приложение Добавление 1C)
tp15638VehicleRegistrationPlate – БУЛЕВО – 1= Неверное использование карточки
(см. Приложение Добавление 1C)
tp15638DriverCard БУЛЕВО, – 0= Указывает на действительную карточку водителя
(см. Приложение 1C)
tp15638CardInsertion БУЛЕВО, – 1= Ввод карточки во время движения
(см. Приложение Добавление 1C)
```

¹⁷ Если LPN содержит **AlphabetIndicator LatinAlphabetNo2** или **LatinCyrillicAlphabet**, специальные символы перераспределяются на блоке дорожного устройства мониторинга с применением специальных правил в соответствии с **Приложением E ISO/DIS 14906.2**.

tp15638MotionDataError	БУЛЕВО, - 1= Ошибка данных о движении
(см. Приложение Добавление 1C)	
tp15638 VehicleMotionConflict	БУЛЕВО, - 1= Противоречивые данные о движении
(см. Приложение Добавление 1C)	
tp156382ndDriverCard	БУЛЕВО, - 1= Противоречивые данные о скорости
(см. Приложение Добавление 1C)	
tp15638DateTachoConnected	БУЛЕВО, - 1 = выбрана другая деятельность; - 0= выбранный режим управления
tp15638LastSessionClosed	БУЛЕВО, - 1= неправильно, 0= правильно, закрыто
tp15638Прерывание электропитания за последние 10 дней	ЦЕЛОЕ ЧИСЛО (0..127), - Перерывы в подаче электропитания
tp15638SensorFault	ЦЕЛОЕ ЧИСЛО (0..255), - eventFaultType согласно словарю данных
- Все последующие типы, связанные со временем, как определено в Приложении Добавлении 1C.	
tp15638TimeAdjustment	ЦЕЛОЕ ЧИСЛО (0..4294967295), - Время последней корректировки времени
tp15638LatestBreachAttempt	ЦЕЛОЕ ЧИСЛО (0..4294967295), - Время последней попытки взлома
tp15638LastCalibrationData	ЦЕЛОЕ ЧИСЛО (0..4294967295), - Время последней калибровки данных
tp15638PrevCalibrationData	ЦЕЛОЕ ЧИСЛО (0..4294967295), - Время предыдущей калибровки данных
tp15638DateTachoConnected	INTEGER(0..4294967295), - Дата подключения тахографа
tp15638CurrentSpeed	ЦЕЛОЕ ЧИСЛО (0..255), - Последняя текущая записанная скорость
tp15638Timestamp	ЦЕЛОЕ ЧИСЛО (0..4294967295) - Временная метка текущей записи2
tp15638LatestAuthenticatedPosition	ЦЕЛОЕ ЧИСЛО R(0..4294967295), - Время последнего аутентифицированного местоположения водителя
tp15638ContinuousDrivingTime	ЦЕЛОЕ ЧИСЛО (0..255), - Время непрерывного управления водителем
tp15638DailyDrivingTimeShift	ЦЕЛОЕ ЧИСЛО (0..255), - Наибольшее суточное время управления водителем за текущую и предыдущую смены RTMPRE
tp15638DailyDrivingTimeWeek	ЦЕЛОЕ ЧИСЛО (0..255), - Наибольшее суточное время управления водителем за текущую и предыдущую смены RTM неделю
tp15638WeeklyDrivingTime	ЦЕЛОЕ ЧИСЛО (0..255), - Время непрерывного управления водителем
tp15638FortnightlyDrivingTime	ЦЕЛОЕ ЧИСЛО (0..255), - Время двухнедельного управления водителем
}	
Rtm-ContextMark ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {	
standardIdentifier StandardIdentifier, - идентификатор части TARV и ее версии	
RtmCommProfile ЦЕЛОЕ ЧИСЛО (0	
C1 (1),	
C2 (2)	
} (0..255) ПО УМОЛЧАНИЮ 1	
}	
RtmTransferAck ::= ЦЕЛОЕ ЧИСЛО {	
Ok (1),	
NoK (2)	
} РАЗМЕР (1..255)	
StandardIdentifier ::= ИДЕНТИФИКАТОР ОБЪЕКТА	
activityDayDistance	
integer [0] ЦЕЛОЕ ЧИСЛО,	
bitstring [1] БИТОВАЯ СТРОКА,	
octetstring [2] ОКТЕТНАЯ СТРОКА (РАЗМЕР (0..127, ...)),	
universalString [3] Универсальная строка,	
beaconId [4] Идентификатор маяка,	
t-apdu [5] T-APDU,	
dsrcApplicationEntityId [6] DSRCApplicationEntityID,	
dsrcAse-Id [7] Dsrc-EID,	
attrIdList [8] Список атрибутов,	
attrList [9] AttributeList{RtmContainer},	
rtmData [10] tmData,	
rtmContextmark [11] Rtm-ContextMark,	
reserved12 [12] NULL,	
reserved13 [13] NULL,	
reserved14 [14] NULL,	
время [15] Время,	
- значения от 16 до 255 зарезервированы для использования в ISO/CEN	
}}	
КОНЕЦ	

5.4.54.4.101 Элементы RtmData, выполняемые действия и определения

DSC_41 Значения данных, которые рассчитывает БУ и которые используются для обновления защищенных данных в DSRC-VU, вычисляются в соответствии с правилами, представленными в таблице 14.3:

Таблица 14.3

Элементы RtmData, выполняемые действия и определения

(1) Элемент данных RTM	(2) Действие, выполняемое БУ	3) Определение данных ASN.1
RTM1 Регистрация транспортных средств Номерной знак	БУ устанавливает значение элемента данных RTM1 <i>tp15638VehicleRegistrationPlate</i> из зарегистрированного значения типа данных <i>VehicleRegistrationIdentification</i> как оно определено в приложении подразделе 1 <i>VehicleRegistrationIdentification</i>	Номерной знак транспортного средства, выраженный в виде строки символов tp15638VehicleRegistrationPlate LPN – Регистрация транспортных средств Номерной знак, взятый из ISO 14906 с ограничением, указанным в EN 15509, который представляет собой последовательность, состоящую из кода страны, за которым следуют в алфавитном порядке указатель, за которым в свою очередь следует непосредственно номерной знак, который всегда состоит из 14 октетов (заполненных нулями), поэтому длина типа LPN по стандарту EN 15509 всегда составляет 17 октетов, из которых 14 — это «реальный номерной знак»
RTM2 Событие, связанное с превышением скорости	БУ генерирует булево значение для элемента данных RTM2 <i>tp15638SpeedingEvent</i> Значение <i>tp15638SpeedingEvent</i> рассчитывается БУ на основе количества событий превышения скорости, зарегистрированных БУ за последние 10 дней, как определено в приложении добавлении 1C Если имеется хотя бы одно событие <i>tp15638SpeedingEvent</i> за последние 10 дней, то значение <i>tp15638SpeedingEvent</i> устанавливается в положение TRUE ELSE, если за последние 10 дней событий не было, <i>tp15638SpeedingEvent</i> устанавливается в положение FALSE	1 (TRUE): если последний случай превышения скорости закончился в течение последних 10 дней или все еще продолжается; Указывает нарушения скорости в течение последних 10 дней с момента возникновения 0 (FALSE): в любом другом случае
RTM3 Вождение без действительной карточки	БУ генерирует булево значение для элемента данных RTM3 <i>tp15638DrivingWithoutValidCard</i> БУ присваивает переменной <i>tp15638DrivingWithoutValidCard</i> значение True, если в данных БУ по крайней мере за последние 10 дней зарегистрировано хотя бы одно событие типа «Вождение без соответствующей карточки», как определено в приложении добавлении 1C ELSE если за последние 10 дней событий не было,	1 (TRUE): если последнее событие «управление без соответствующей карточки» завершилось в течение последних 10 дней или все еще продолжается 0 (FALSE): в любом другом случае. Указывает на использование недействительной карточки
tp15638DrivingWithoutValidCard. БУЛЕВО ЗНАЧЕНИЕ		

(1) Элемент данных RTM	(2) Действие, выполняемое БУ	3) Определение данных ASN.1
RTM4 Действительная карточка водителя	<p>tp15638SpeedingEvent устанавливается в положение FALSE</p> <p>БУ генерирует для элемента данных RTM4 соответствующее булево значение tp15638DriverCard на основе вставленной в считывающее устройство водителя действительной карточки данных, хранящихся в БУ и определенных в приложении добавлении 1</p> <p>Если действительная карточка водителя отсутствует, БУ устанавливает переменную в положение TRUE</p> <p>ELSE, если вставлена действительная карточка водителя, БУ должно установить переменную в положение FALSE</p>	<p>1 (TRUE): если в считывающем устройстве БУ водителя действительная карточка водителя отсутствует</p> <p>Булево значение tp15638DriverCard</p> <p>0 (FALSE): указывает на то, что в считывающем устройстве БУ водителя есть действительная карточка водителя</p>
RTM5 Ввод карточки во время управления	<p>БУ генерирует булево значение для элемента данных RTM5 tp15638CardInsertion</p> <p>БУ присваивает переменной tp15638CardInsertion значение TRUE, если данные БУ зарегистрировали за последние 10 дней было зарегистрировано хотя бы одно событие типа «ввод карточки в БУ во время управления в течение последних 10 дней», как это определено в приложении добавлении 1С</p> <p>ELSE если за последние 10 дней событий не было, tp15638CardInsertion значение устанавливается в положение FALSE</p>	<p>1 (TRUE): если самое последнее событие, указывающее на вставку карты ввод карточки во время движения управления произошло в течение последних 10 дней</p> <p>tp15638CardInsertion БУЛЕОВО ЗНАЧЕНИЕ</p> <p>0 (FALSE): в любом другом случае</p>
RTM6 Ошибочные данные о движении	<p>БУ генерирует соответствующее булево значение для элемента данных RTM</p> <p>БУ присваивает переменной tp15638CardInsertion значение TRUE, если данные БУ зарегистрировали за последние 10 дней было зарегистрировано хотя бы одно событие типа «ошибочные данные о движении ввод карточки в БУ во время управления в течение последних 10 дней», как это определено в приложении добавлении 1С</p> <p>ELSE если за последние 10 дней событий не было,</p>	<p>1 (TRUE): если самое последнее событие типа «ошибочные данные о движении» указывает на то, что данное событие завершилось в течение последних 10 дней или все еще продолжается</p> <p>tp15638MotionDataError БУЛЕОВО ЗНАЧЕНИЕ</p> <p>0 (FALSE): в любом другом случае</p>

(1) Элемент данных RTM	(2) Действие, выполняемое БУ	3) Определение данных ASN.1	
RTM7 Противоречивые данные о движении транспортного средства	<p>tp15638MotionDataError значение устанавливается в положение FALSE</p> <p>БУ генерирует для элемента данных RTM7 соответствующее булево значение</p> <p>БУ присваивает переменной tp15638VehicleMotionConflict значение TRUE, если за последние 10 дней в БУ было зарегистрировано по меньшей мере одно событие типа «ошибочные данные о движении» в БУ было зарегистрировано хотя бы одно событие типа VehicleMotionConflict в течение последних 10 дней (значение '0A'H).</p> <p>ELSE если за последние 10 дней событий не было, tp15638VehicleMotionConflict значение устанавливается в положение FALSE</p>	<p>1 (TRUE): если самое последнее событие типа «противоречивые данные о движении» указывает на то, что данное событие завершилось в течение последних 10 дней или все еще продолжается</p> <p>0 (FALSE): в любом другом случае</p>	tp15638VehicleMotionConflict БУЛЕВО ЗНАЧЕНИЕ
RTM8 Карточка второго водителя	<p>БУ генерирует соответствующее булево значение для элемента данных RTM8 на основе Приложения добавления 1С («Данные о деятельности водителя» — ЭКИПАЖА и ВТОРОГО ВОДИТЕЛЯ)</p> <p>Если введена действительная карточка второго водителя, БУ устанавливает значение RTM8 переменной в положение TRUE</p> <p>ELSE, если вторая действительная карточка водителя не введена, БУ устанавливает переменную в положение FALSE</p>	<p>1 (TRUE): если указывает на введенную в БУ введена действительная карточка второго водителя</p> <p>2 (FALSE): если в БУ VU.inserted отсутствует действительной карточки второго водителя нет</p>	БУЛЕВО значение tp15638DriverCard
RTM9 Текущая деятельность	<p>БУ генерирует для элемента данных RTM9 соответствующее булево значение</p> <p>Если текущая деятельность зарегистрирована в БУ как любая другая деятельность, кроме «УПРАВЛЕНИЯ», как определено в Приложении добавлении 1С, БУ устанавливает значение переменной RTM9 на TRUE</p> <p>ELSE если текущая деятельность записана в БУ как «Управление», БУ должен установить переменную в FALSE</p>	<p>1 (TRUE): = выбран иной вид деятельности;</p> <p>(FALSE): = выбрано управление</p>	tp15638eCurrentActivityDriving БУЛЕВО ЗНАЧЕНИЕ

(1) Элемент данных RTM	(2) Действие, выполняемое БУ		3) Определение данных ASN.1
RTM10 Последний сеанс закрыт	<p>БУ генерирует булево значение для элемента данных RTM10</p> <p>Если последний сеанс использования карточки не был закрыт должным образом, как определено в Приложении добавлении 1С, БУ устанавливает значение переменной RTM10variable на TRUE</p> <p>ELSE если последний сеанс работы с картой был закрыт надлежащим образом, БУ должно установить переменную в FALSE</p>	<p>1 (TRUE): по крайней мере одна из введенных карточек явилась причиной события «неправильное ненадлежащее завершение» последнего сеанса использования карточки</p> <p>0 (FALSE): ни одна из вставленных карточек не явилась причиной события «последний сеанс использования карточки завершен неправильно ненадлежащим образом»</p>	tp15638LastSessionClosed БУЛЕВО ЗНАЧЕНИЕ
RTM11 Источник питания Прерывание электропитания	<p>БУ генерирует соответствующее целое значение для элемента данных RTM 11</p> <p>БУ присваивает переменной tp15638PowerSupplyInterruption значение, равное количеству данных о зарегистрированных самых длительных событиях прерывания подачи электропитания, хранящихся в БУ в течение последних 10 дней, как определено в добавлении 1С в соответствии со статьей 9 Регламента (ЕС) 165/2014 типа «Перерыв в подаче электроэнергии», как определено в приложении 1С</p> <p>Если в течение последних 10 дней БУ не зарегистрировал ни одного события типа «перерыв в электропитании», он устанавливает значение RTM11 на 0</p> <p>ELSE если за последние 10 дней не было случаев прерывания подачи электроэнергии, значение целого числа должно быть установлено на 0</p>	<p>– Номер зарегистрированного источника питания</p> <p>События, связанные с перерывами в течение последних 10 дней е момента возникновения</p>	Tp15638PowerSupplyInterruption ЦЕЛОЕ ЧИСЛО (0..127)
RTM12 Неисправность датчика	<p>БУ генерирует целое число для элемента данных RTM12</p> <p>БУ присваивает переменной sensorFault значение:</p> <p>– 1, если произошло событие типа ‘35’H «неисправность датчика» была зафиксирована устранена в течение последних 10 дней или все еще продолжается</p> <p>– 2, если произошло событие типа «неисправность приемника»</p>	<p>– Неисправность датчика: один октет в соответствии со словарем данных</p>	Tp15638tp15638sSensorFault ЦЕЛОЕ ЧИСЛО (0..255)

(1) Элемент данных RTM	(2) Действие, выполняемое БУ	3) Определение данных ASN.1
RTM13 Корректировка времени	<p>ГНСС» (внутренняя или внешняя со значениями перечисления '51'Н '36'Н или '52'Н '37'Н) была зафиксирована устранена в течение последних 10 дней или все еще продолжается</p> <p>– 3, если событие типа '53'Н External '0E'Н «Ошибка связи с внешним устройством связи GNSS» завершилось в течение последних 10 дней или все еще продолжается</p> <p>– 4 Если были зарегистрированы неисправности датчика и приемника GNSS за последние 10 дней были устранены или все еще продолжают</p> <p>– 5 Если и неисправность датчика, и ошибка связи с внешним устройством ГНСС были зарегистрированы устранены в течение последних 10 дней или все еще продолжают</p> <p>– 6 Если и неисправность приемника, и ошибка связи с внешним устройством ГНСС были зарегистрированы устранены в течение последних 10 дней или все еще продолжают</p> <p>– 7 Если все три неисправности датчика были зарегистрированы устранены за последние 10 дней или все еще продолжают</p> <p>ИЛИ присваивается значение 0 Если за последние 10 дней в момент возникновения не было зарегистрировано устранено ни одно событие или если оно все еще продолжается, БУ устанавливает значение RTM12 на 0</p> <p>БУ генерирует целочисленное значение (timeReal из Добавления подраздела 1) для элемента данных RTM13 на основе наличия данных корректировки времени, как определено в Приложении добавлении 1С</p> <p>БУ присваивает устанавливает значение RTM13 на то время, когда была произведена последняя корректировка данных времени</p> <p>ELSE Если событие «Корректировка времени», как это</p>	<p>oldTimeValue самой ближайшей последней корректировки времени</p> <p>tp15638TimeAdjustment ЦЕЛОЕ ЧИСЛО (0..4294967295)</p>

(1) Элемент данных RTM	(2) Действие, выполняемое БУ	3) Определение данных ASN.1
RTM14	определено в приложении добавлении 1С , отсутствует в данных БУ, оно должно установить значение RTM13 на 0	tp15638LatestBreachAttempt ЦЕЛОЕ ЧИСЛО(0..4294967295)
Попытка нарушения системы защиты	БУ генерирует целочисленное значение (timeReal из добавления подраздела 1) для элемента данных RTM14 в связи с наличием события типа «попытка нарушения системы защиты», как определено в приложении добавлении 1С	Время начала самого последнего сохраненного события , связанного с попыткой нарушения безопасности — Значение по умолчанию =0x00FF
RTM15	БУ должно установить значение времени последнего события типа «попытка нарушения системы защиты», зарегистрированного БУ ELSE Если в данных БУ есть событие «попытка нарушения системы защиты», как это определено в добавлении 1С , он устанавливает значение RTM14 на 0x00FF.	tp15638LastCalibrationData ЦЕЛОЕ ЧИСЛО (0..4294967295)
Последняя калибровка	БУ генерирует целочисленное значение (timeReal из добавления подраздела 1) для элемента данных RTM15 на основе наличия данных, касающихся последней калибровки, как это определено в приложении добавлении 1С и подразделе 1 БУ устанавливает значение времени двух последних калибровок (RTM15 на oldTimeValue последней записи калибровки и RTM16), которые установлены в VuCalibrationData, определенных в подразделе добавлении 1 Если калибровка не проводилась, БУ устанавливает значение или RTM15 на 0 реального времени последней записи калибровки	Прежнее значение времени самой последней записи калибровки
RTM16	БУ генерирует целочисленное значение (timeReal из добавления подраздела 1) для элемента данных RTM16 на основе записей калибровки, предшествующих последней калибровке ELSE если предыдущая калибровка не проводилась, БУ устанавливает значение RTM16 на значение oldTimeValue записи калибровки, предшествующей последней калибровке	tp15638PrevCalibrationData ЦЕЛОЕ ЧИСЛО(0..4294967295)
Предыдущая калибровка		oldTimeValue предыдущей записи калибровки, предшествующей самой последней записи калибровки data

(1) Элемент данных RTM	(2) Действие, выполняемое БУ	3) Определение данных ASN.1	
RTM17 Дата подключения тахографа	<p>Если предшествующей калибровки не было, БУ устанавливает значение RTM16 на 0</p> <p>Для элемента данных RTM17 БУ генерирует целочисленное значение (timeReal из приложения добавления 1) для элемента данных RTM17</p> <p>БУ устанавливает значение RTM17 на дату времени первой калибровки и первоначальной установки БУ в данном транспортном средстве</p> <p>БУ извлекает эти данные из файла VuCalibrationData (приложение добавление 1) из записи vuCalibrationRecords на основании CalibrationPurpose: '03'H</p> <p>Если калибровка не проводилась, БУ устанавливает значение RTM17 на 0</p>	Дата первой калибровки БУ на данном транспортном средстве подключения тахографа	tp15638DateTachoConnected ЦЕЛОЕ ЧИСЛО(0..4294967295)
RTM18 Текущая скорость	<p>БУ генерирует соответствующее целочисленное значение для элемента данных RTM18</p> <p>БУ устанавливает значение параметра RTM18 на последнюю текущую зарегистрированную скорость на момент последнего обновления RtmData</p>	Последняя текущая зарегистрированная скорость	tp15638CurrentSpeed ЦЕЛОЕ ЧИСЛО (0..255)
RTM19 Временная метка	<p>Для элемента данных RTM19 БУ генерирует целочисленное значение для элемента данных RTM19 (timeReal из приложения подраздела 1)</p> <p>БУ устанавливает значение параметра RTM19 на время самого последнего обновления RtmData.</p>	Временная метка текущей записи TachographPayload	tp15638Timestamp ЦЕЛОЕ ЧИСЛО(0..4294967295)
RTM20 Время, в которое было доступно последнее аутентифици- рованное местоположение транспортного средства	<p>БУ генерирует целочисленное значение (timeReal из добавления 1) для элемента данных RTM20</p> <p>БУ устанавливает значение RTM20 на время, в которое было доступно по приемнику GNSS последнее аутентифицированное положение транспортного средства</p> <p>Если аутентифицированное положение транспортного средства в какое-то время было недоступно по приемнику</p>	Временная метка последнего аутентифицированного местоположения транспортного средства	tp15638LatestAuthenticated Position ЦЕЛОЕ ЧИСЛО(0..4294967295)

(1) Элемент данных RTM	(2) Действие, выполняемое БУ		3) Определение данных ASN.1
RTM21 Время непрерывного управления	GNSS, БУ устанавливает значение RTM20 на 0 БУ генерирует целочисленное значение для элемента данных RTM21 БУ устанавливает значение RTM21 на текущее время непрерывного управления водителя	Время непрерывного управления водителя, закодированное как целочисленное значение Длина: 1 байт Разрешение: 2 минуты/бит Смещения нет Диапазон данных: от 0 до 250 Значение 250 указывает на то, что время непрерывного управления водителя равно или превышает 500 минут Значения 251–254 не используются. Значение 255 указывает на то, что информация недоступна	tp15638ContinuousDrivingTime ЦЕЛОЕ ЧИСЛО (0..255)
RTM22 Самое продолжительное ежедневное время управления в текущей и предыдущей смене RTM, рассчитанное в соответствии с приложением к подразделу 14	БУ генерирует целочисленное значение для элемента данных RTM22 БУ устанавливает значение RTM22 на более продолжительное из двух ежедневных периодов времени управления водителя, относящихся либо к текущей, либо к предыдущей смене RTM	Время непрерывного управления водителя, закодированное как целочисленное значение Длина: 1 байт Разрешение: 4 минуты/бит Смещения нет Диапазон данных: от 0 до 250 Значение 250 указывает на то, что время ежедневного управления водителя равно или превышает 1000 минут Значения 251–254 не используются Значение 255 указывает на то, что информация недоступна	tp15638ContinuousDrivingTime ЦЕЛОЕ ЧИСЛО (0..255)
RTM23 Самое продолжительное ежедневное время управления в течение текущей недели,	БУ генерирует целое численное значение для элемента данных RTM23 БУ устанавливает значение RTM23 на самое продолжительное ежедневное время управления водителя,	Время ежедневного непрерывного управления водителя, закодированное как целочисленное значение	tp15638ContinuousDrivingTime ЦЕЛОЕ ЧИСЛО (0..255),

(1) Элемент данных RTM	(2) Действие, выполняемое БУ	3) Определение данных ASN.1
рассчитанное в соответствии с приложением к подразделу 14	которое является либо текущей сменой RTM, либо любой завершенной сменой RTM, которая началась или закончилась на текущей неделе	<p>Длина: 1 байт</p> <p>Разрешение: 4 минуты/бит</p> <p>Смещения нет</p> <p>Диапазон данных: от 0 до 250</p> <p>Значение 250 указывает на то, что время ежедневного управления водителем равно или превышает 1000 минут</p> <p>Значения 251–254 не используются.</p> <p>Значение 255 указывает на то, что информация недоступна</p>
RTM24 Самое продолжительное ежедневное время управления в течение текущей недели, рассчитанное в соответствии с приложением к подразделу 14	БУ генерирует целочисленное значение для элемента данных RTM24 БУ устанавливает значение RTM24 на еженедельное время непрерывного управления водителем	<p>Время управления водителем, закодированное как целочисленное значение</p> <p>Длина: 1 байт</p> <p>Разрешение: 20 минуты/бит</p> <p>Смещения нет</p> <p>Диапазон данных: от 0 до 250</p> <p>Значение 250 указывает на то, что время еженедельного управления водителем равно или превышает 5000 минут</p> <p>Значения 251–254 не используются</p> <p>Значение 255 указывает на то, что информация недоступна</p> <p>tp15638ContinuousDrivingTime ЦЕЛОЕ ЧИСЛО (0..255)</p>
RTM25 Самое продолжительное двухнедельное время управления, рассчитанное в соответствии с приложением к подразделу 14	БУ генерирует целочисленное значение для элемента данных RTM25 БУ устанавливает значение RTM25 на двухнедельное время управления водителем	<p>Время двухнедельного управления водителем, закодированное как целочисленное значение</p> <p>Длина: 1 байт</p> <p>Разрешение: 30 минут/бит</p> <p>Смещения нет</p> <p>Диапазон данных: от 0 до 250</p> <p>tp15638ContinuousDrivingTime ЦЕЛОЕ ЧИСЛО (0..255)</p>

(1) Элемент данных RTM	(2) Действие, выполняемое БУ	3) Определение данных ASN.1
		<p>Значение 250 указывает на то, что время двухнедельного управления водителем равно или превышает 7500 минут</p> <p>Значения 251–254 не используются</p> <p>Значение 255 указывает на то, что информация недоступна</p>

Примечание: RTM22, RTM23, RTM24 и RTM25 рассчитываются в соответствии с приложением к данному подразделу.

5.4.64.4.102 Механизм передачи данных

- DSC_42 Рабочие данные, описанные выше, запрашиваются REDCR после этапа инициализации и затем передаются *DSRC-VU* в выделенное окно. Для извлечения данных REDCR использует команду GET.
- DSC_43 Для всех обменов DSRC данные кодируются с использованием PER (Правила кодирования уплотненных данных) UNALIGNED, кроме **TachographPayload** и **OwsPayload**, которые кодируются с использованием правил OER (правила кодирования октетов), определенных в ISO/IEC 8825-7, Rec. ITU-T X.696.

5.4.74.4.103 Детальное описание операции DSRC

- DSC_44 Инициализация осуществляется в соответствии с DSC_44-DSC_48 и таблицами 14.4–14.9. На этапе инициализации REDCR начинает отправлять фрейм, содержащий BST (таблицу использования радиомаяков) в соответствии с EN 12834 и EN 13372, 6.2, 6.3, 6.4 и 7.1 с настройками, указанными в следующей таблице 14.4.

Таблица 14.4
Инициализация. Настройки фрейма VST

Поле	Настройки
Идентификатор ссылки	Широковещательный адрес
Идентификатор радиомаяка	В соответствии с EN 12834
Время	В соответствии с EN 12834
Профиль	Расширение отсутствует, используется 0 или 1
Обязательные приложения	Расширение отсутствует, EID отсутствует, Параметр отсутствует, AID = 2 Freight&Fleet Freight&Fleet
Необязательные приложения	Отсутствуют
Количество профилей	Нет расширения, количество профилей в списке = 0
Заголовок дробления	Дробления нет

Практический пример настроек, перечисленных в таблице 14.4 с указанием битовых шифров, приводится в следующей таблице 14.5.

Таблица 14.5

Инициализация — пример содержимого фрейма BST

Октет #	Атрибут/Поле	Биты в октете	Описание
1	FLAG	0111 1110	Стартовый флаг
2	Broadcast ID	1111 1111	Адрес вещания
3	MAC Control Field	1010 0000	Командный PDU
4	LLC Control field	0000 0011	Команда UI пользовательского
5	Fragmentation header	1xxx x001	Дробления нет
6	BST	1000	Запрос на инициализацию
	SEQUENCE { OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	Необязательные приложения отсутствуют
		xxx	Идентификатор изготовителя
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727) }	xxx	27-битный идентификатор доступен для изготовителя
9		xxxx xxxx	
10		xxxx xxxx	
11		xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	32-битный UNIX реального
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,...)	0000 0000	Расширения нет. Пример профиля 0
17	MandApplications SEQUENCE (SIZE(0..127,...)) OF {	0000 0001	Расширения нет, Количество mandApplications = 1
18	SEQUENCE { OPTION indicator OPTION indicator AID DSRCApplicationEntityID } }	0	EID отсутствует
		0	Параметр отсутствует
		00 0010	Расширения нет. AID = 2
19	ProfileList SEQUENCE (0..127,...) OF Profile }	0000 0000	Расширения нет, количество профилей в списке = 0
20	FCS	xxxx xxxx	Последовательность проверки фреймов
21		xxxx xxxx	
22	Флаг	0111 1110	Конечный флаг

DSC_45 DSRC-VU запрашивает, после получения BST, частное окно, как указано в EN 12795 и EN 13372, 7.1.1, без определенных настроек RTM. В таблице 14.6 приводится пример битового шифра.

Таблица 14.6

Инициализация. Содержание запроса фрейма на выделение частного окна

Октет #	Атрибут/Поле	Биты в октете	Описание
1	ФЛАГ	0111 1110	Начальный флаг
2	Частный LID	xxxx xxxx	Адрес соединения конкретного DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Поле управления MAC	0110 0000	Выделение частного окна
7	FCS	xxxx xxxx	Последовательность проверки фреймов
8		xxxx xxxx	
9	Флаг	0111 1110	Конечный флаг

DSC_47 DSRC-VU, получив выделенное частное окно, передает свою VST (таблицу обслуживания транспортного средства), как указано в EN 12834 и EN 13372, 6.2, 6.3, 6.4 и 7.1 с настройками, представленными в таблице 14.8, с использованием выделенного окна передачи.

Таблица 14.8

Инициализация. Настройки фрейма VST

Поле	Настройки
Частный LID	В соответствии с EN 12834
Параметры VST	Fill=0, затем для каждого поддерживаемого приложения: EID присутствует, параметр присутствует, AID = 2, EID, сгенерированный OBU
Параметр	Расширения нет, содержит контекстную метку RTM
ObeConfiguration	Необязательное поле ObeStatus может присутствовать, но не должно использоваться REDCR
Дробление	Дробления нет
Настройки уровня 2	Команда PDU, команда пользовательского интерфейса

DSC_48 DSRC-VU поддерживает приложение «Freight and Fleet», определяемое по идентификатору приложения '2'. Могут поддерживаться и другие идентификаторы приложений, но в данной VST их нет, так как BST требует лишь AID = 2. В поле приложений содержится перечень поддерживаемых вариантов приложений в DSRC-VU. В случае каждого поддерживаемого приложения дается ссылка на соответствующий стандарт, которая состоит из контекстной метки Rtm в виде идентификатора объекта (OBJECT IDENTIFIER), представляющего собой соответствующий стандарт, его части (9 в случае RTM) и, возможно, его версию, а также EID, который генерируется DSRC-VU с учетом данного варианта приложения.

Практический пример настроек, перечисленных в таблице 14.8 с указанием битовых шифров, приводится в следующей таблице 14.9.

Таблица 14.9

Инициализация — пример содержимого фрейма VST

Октет #	Атрибут/Поле	Биты в октете	Описание
1	FLAG	0111 1110	Стартовый флаг
2	Private LID	xxxx xxxx	Адрес соединения конкретного DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	Командный PDU
7	LLC Control field	0000 0011	Команда пользовательского интерфейса
8	Fragmentation header	1xxx x001	Дробления нет
9	VST SEQUENCE { Fill BIT STRING (SIZE(4))	1001	Ответ на инициализацию
		0000	Не используется и установлен на 0
10	Profile INTEGER (0..127,...)	0000 0000	Расширения нет. Пример профиля 0 Без продления, 1 приложение
11		0000 0001	
12	SEQUENCE { OPTION indicator OPTION indicator AID DSRCApplicationEntityID	1	EID присутствует
		1	Параметр присутствует
		00 0010	Расширения нет. AID= 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Определяется на уровне OBU и идентифицирует экземпляр приложения
14	Parameter Container {	0000 0010	Расширения нет, выбор контейнера = 02, октетная строка
15		0000 0110	Расширения нет, длина контекстной метки Rtm = 6
16	Rtm-ContextMark ::= SEQUENCE { standardIdentifier	0000 0101	Первый октет - 05H, что является его длиной. Последующие 5 октетов кодируют идентификатор объекта поддерживаемого стандарта, часть и версию. {ISO (1) Стандарт (0) TARV (15638) часть9(9) Вариант2 (2).
17		0010 1000	
18		1111 1010	
19		0001 0110	
20		0000 1001	
21		0000 0010	
22	ObeConfiguration Sequence { OPTION indicator	0	ObeStatus не присутствует
	EquipmentClass INTEGER (0..32767)	xxx xxxx	Это поле используется для переноса указания изготовителя о версии программного/аппаратного обеспечения интерфейса DSRC
23		xxxx xxxx	
24	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Идентификатор изготовителя для DSRC-VU, как описано в ISO 14816 Register
25		xxxx xxxx	
26	FCS	xxxx xxxx	Последовательность проверки фреймов
27		xxxx xxxx	
28	Флаг	0111 1110	Конечный флаг

Октет#	Атрибут/поле	Биты в октете	Описание
1	ФЛАГ	0111 1110	Стартовый флаг
2	Частный LID	xxxx/x/xx/xx	Адрес соединения конкретного DSRC БУ
3		xxxx/x/xx/xx	
4		xxxx/x/xx/xx	
5		xxxx/x/xx/xx	
6	Поле управления MAC	1100-0000	
7	Поле управления LLC	0000-0011	Команда пользовательского интерфейса
8	Заголовок дробления	1xxx-x001	Дробления нет
9	VST	1001	Ответ на инициализацию
	SEQUENCE { Fill BIT STRING (SIZE4)}	0000	Не используется и установлен на 0
10	Профиль INTEGER (0...127,...)	0000-0000	Расширения нет. Пример профиля 0
11		0000-0001	Без продления, 1 приложение
12	SEQUENCE { Индикатор-Варианта Индикатор-Варианта AID-DSRCApplicationEntityID }	1	EID присутствует
		1	Параметр присутствует
		00-0010	Расширения нет. AID=2 Freight&Fleet
13	EID-Dsrc-EID	xxxx/x/xx/xx	Определяется в рамках OBU и идентифицирует экземпляр приложения.
14	Parameter-Container {	0000-0010	Расширения нет. Выбор контейнера—02, октетная строка
15		0000-1000	Расширения нет, длина контекстной метки Rtm=8
16	Rtm-ContextMark ::= SEQUENCE { StandardIdentifier	0000-0110	Последующие 5 октетов кодируют идентификатор объекта поддерживаемого стандарта, часть и версию. {ISO (1) Standard (0) TARV (15638) part9(9) Version2 (2)}
17	StandardIdentifier	0000-0110	
18		0010-1000	Первый октет—06H, который является идентификатором объекта. Первый октет—05H, что является его длиной.
19		1000-0000	Последующие 6 октетов кодируют идентификатор объекта примера
20		1111-1010	Проеьба обратить внимание, что
21		0001-0110	присутствует только один элемент
22		0000-1001	последовательности (необязательный элемент RtmCommProfile опущен)
23		0000-0001	
24	Последовательность конфигурации ObeConfiguration {Индикатор ВАРИАНТА EquipmentClass INTEGER (0..3276 7)	0 xxxx xxxx	ObeStatus не присутствует

Октет #	Атрибут/поле	Биты в октете	Описание
25		xxxx/x/xx/xx	
26	ManufacturerId INTEGER (0..65535)	xxxx/x/xx/xx	Идентификатор изготовителя для DSRC-VU, как описано в ISO 14816 Register
27		xxxx-xxxx	
28		xxxx-xxxx	Последовательность проверки фреймов
29		xxxx/x/xx/xx	
30	Флаг	0111 1110	Конечный флаг

DCS_49 Затем REDCR считывает данные, выдавая команду GET по аналогии с командой GET, представленной в EN 13372, 6.2, 6.3, 6.4 и EN 12834, а настройки — как указано в таблице 14.10.

Таблица 14.10

Представление — Настройки фрейма запроса GET

Поле	Настройки
Идентификатор инвокера (IID)	Отсутствует
Идентификатор ссылки (LID)	Адрес соединения конкретного DSRC-VU
Измерение расстояния мерной цепью	Нет
Идентификатор элемента (EID)	Как указано в VST. Расширения нет
Учетные данные доступа	Нет
Список атрибутов	Нет расширения, 1 атрибут, AttributeID = 1 (RtmData)
Дробления нет	Нет
Настройки уровня 2	Команда PDU, опрашиваемая команда ACn

Таблица 14.11 содержит пример считывания данных RTM.

Таблица 14.11

Презентация — Пример кадра запроса на получение

Октет #	Атрибут/Поле	Биты в октете	Описание
1	ФЛАГ	0111 1110	Стартовый флаг
2	Частный LID	xxxx xxxx	Адрес соединения конкретного DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Поле управления MAC	1010 s000	Командный PDU
7	Поле управления LLC	n111 0111	Опрашиваемая команда ACn, n бит

Октет #	Атрибут/Поле	Биты в октете	Описание
8	Заголовок дробления	1xxx x001	Дробления нет
9	Get.request SEQUENCE { OPTION indicator OPTION indicator OPTION indicator Fill BIT STRING(SIZE(1))	0110 0 0 1 0	Получить запрос Учетные данные доступа отсутствуют IID отсутствует AttributeIdList присутствует Установить на 0
10	EID INTEGER(0..127,...)	xxxx xxxx	EID экземпляра приложения RTM Как указано в VS Расширения нет
11	AttributeIdList SEQUENCE OF { AttributeId	0000 0001	Расширения нет, число атрибутов = 1
12		0000 0001	AttributeId=1, RtmData. Расширения нет
13	FCS	xxxx xxxx	Последовательность проверки фреймов
14		xxxx xxxx	
15	Флаг	0111 1110	Конечный флаг

DSC_50 DSRC-VU, получив запрос GET, отправляет ответ GET с запрошенными данными, соответствующий ответу GET, определенному в EN 13372, 6.2, 6.3, 6.4 и EN 12834, с настройками, указанными в таблице 14.12.

Таблица 14.12

Представление — настройки фрейма запроса GET

Поле	Настройки
Идентификатор вызова (IID)	Отсутствует
Идентификатор ссылки (LID)	В соответствии с EN 12834
Сцепление блоков	Нет
Идентификатор элемента (EID)	Как указано в VST
Учетные данные доступа	Нет
Дробление	Нет
Настройки уровня 2	PDU ответа, ответ доступен и команда принята, команда AСп

В таблице 14.13 приведен пример считывания данных RTM.

Таблица 14.13

Представление — Пример содержания фрейма ответа

Оклет #	Атрибут/Поле	Биты в окете	Описание
1	ФЛАГ	0111 1110	Стартовый флаг
2	Частный LID	xxxx xxxx	Адрес соединения конкретного DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Поле управления MAC	1101 0000	PDU ответа
7	Поле управления LLC	n111 0111	Ответ доступен, команда ACn n бит
8	Поле Статус LLC	0000 0000	Ответ доступен и команда принята
9	Заголовок дробления	1xxx x001	Дробления нет
10	Get.response	0111	Ответ на запрос
	SEQUENCE {		
	OPTION indicator	0	IID отсутствует
	OPTION indicator	1	IID присутствует
	OPTION indicator	0	Статус возврата отсутствует
	Fill BIT STRING(SIZE(1))	0	Не используется
11	EID INTEGER(0..127,...)	xxxx xxxx	Ответ из приложения RTM Объект: Расширения нет
12	AttributeList SEQUENCE OF {	0000 0001	Расширения нет, количество профилей в списке = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Расширения нет, AttributeId=1 (RtmData)
14	AttributeValue CONTAINER { }}}	0000 1010	Расширения нет, Выбор контейнера = 1010
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
...		...	
n		kkkk kkkk	
n + 1	FCS	xxxx xxxx	Последовательность проверки фреймов
n + 2		xxxx xxxx	
n + 3	Флаг	0111 1110	Конечный флаг

DSC_51 Затем REDCR закрывает связь, выдавая EVENT_REPORT, команду RELEASE в соответствии с EN 13372, 6.2, 6.3, 6.4 и EN 12834 ,7.3.8, без конкретных настроек RTM. В таблице 14.14 показан пример битового шифра команды RELEASE.

Таблица 14.14

Завершение — Содержание фрейма EVENT_REPORT (Сброс)

Октет #	Атрибут/Поле	Биты в октете	Описание
1	ФЛАГ	0111 1110	Стартовый флаг
2	Частный LID	xxxx xxxx	Адрес соединения конкретного DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Поле управления MAC	1000 s000	Фрейм содержит командный LPDU
7	Поле управления LLC	0000 0011	Команда пользовательского интерфейса
8	Заголовок дробления	1xxx x001	Дробления нет
9	EVENT_REPORT.request	0010	EVENT_REPORT (Сброс)
	SEQUENCE {		
	OPTION indicator	0	Учетные данные доступа отсутствуют
	OPTION indicator	0	Параметр события отсутствует
	Mode BOOLEAN	0	EID Отсутствует
		0	Ответ не ожидается
10	EID INTEGER (0..127,...)	0000 0000	Расширения нет, EID = 0 (Система)
11	EventType INTEGER (0..127,...) }	0000 0000	Тип события 0 = Сброс
12	FCS	xxxx xxxx	Последовательность проверки фреймов
13		xxxx xxxx	
14	Флаг	0111 1110	Конечный флаг

DSC_52 Ответ DSRC-VU на команду Сброс не ожидается. После этого связь закрывается.

5.4.84.4104 Детальное описание операции по проверке DSRC

DSC_53 Полные испытания, включающие в себя защиту данных, проводятся, как описано в ~~приложении~~ **подразделе 11** «Общие механизмы безопасности», уполномоченными лицами с доступом к процедурам защиты, пользуясь в этих целях обычной командой GET, как описано выше.

DSC_54 Испытания на ввод в эксплуатацию и периодические проверки, требующие расшифровки и понимания содержания расшифрованных данных, проводятся так, как описано в ~~приложении~~ **подразделе 11** «Общие механизмы безопасности» и ~~приложении~~ **подразделе 9** «Перечень минимальных требуемых испытаний на утверждение типа».

Вместе с тем базовую связь DSRC можно проверить с помощью команды ECHO. Такие проверки могут быть необходимы при вводе в эксплуатацию, периодических

инспекциях или по требованию компетентного контрольного органа ~~или на основании Регламента (ЕС) № 165/2014 (см. 6 ниже)~~.

DSC_55 Для проведения такой основной проверки связи в ходе сеанса REDCR выдает команду ECHO, т. е. после успешного завершения этапа инициализации. Таким образом, последовательность действий в этом случае похожа на последовательность контрольного запроса:

↪ Этап 1 REDCR направляет таблицу использования радиомаяков (BST), в которую включены идентификаторы приложений (AIDs) в перечне поддерживаемых функций. В приложениях RTM это будет просто функция со значением AID = 2.

DSRC-VU оценивает полученную BST и, если устанавливает, что BST запрашивает приложение Freight&Fleet (AID = 2), DSRC-VU выдает ответ. Если REDCR не предлагает AID = 2, то DSRC-VU завершает операцию с REDCR.

↪ Этап 2 DSRC-VU передает запрос на выделение частного окна.

↪ Этап 3 REDCR отправляет сообщение о выделении частного окна.

↪ Этап 4 DSRC-VU использует выделенное частное окно для передачи своей таблицы обслуживания транспортного средства (VST). В такой VST представлен перечень всех различных вариантов инстанцирования приложений, которые данное DSRC-VU поддерживает в рамках AID=2. Различные варианты инстанцирования определяются при помощи уникальных EID, каждый из которых связан со значением параметра с указанием на вариант поддерживаемого приложения.

↪ Этап 5 Затем REDCR анализирует предложенную VST и прерывает связь (RELEASE), так как больше в VST нет никакой нужды (т. е. получает VST из DSRC-VU, которое не является RTM БУ), или, если получает соответствующую VST, запускает инстанцирование приложения.

↪ Этап 6 REDCR выдает команду (ECHO) конкретному DSRC-VU и выделяет частное окно.

↪ Этап 7 DSRC-VU использует выделенное частное окно для направления фрейма с ответом ECHO.

В таблице ниже приводится практический пример сеанса обмена командой ECHO.

DSC_56 Инициализация осуществляется в соответствии с (DSC_44-DSC_48) и таблицами 14.4–14.9.

DSC_57 Затем REDCR выдает команду ACTION, ECHO в соответствии с ISO 14906, содержащую 100 октетов данных и без конкретных настроек RTM. Таблица 14.15 отражает содержание фрейма, который передает REDCR.

Таблица 14.15

Пример фрейма запроса ACTION, ECHO

Октет #	Атрибут/Поле	Биты в октете	Описание
1	ФЛАГ	0111 1110	Стартовый флаг
2	Частный LID	xxxx xxxx	Адрес соединения конкретного DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Поле управления MAC	1010 s000	Командный PDU
7	Поле управления LLC	n111 0111	Опрашиваемая команда ACn, n бит

Октет #	Атрибут/Поле	Биты в октете	Описание
8	Заголовок дробления	1xxx x001	Дробления нет
9	ACTION.request SEQUENCE {	0000	Запрос на действия (ECHO)
	OPTION indicator	0	Учетные данные доступа отсутствуют
	OPTION indicator	1	Параметр присутствует
	OPTION indicator	0	ИД отсутствует
	Режим BOOLEAN	1	Ответ ожидается
10	EID INTEGER (0..127,...)	0000 0000	Расширения нет, EID = 0 (Система)
11	ActionType INTEGER (0..127,...)	0000 1111	Расширения нет, тип действия: Запрос ECHO
12	ActionParameter CONTAINER {	0000 0010	Расширения нет, Выбор контейнера = 1010.
13		0110 0100	Расширения нет. Длина строки = 100 октетов
14		xxxx xxxx	Данные подлежат отображению
...	}}	...	
113		xxxx xxxx	
114	FCS	xxxx xxxx	Последовательность проверки фреймов
115		xxxx xxxx	
116	Флаг	0111 1110	Конечный флаг

DSC_58 *DSRC-VU*, получив запрос ECHO, передает ответ ECHO из 100 октетов данных, отражая полученную команду в соответствии с ISO 14906, без конкретных настроек RTM. В таблице 14.16 приводится пример кодирования на уровне битов.

Таблица 14.16
Пример фрейма ответа ACTION, ECHO

Октет #	Атрибут/Поле	Биты в октете	Описание
1	ФЛАГ	0111 1110	Стартовый флаг
2	Частный LID	xxxx xxxx	Адрес соединения конкретного БУ
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Поле управления MAC	1101 0000	PDU ответа
7	Поле управления LLC	n111 0111	Опрашиваемая команда ACn, n бит
8	Поле статуса LLC	0000 0000	Ответ доступен
9	Заголовок дробления ?Дробление	1xxx x001	Дробления нет

Октет #	Атрибут/Поле	Биты в октете	Описание
10	ACTION.response SEQUENCE {	0001	Ответные ДЕЙСТВИЯ (ECHO)
	OPTION indicator	0	ID отсутствует
	OPTION indicator	1	Параметр присутствует
	OPTION indicator	0	Статус возврата отсутствует
	Fill BIT STRING (SIZE (1))	0	Не используется
11	EID INTEGER (0..127,...)	0000 0000	Расширения нет, EID = 0 (Система)
12	ResponseParameter CONTAINER {	0000 0010	Расширения нет, выбор контейнера = 2
13		0110 0100	Расширения нет Длина строки = 100 октетов
14		xxxx xxxx	Отображенные данные
...		
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Последовательность проверки фреймов
115		xxxx xxxx	
116	Флаг	0111 1110	Конечный флаг

5.54.5 ~~Поддержка Директивы 2015/71/ЕС (текст удален)~~ Зарезервировано для использования в будущем

5.64.5.7 Механизмы передачи Передача данных между DSRC_VU и БУ

~~DSC_64 — Механизмы передачи данных OWS между устройством мониторинга и объектом DSRC на транспортном средстве должно быть таким же, как и в случае данных RTM (см. 4.4.102).~~

~~DSC_65 — Передача данных между платформой, собирающей данные о максимальных показателях веса, и системой DSRC на транспортном средстве должна быть основана на физическом соединении, интерфейсах и протоколе, определенных в разделе 4.6.~~

~~4.6 Передача данных между DSRC_VU и БУ~~

5.6.14.6.1 Физическое соединение и интерфейсы

DSC_66 Соединение между БУ и DSRC-VU может осуществляться при помощи физического кабеля или беспроводной связи ближнего действия на основе Bluetooth v4.0 BLE.

DSC_67 Вне зависимости от выбора физического соединения интерфейса, необходимо соблюдать следующие требования:

DSC_68 а) Для того чтобы можно было привлекать различных подрядчиков для поставок БУ и DSRC-VU, а также различных партий DSRC-VU, соединение между БУ и DSRC-VU, которое не является встроенным, должно представлять собой открытое стандартное соединение. БУ соединяется с DSRC-VU либо

- i) с помощью фиксированного кабеля длиной не менее 2 метров, с использованием прямого соединителя DIN 41612 H11, утвержденного 11-контактного штекерного соединителя DSRC-VU, который подходит к соответствующему утвержденному гнездовому разъему DIN/ISO со стороны БУ;
 - ii) с помощью энергосберегающей системы Bluetooth Low Energy (BLE);
 - iii) с помощью соединения, соответствующего стандарту ISO 11898 или SAE J1939;
- DSC_69 b) определение интерфейсов и соединения между БУ и DSRC-VU должно поддерживать команды протокола приложения, определенные в пункте 5.6.2; и
- DSC_70 c) БУ и DSRC-VU должны поддерживать работу по передаче данных через соединение в части производительности и питания.

5.6.24.6.2 Протокол приложения

DSC_71 Протокол приложения между устройством удаленной связи БУ и DSRC-VU отвечает за периодическую передачу данных удаленной связи из БУ в DSRC.

DSC_72 В этой связи необходимо выделить следующие пять категорий:

1. Инициализация канала связи — Запрос
2. Инициализация канала связи — Ответ
3. Передача данных с идентификатором приложения RTM и полезным информационным наполнением, определяемым по данным RTM
4. Подтверждение получения данных
5. Прекращение канала связи — Запрос
6. Прекращение канала связи — Ответ

DSC_73 В ASN1.0 предыдущие команды можно определить следующим образом:

ОПРЕДЕЛЕНИЯ протокола DT удаленной связи ::= НАЧАЛО

```
RCDT-Инициализация канала связи — Запрос ::= SEQUENCE { LinkIdentifier INTEGER
}
```

```
RCDT-Инициализация канала связи — Ответ ::= SEQUENCE { LinkIdentifier INTEGER
ответ БУЛЕВО ЗНАЧЕНИЕ
}
```

```
RCDT- Send Data ::= SEQUENCE {
LinkIdentifier INTEGER,
DataTransactionId INTEGER, RCDTData
SignedTachographPayload
}
```

```
RCDTData Acknowledgment ::= SEQUENCE {
LinkIdentifier INTEGER, DataTransactionId
INTEGER,
ответ БУЛЕВО ЗНАЧЕНИЕ
}
```

```

RCDT-Инициализация канала связи - Запрос ::= SEQUENCE { LinkIdentifier INTEGER
}
RCDT-Закрытие канала связи - Ответ ::= SEQUENCE { LinkIdentifier INTEGER
ответ БУЛЕВАО ЗНАЧЕНИЕ
}

```

Конец

DSC_74 Описание команд и параметров показано ниже:

RCDT-Инициализация канала связи — запрос используется для инициализации канала связи. Команда отправляется БУ на DSRC-VU. БУ устанавливает LinkIdentifier и передает его DSRC-VU в целях отслеживания конкретного канала связи.

(Примечание: Эта функция служит для поддержки будущих каналов и других приложений/модулей, например, для взвешивания на борту).

RCDT-Communication Link Initialization — Response используется для ответа на запрос инициализации канала связи. Команда отправляется DSRC-VU на БУ. Эта команда выдает результат инициализации в виде: ответ = 1 (успешно) или =0 (безуспешно).

DSC_75 Инициализация канала связи производится только после включения установки, калибровки и запуска двигателя/БУ.

RCDT-Send Data используется БУ для отправки подписанных RCDTData (т. е. данных удаленной связи) на DSRC-VU. Эти данные передаются через каждые 60 секунд. Параметр DataTransactionId идентифицирует конкретную передачу данных. LinkIdentifier также используется для обеспечения правильности соответствующей ссылки.

RCDT-Data Acknowledgment отправляется DSRC-VU для обеспечения обратной связи с БУ в порядке получения данных от команды RCDT-Send Data, идентифицированной параметром DataTransactionId. Параметр ответа = 1 (успешно) или =0 (безуспешно). Если БУ получает более трех ответов, равных 0, или если БУ не получает подтверждения данных RCDT для конкретных ранее отправленных данных RCDT — Send Data с конкретным идентификатором DataTransactionId, то БУ генерирует и регистрирует этот случай как соответствующее событие.

RCDT-Communication Link Termination request отправляется БУ в DSRC-VU для отключения канала связи применительно к конкретному идентификатору LinkIdentifier.

DSC_76 При перезапуске DSRC-VU или БУ, все существующие каналы связи должны быть удалены, поскольку в случае внезапного отключения БУ некоторые каналы связи могут «зависнуть».

RCDT-Communication Link Termination — Ответ отправляется DSRC-VU в БУ в порядке подтверждения запроса на перекрытие канала связи со стороны БУ применительно к конкретному идентификатору LinkIdentifier.

5.74.7 Обработка ошибок

5.7.14.7.1 Регистрация и передача данных в DSRC-VU

DSC_77 Данные передаются всегда в защищенном виде функцией VUSM в DSRC-VU. VUSM проверяет, ~~правильно~~ успешно ли были переданы зарегистрированные данные, в DSRC-VU. Регистрация и сообщения о любых ошибках при передаче данных из БУ в блок памяти DSRC-VU записываются с помощью функции EventFaultType в качестве соответствующего события со значением перечисления '62'NRemote'0C'N ошибка связи с устройством удаленной связи вместе с временной меткой. VUSM проверяет, успешно ли были переданы зарегистрированные данные в DSRC-VU.

- DSC_78 ~~Зарезервировано для использования в будущем—БУ хранит файл с уникальным названием, который могут легко найти инспекторы с целью регистрации сбоев внутренней связи БУ.~~
- DSC_79 Если функция VUPM пытается получить данные БУ из модуля безопасности (с целью передать их VU-DSRC), но безуспешно, она регистрирует этот сбой в качестве события EventFaultType и значением перечисления '62'Н Ошибка связи устройства удаленной связи вместе с временной меткой. Эта ошибка связи обнаруживается в том случае, когда не получено сообщение RCDT Data Acknowledgment на соответствующее сообщение RCDT Send Data (т. е. с таким же идентификатором DataTransactionId как и в сообщениях Send Data and Acknowledgment) более трех раз подряд.

5.7.24.7.2 Ошибки беспроводной связи

- DSC_80 Обработка ошибок связи соответствует определенным стандартам DSRC, а именно: EN 300 674-1, EN 12253, EN 12795, EN 12834 и соответствующим параметрам EN 13372.

5.7.2.14.7.2.1 Ошибки шифрования и подписи

- DSC_81 Ошибки шифрования и подписи обрабатываются, как описано в ~~приложении~~ подразделе 11 «Общие механизмы безопасности», и отсутствуют в сообщениях об ошибках, связанных с передачей данных DSRC.

5.7.2.24.7.2.2 Регистрация ошибок

Среда DSRC представляет собой динамичную беспроводную связь в случае неопределенных атмосферных условий и условий интерференции, в частности, в случае сочетания портативных REDCR и «движущегося транспортного средства» в условиях применения данного приложения. Поэтому необходимо четко различать безуспешную попытку считывания и состояние «ошибка». В случае операции через беспроводной интерфейс безуспешная попытка считывания встречается довольно часто, вследствие чего обычно предпринимается повторная попытка в виде ретрансляции BST и повторения прежней последовательности, что в большинстве случаев обеспечивает успешное соединение и передачу данных, кроме случаев, когда данное транспортное средство выходит за пределы радиуса действия за время, необходимое для повторной ретрансляции. (Успешный вариант считывания может включать в себя несколько попыток и повторных попыток).

Сбой в считывания данных может быть вызван тем, что антенны были неправильно сопряжены (сбой «визирования») по той причине, что одна из антенн экранирована — это может быть обусловлено как преднамеренным действием, так и физическим присутствием другого транспортного средства; радиопомехами, особенно на уровне частот порядка 5,8 ГГц WIFI, или другими средствами общедоступных беспроводных коммуникаций, или помехами от радара, или сложными атмосферными условиями (например, во время грозы) или просто в результате выхода за пределы зоны действия связи DSRC. Отдельные случаи сбоев в считывании данных по своей природе не могут регистрироваться, просто по той причине, что связь не была установлена.

Однако, если представитель компетентного контрольного органа производит визирование транспортного средства и пытается направить контрольный запрос в DSRC-VU, но данные не передаются, то такой сбой может возникнуть в результате преднамеренного взлома, поэтому данному сотруднику компетентного контрольного органа требуется соответствующее средство регистрации такой неудачной попытки и возможность предупредить своих коллег далее по цепочке о том, что в данном случае речь может идти о каком-либо нарушении. Его коллеги могут в этом случае остановить транспортное средство и провести физический досмотр. Однако, поскольку связь установить не удалось, DSRC-VU не может предоставить данные об этом сбое в

работе. По этой причине регистрация таких случаев предусматривается как проектная функция аппаратуры REDCR.

«Сбой в считывании» в техническом плане «ошибкой» не является. В данном контексте ошибка — это получение неверного значения.

Данные, передаваемые в DSRC-VU, предоставляются уже в защищенном виде и потому должны проверяться поставщиком этих данных (см. 5.4).

Данные, передаваемые впоследствии через воздушный интерфейс, проверяются при помощи циклического контроля избыточности на уровне связи. Если проверка CRC успешна, значит данные верны. Если проверка CRC не подтверждается, то данные передаются снова. Вероятность, что данные могут успешно пройти через CRC в неправильном виде, статистически настолько низка, что ею можно пренебречь.

Если CRC не дает подтверждения и нет времени на повторную передачу и получение верных данных, то в результате будет допущена не ошибка, а инстанцирование определенного типа сбоя в считывании данных.

Единственный значимый «сбой» в считывании данных, который можно зарегистрировать, — это число успешно инициированных операций, в результате которых не удалось произвести успешную передачу данных в REDCR.

DSC_82 В этой связи REDCR записывает, ставит временную метку и регистрирует число, если этап инициализации запроса DSRC успешно завершен, но операция прерывается до того, как данные будут успешно извлечены REDCR. Эти данные должны быть доступны для представителя компетентного контрольного органа и храниться в памяти оборудования REDCR. Способы, которыми это достигается, зависят от проекта изделия или указаний компетентного контрольного органа.

Единственные значимые данные, касающиеся «ошибки», которые можно зарегистрировать, — это число случаев, когда REDCR не может расшифровать полученные Данные. Однако следует отметить, что это будет относиться только к эффективности программного обеспечения REDCR. Данные могут быть технически расшифрованы, но при этом быть лишены семантического смысла.

DSC_83 Поэтому REDCR записывает, ставит временную метку, указывает число случаев, когда была совершена, но не удалась попытка расшифровки данных, полученных через интерфейс DSRC.

6.5. Испытания при вводе в эксплуатацию и периодических проверках функции удаленной связи

6.15.1 Общие положения

DSC_84 DSC_84 В случае функции удаленной связи предусмотрены два типа испытаний:

1) Испытание ECHO для проверки *беспроводного* канала связи DSRC-REDCR >>:-<DSRC-VU.

2) Сквозные испытания на безопасность с целью удостовериться в том, что карточка мастерской может получить доступ к зашифрованным и подписанным данным в БУ, передаваемым по каналу беспроводной связи.

6.25.2 ECHO

Этот пункт содержит положения, конкретно предназначенные для проверки только того, что функция DSRC-REDCR >>:-<DSRC-VU активирована.

Цель команды ECHO — позволить мастерским или испытательным станциям по официальному утверждению типа испытывать оборудование на работоспособность DSRC без необходимости доступа к данным безопасности. Поэтому испытательное оборудование должно быть способно лишь инициализировать связь DSRC (отправив BST с AID=2) и затем отправить команду ECHO, и, при условии, что DSRC работает, получить ответное сообщение ECHO. Более подробную информацию см. пункт 5.4.8. В предположении, что ответное сообщение правильное, можно сделать вывод о том, что связь (*DSRC-REDCR >>-:<DSRC-VU*) функционирует правильно.

6.35.3 Испытания на подтверждение защищенности содержания данных

- DSC_85 Данные испытания проводят в целях подтверждения сквозной защиты потока данных в плане безопасности. Для проведения такого испытания требуется соответствующее считывающее устройство DSRC. Испытательное считывающее устройство DSRC имеет те же функциональные особенности и выполнено с соблюдением тех же спецификаций, что и считывающее устройство, используемое правоохранительными органами, с той лишь разницей, что для аутентификации пользователя испытательного считывающего устройства DSRC используется не карточка контролера, а карточка мастерской. Испытание может быть выполнено после первоначальной активации смарт-тахографа или в конце процедуры калибровки. После активации бортового устройства генерирует и передает на DSRC-VU защищенные данные раннего обнаружения.
- DSC_86 Сотрудники мастерской должны расположить испытательное считывающее устройство DSRC на расстоянии от 2 до 10 метров перед транспортным средством.
- DSC_87 Затем они вводят карточку мастерской в испытательное считывающее устройство DSRC в порядке запроса данных раннего обнаружения у бортового устройства. После успешного контрольного запроса сотрудники мастерской получают доступ к полученным данным с целью убедиться в целостности и правильности их расшифровки.

Приложение

Правила исчисления ежедневного, еженедельного и двухнедельного времени работы водителя

1. Основные правила вычислений

БУ рассчитывает ежедневное время управления, еженедельное время управления и двухнедельное время управления, используя соответствующие данные, хранящиеся в карточке водителя (или мастерской), введенной в считывающее устройство водителя (считывающее устройство 1, устройство для считывания карточек #1) бортового устройства, и выбранные действия водителя на время, пока эта карточка введена в БУ.

Время управления не рассчитывается до тех пор, пока не будет вставлена карточка водителя (или мастерской).

Период(ы) UNKNOWN (НЕИЗВЕСТНО), обнаруженный(е) в течение периода времени, необходимого для вычислений, приравнивается(ются) к периодам BREAK/REST (ПЕРЕРЫВ/ОТДЫХ).

Периоды UNKNOWN и деятельность с отрицательной продолжительностью (т. е. случаи, когда начало деятельности происходит позже, чем ее завершение), которые обусловлены наложением времени между двумя различными БУ или корректировкой времени, не учитываются.

Виды деятельности, записанные на карточке водителя, которые относятся к периодам OUT OF SCOPE (НЕПРИМЕНИМО) в соответствии с определением (gg) добавления 1C, интерпретируются следующим образом:

- BREAK/REST (ПЕРЕРЫВ/ОТДЫХ) считаются как «ПЕРЕРЫВ» или «ОТДЫХ».
- WORK и DRIVING (РАБОТА и УПРАВЛЕНИЕ) считается как «РАБОТА».
- AVAILABILITY считается как «ДОСТУПНОСТЬ».

В контексте настоящего приложения БУ считает, что ежедневный период отдыха приходится на начало записей деятельности, регистрируемой на карточке.

2. Концепции

Следующие концепции относятся исключительно к данному добавлению и предназначены для уточнения расчета времени управления на уровне БУ и его последующей передачи удаленным средством связи.

а) «RTM-shift» (Смена RTM) — период между окончанием данного периода ежедневного отдыха и окончанием непосредственно следующего за ним очередного периода ежедневного отдыха.

БУ начинает регистрацию новой смены RTM после завершения соответствующего периода ежедневного отдыха.

Текущая смена RTM — это период, исчисляемый с момента окончания последнего ежедневного периода отдыха.

б) «Accumulated driving time» (накопленное время управления) — совокупная продолжительность всех видов деятельности водителя по УПРАВЛЕНИЮ транспортным средством в течение периода, когда он не находился в состоянии OUT OF SCOPE (НЕПРИМЕНИМО);

в) «Ежедневное время управления» — накопленное время управления в течение смены RTM.

d) «Еженедельное время управления» — накопленное время управления за текущую неделю.

e) «Период непрерывного отдыха» — любой непрерывный период BREAK/REST (перерыв/отдых).

f) «Двухнедельное время управления» — накопленное время управления за предшествующую и текущую неделю.

g) «Период ежедневного отдыха» — период BREAK/REST (перерыв/отдых), который может быть либо

- соответствующим регулярным периодом ежедневного отдыха;
- разделенным на части ежедневным отдыхом; или
- соответствующим сокращенным периодом ежедневного отдыха.

В контексте приложения 14, когда БУ рассчитывает еженедельные периоды отдыха, эти еженедельные периоды отдыха рассматриваются как ежедневные периоды отдыха;

h) «Нормальный ежедневный период отдыха» — любой период отдыха продолжительностью не менее 11 часов.

В порядке исключения, когда действует условие FERRY/TRAIN CROSSING (ПЕРЕЕЗД НА ПАРОМЕ/ПОЕЗДЕ), регулярный ежедневный период отдыха может прерываться максимум два раза на другие виды деятельности, кроме отдыха, максимальной суммарной продолжительностью один час, т. е. регулярный ежедневный период отдыха, содержащий период(ы) переезда на пароме/поезде, может быть разделен на две или три части. БУ рассчитывает регулярный ежедневный период отдыха в тот момент, когда накопленное время отдыха, рассчитанное в соответствии с пунктом 3, составляет не менее 11 часов.

Если регулярный ежедневный период отдыха был прерван, БУ:

- не включает в расчет ежедневного времени управления деятельность, связанную с управлением, во время этих перерывов; и
- начинает отсчитывать новую смену RTM в конце регулярного ежедневного периода отдыха, который был прерван.

A	B	C	D	E	F	G
☉/☼/☐	h	☉/☼/☐	h ☼	☉/☼/☐	h	☉/☼/☐
Working Period	2 h	30 min	8 h	30 min	2 h	New Day

Рис. 1. Пример прерывания ежедневного отдыха из-за переезда на пароме/поезде

i) «Сокращенный ежедневный период отдыха» — любой период отдыха продолжительностью не менее 9 и не более 11 часов.

j) «Разделенный ежедневный отдых» — ежедневный отдых, состоящий из двух частей:

- первая часть — любой период непрерывного отдыха продолжительностью не менее 3 и менее 9 часов;
- вторая часть — любой период непрерывного отдыха продолжительностью не менее 9 часов.

В качестве исключения, когда условие FERRY/TRAIN CROSSING (ПЕРЕЕЗД НА ПАРОМЕ/ПОЕЗДЕ) действует в течение одной или обеих частей разделенного ежедневного периода отдыха, этот разделенный ежедневный период отдыха может быть прерван максимум два раза другими видами деятельности суммарной продолжительностью не более одного часа, т. е.:

Если ни одно из вышеперечисленных условий не выполняется, то к накопленному времени отдыха добавляется период непрерывного отдыха, непосредственно предшествовавший данному перерыву.

Если выполняется хотя бы одно из вышеуказанных условий, БУ либо прекращает расчет накопленного времени отдыха в соответствии с этапом 2, либо выявляет перерывы во времени отдыха, имевшие место после появления метки FERRY/TRAIN CROSSING (BEGIN), в соответствии с этапом 3.

b) Этап 2

В случае каждого перерыва, выявленного в соответствии с этапом 1, БУ проверяет, следует ли прекратить расчет накопленного времени отдыха. БУ останавливает процесс расчета в том случае, когда к накопленному времени отдыха добавляются два непрерывных периода отдыха, имевших место до активации метки FERRY/TRAIN CROSSING (BEGIN), включая в этом случае периоды отдыха, добавленные в первой части отдельного ежедневного периода отдыха, который также был прерван паромным/железнодорожным переездом. В противном случае БУ действует в соответствии с этапом 3.

c) Этап 3

Если после выполнения этапа 2 БУ продолжает расчет накопленного времени отдыха, то в этом случае БУ выявляет перерывы, имевшие место после деактивации условия, связанного с ПЕРЕЕЗДОМ НА ПАРОМЕ/ПОЕЗДЕ, в соответствии с рисунком 3 и в данном случае в соответствии с рис. 4.

В случае каждого обнаруженного перерыва БУ проверяет, превышает ли этот перерыв суммарное время всех обнаруженных перерывов более чем на один час, и если превышает, то в этом случае расчет накопленного периода отдыха прекращается в конце непрерывного периода отдыха, предшествующего этому перерыву. В противном случае, периоды непрерывного отдыха, имеющие место после соответствующих перерывов, добавляются к расчету периода ежедневного отдыха до тех пор, пока не будет выполнено условие на этапе 4.

d) Этап 4

Расчет накопленного времени отдыха прекращается в том случае, когда в результате выполнения этапов 1 и 3 БУ добавляет максимум два непрерывных периода отдыха к периоду отдыха, в случае которого было активировано условие FERRY/TRAIN CROSSING, включая в этом случае перерывы, имевшие место в ходе первой части разделенного ежедневного периода отдыха в связи с переездом на пароме/поезде.

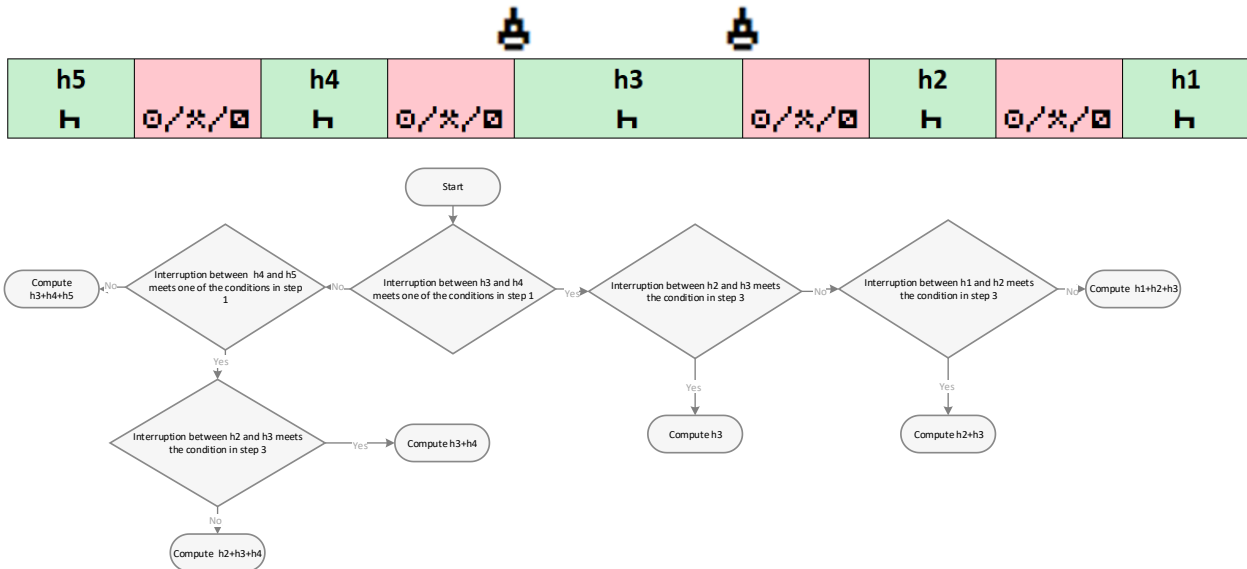


Рис 3. Расчет продолжительности периодов времени отдыха, производимого БУ с целью определить, должен ли прерванный период отдыха учитываться как обычный ежедневный период отдыха или как первая часть разделенного ежедневного периода отдыха

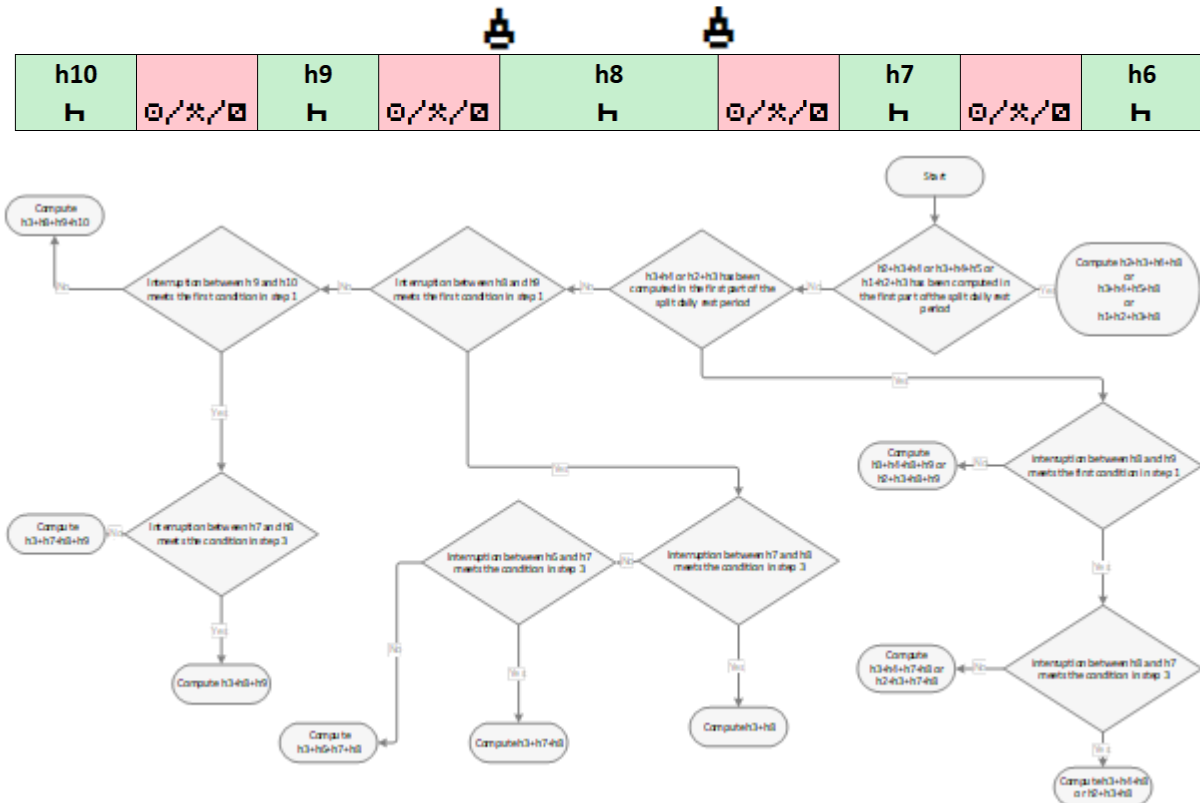


Рис 4. Расчет продолжительности периодов времени отдыха, производимый БУ с целью определить, должен ли прерванный период отдыха учитываться как обычный ежедневный период отдыха или как вторая часть разделенного ежедневного периода отдыха

БУ также рассчитывает недельное и двухнедельное время управления. Время управления, которое приходится на перерывы в ежедневном отдыхе в связи с переездом на пароме/поезде, включается в расчет еженедельного и двухнедельного времени управления.

Подраздел 15

Переход на новые версии: управление системой параллельного использования оборудования разных поколений

Содержание

	<i>Стр.</i>
1. Определения	641
2. Общие положения	641
2.1 Обзор проблемы перехода	641
2.2 Эксплуатационная совместимость между БУ и карточками	641
2.3 Эксплуатационная совместимость между БУ и датчиком движения	642
2.4 Эксплуатационная совместимость между бортовыми устройствами, карточками тахографа и оборудованием для загрузки данных	642
2.4.1 Прямая загрузка данных карточки СПА	642
2.4.2 Загрузка данных карточки через бортовое устройство	643
2.4.3 Загрузка данных с бортового устройства	643
2.5 Эксплуатационная совместимость между БУ и калибровочным оборудованием	643
3. Основные этапы в течение периода до даты ввода в эксплуатацию	644
4. Нормативные положения на период после даты ввода в эксплуатацию	644

1. Определения

Для целей настоящего ~~приложения~~ **подраздела** используются следующие определения:

система смарт-тахографа: см. определение в настоящем ~~приложении~~ **добавлении** (глава 1: определение bbb);

система тахографа первого поколения: см. определение в ~~настоящем регламенте~~ **(статья 2: определение 1) во введении к настоящему добавлению;**

система тахографа второго поколения: см. определение в ~~настоящем регламенте~~ **(статья 2: определение 1) во введении к настоящему добавлению;**

дата ввода в эксплуатацию: см. определение в настоящем ~~дополнении~~ **добавлении** (глава 1: определение ccc);

специализированная программируемая аппаратура (СПА): оборудование, используемое для загрузки данных, в соответствии с определением в ~~добавлении~~ **подразделе 7 настоящего приложения добавления.**

2. Общие положения

2.1 Обзор проблемы перехода

Во **введении к вводящей части данного приложения к данному подразделу** содержится обзор проблемы перехода между системами тахографов первого и второго поколения, **а также введения в эксплуатацию второй версии контрольного устройства второго поколения и карточек тахографа.**

В дополнение к положениям ~~пreamбулы~~ **данного введения можно обратить внимание на следующую информацию:**

- датчики движения первого поколения ~~не будут~~ **несовместимы с любой версией** бортовых устройств второго поколения.
- на транспортных средствах ~~вместе~~ с бортовыми устройствами **любой версии** второго поколения могут устанавливаться **только** датчики движения второго поколения.
- оборудование для загрузки данных и калибровки ~~необходимо должно будет развиваться, совершенствоваться, с тем чтобы оно могло~~ **поддерживать эксплуатацию записывающего оборудования контрольных устройств и карточек тахографов обоих поколений или версий.**

2.2 Эксплуатационная совместимость между БУ и карточками

Предполагается, что карточки тахографа первого поколения совместимы с бортовыми устройствами первого поколения (в соответствии с ~~дополнением 1В настоящего регламента~~) **добавлением 1В**, а карточки тахографа второго поколения совместимы с бортовыми устройствами **любой версии** второго поколения в соответствии с ~~дополнением~~ **добавлением 1С к настоящему Регламенту Соглашению.** Кроме того, применяются требования, изложенные ниже.

MIG_001 За исключением случаев, предусмотренных в требованиях MIG_004 и MIG_005, карточки тахографа первого поколения могут и дальше использоваться в **любой версии** бортовых устройств второго поколения до истечения их срока действия. Однако их держатели могут попросить заменить их карточками тахографа второго поколения, как только они станут доступны.

- MIG_002 **Любая версия** бортового устройства второго поколения может использовать любые вводимые в них карточки водителя, контролера и предприятия первого поколения.
- MIG_003 Эту возможность бортовых устройств могут окончательно и бесповоротно устранить мастерские с целью исключить дальнейшее использование карточек тахографа первого поколения. Это можно будет сделать только на основании соответствующей процедуры, имеющей целью **обратиться** после того, как Европейская комиссия начнет процедуру, в рамках которой к мастерским с просьбой принять такие меры, например, во время регулярной проверки тахографа.
- MIG_004 Бортовые устройства второго поколения могут использовать только карточки мастерской второго поколения.
- MIG_005 Для определения режима работы **любая версия** бортовых устройств второго поколения учитывает только типы введенных действительных карточек независимо от их поколений **или версий**.
- MIG_006 Любая **версия** действительной карточки тахографа второго поколения ~~должна иметь возможность~~ **может** использоваться в бортовых устройствах первого поколения точно так же, как и карточка тахографа первого поколения того же типа.

2.3 Эксплуатационная совместимость между БУ и датчиком движения

Предполагается, что датчики движения первого поколения совместимы с бортовыми устройствами первого поколения, а датчики движения второго поколения — с бортовыми устройствами второго поколения **любой версии**. Кроме того, применяются требования, изложенные ниже.

- MIG_007 **Любая версия** бортовых устройств второго поколения не может быть сопряжена и использоваться с датчиками движения первого поколения.
- MIG_008 Датчики движения второго поколения могут быть сопряжены и использоваться только с бортовыми устройствами второго поколения, **независимо от версии**, или с бортовыми устройствами обоих поколений.

2.4 Эксплуатационная совместимость между бортовыми устройствами, карточками тахографа и оборудованием для загрузки данных

- MIG_009 Оборудование для загрузки данных может ~~использоваться совместно только со всеми поколениями~~ **использоваться совместно** бортовых устройств и карточек тахографа ~~или с обоими поколениями~~.

2.4.1 Прямая загрузка данных карточки СПА

- MIG_010 СПА загружает данные с карточек тахографа одного поколения, введенных в считывающие устройства, при помощи механизмов защиты и протокола загрузки данных этого поколения; данные загружаются в формате данного поколения **и данной версии**.
- MIG_011 Для того чтобы водителей могли проверять контрольные органы третьих стран, не являющихся членами ЕС, можно также загружать данные карточек водителя (и мастерской) второго поколения, **независимо от версии**, точно таким же образом, как и данные карточек водителя (мастерской) первого поколения. Такая загрузка включает:
- неподписанные файлы EF ИС и ICC (**факультативно**);
 - неподписанные EF (~~1-е~~ **первое** поколение) Card_Certificate и CA_Certificate;

- другие EF с данными, которые содержатся в приложении (в DF тахографа) и запрашиваются протоколом загрузки карточки первого поколения. Данная информация защищается цифровой подписью в соответствии с механизмами безопасности первого поколения.

Такая загрузка не включает в себя данных в EF приложений, имеющихся только на карточках водителя (и мастерской) **версии 1 и версии 2** второго поколения (данные в EF приложений в **DF Tachograph_G2**).

2.4.2 Загрузка данных карточки через бортовое устройство

- MIG_012 Данные загружаются с карточки **любой версии** второго поколения, введенной в бортовое устройство первого поколения, с использованием протокола загрузки данных первого поколения. Карточка отвечает на команды бортового устройства точно так же, как и карточка первого поколения, при том что формат загружаемых данных такой же, как и данных, загружаемых с карточки первого поколения.
- MIG_013 Данные загружаются с карточки первого поколения, введенной в бортовое устройство второго поколения **любой версии**, с использованием протокола загрузки данных, определенного в ~~приложении~~ **подразделе 7** настоящего ~~дополнения~~ **добавления**. Бортовое устройство передает команды на карточку точно так же, как и бортовое устройство первого поколения, при том что формат загружаемых данных соответствует формату, определенному для карточек первого поколения.

2.4.3 Загрузка данных с бортового устройства

- MIG_014 ~~Данные~~ **Вне рамок проверки водителей контрольными органами стран, не являющихся членами в ЕС**, данные загружаются из бортовых устройств второго поколения с использованием механизмов безопасности второго поколения и протокола загрузки данных, указанного в ~~добавлении~~ **подразделе 7** настоящего ~~приложения~~ **добавления для соответствующей версии**.
- MIG_015 Для того чтобы водителей могли проверять контрольные органы третьих стран, не являющихся членами ЕС, можно также в качестве варианта предусмотреть возможность загрузки данных из бортовых устройств **любой версии** второго поколения с использованием механизмов безопасности первого поколения. Формат загружаемых данных **в этом случае** такой же, как и в случае данных, загружаемых с бортового устройства первого поколения. Эту функцию можно выбрать из команд в меню.

2.5 Эксплуатационная совместимость между БУ и калибровочным оборудованием

- MIG_016 Калибровочное оборудование способно выполнять калибровку тахографов любого поколения или версии с применением протокола калибровки того же поколения. Калибровочное оборудование может ~~непользоваться~~ **совмещаться с одним поколением со всеми** поколениями **и версиями бортовых устройств** ~~только тахографов или с обоими~~.

3. Основные этапы в течение периода до даты ввода в эксплуатацию

- MIG_017 Испытательные ключи и сертификаты предоставляются изготовителям ~~не позднее чем за 30 месяцев до даты ввода на дату издания настоящего добавления.~~
- MIG_018 Испытания на эксплуатационную совместимость должны быть подготовлены к началу испытаний **версии 2 бортовых устройств и версии 2 карточек тахографов**, если они будут затребованы изготовителями не позднее чем за 15 месяцев до даты введения в эксплуатацию.
- MIG_019 Для тахографов, карточек тахографа и датчиков движения **версии 2 поколения 2 используются те же** ~~Официальные~~ ключи и сертификаты, **что и для оборудования версии 1 поколения 2,** ~~должны быть доступны производителям не позднее чем за 12 месяцев до даты внедрения.~~
- MIG_020 ~~Государства-члены Договаривающиеся стороны~~ могут выпускать карточки мастерской **версии 2** второго поколения не позднее чем за **3 1** месяца до даты ввода в эксплуатацию.
- MIG_021 ~~Государства-члены Договаривающиеся стороны должны иметь возможность могут~~ выпускать все **другие** типы карточек тахографа **версии 2** второго поколения не позднее, чем за **1** месяц до даты ввода в эксплуатацию.

4. Нормативные положения на период после даты ввода в эксплуатацию

- MIG_022 **Начиная с даты ввода в эксплуатацию** ~~государства-члены Договаривающиеся стороны~~ выпускают только карточки тахографа **версии 2** второго поколения.
- MIG_023 Изготовитель бортовых устройств/датчиков движения могут производить бортовые устройства/датчики движения первого поколения до тех пор, пока они будут применяться на практике, с целью замены неисправных компонентов.
- MIG_024 **Начиная с даты ввода в эксплуатацию, неисправные бортовые устройства версии 1 второго поколения или внешние устройства ГНСС заменяются бортовыми устройствами или внешними средствами ГНСС версии 2 второго поколения.**
- MIG_0254 Изготовители бортовых устройств/датчиков движения могут подавать заявки и получать официальное утверждение для технического обслуживания соответствующих типов бортовых устройств/датчиков движения или **версии 1 бортовых устройств второго поколения,** которые уже получили официальное утверждение типа.

Подраздел 16

Адаптер для транспортных средств категорий M1 и N1

Содержание

	<i>Стр.</i>
1. Сокращения и справочные документы	646
1.1 Сокращения	646
1.2 Справочные стандарты	646
2. Общие характеристики и функции адаптера	646
2.1 Общее описание адаптера	646
2.2 Функции	646
2.3 Безопасность	646
3. Требования к контрольному устройству записывающему оборудованию в случае установки адаптера	647
4. Требования к конструкции и функциям адаптера	647
4.1 Обеспечение сопряжения и адаптация входящих импульсов скорости	647
4.2 Индуцирование поступающих импульсов на встроенный датчик движения	648
4.3 Встроенный датчик движения	648
4.4 Требования безопасности	648
4.5 Эксплуатационные характеристики	648
4.6 Материалы	649
4.7 Маркировка	649
5. Требования к записывающему оборудованию контрольному устройству в случае установки адаптера	649
5.1 Установка	649
5.2 Наложение пломб	650
6. Проверка, инспекция и ремонт	650
6.1 Периодические инспекции	650
7. Требования к записывающему оборудованию контрольному устройству в случае использования адаптера	650
7.1 Общие положения	651

1. Сокращения и справочные документы

1.1 Сокращения

TBD	будет определено позднее
БУ	Бортовое устройство

1.2 Справочные стандарты

ISO16844-3 Транспорт дорожный — Системы тахографов — Часть 3: Интерфейс датчика движения

2. Общие характеристики и функции адаптера

2.1 Общее описание адаптера

ADA_001 Адаптер обеспечивает присоединенное БУ защищенными данными движения, постоянно отображающими скорость транспортного средства и пройденное расстояние.

Адаптер предназначен только для тех транспортных средств, которые в обязательном порядке должны быть оснащены ~~записывающим оборудованием~~ **контрольным устройством** в соответствии с настоящим ~~Регламентом~~ **Соглашением**.

Он устанавливается и используется только на тех типах транспортных средств, которые указаны в определении (уу) «адаптер» в ~~приложении~~ **добавлении 1С**, если механически невозможно установить никакие другие датчики движения, которые в остальном соответствуют положениям настоящего ~~приложения~~ **добавления** и его ~~приложений~~ **подразделов 1–16**.

Адаптер механически сопрягается не с движущейся частью транспортного средства, а с помощью интерфейса, передающего импульсы скорости/расстояния, генерируемые встроенными датчиками, или другими интерфейсами.

ADA_002 Датчик движения утвержденного типа (в соответствии с положениями ~~приложения-добавления 1С~~, часть 8 «Утверждение типа ~~записывающего оборудования~~ **контрольного устройства** и карточек тахографов») устанавливается в корпус адаптера, в который также вставляется устройство конвертации импульсов, индуцирующее поступление входящих импульсов на встроенный датчик движения. Сам встроенный датчик движения соединяется с БУ таким образом, чтобы интерфейс между БУ и адаптером соответствовал требованиям ISO16844-3.

2.2 Функции

ADA_003 Адаптер включает следующие функции:

- обеспечение сопряжения и адаптация входящих импульсов скорости;
- индуцирование входящих импульсов на встроенный датчик движения;
- все функции встроенного датчика движения, обеспечивающие поступление защищенных данных о движении на БУ.

2.3 Безопасность

ADA_004 Сертификация защиты адаптера в соответствии с общим уровнем защиты датчика движения, установленным в ~~приложении~~ **подразделе 10**

настоящего ~~дополнения~~ **добавления**, не производится. Вместо этого применяются требования к безопасности, указанные в разделе 4.4 настоящего ~~приложения~~ **подраздела**.

3. Требования к контрольному устройству ~~записывающему~~ **оборудованию** в случае установки адаптера

Требования в последующих главах уточняют, каким образом следует понимать требования настоящего ~~приложения~~ **подраздела** в тех случаях, когда используется адаптер. В скобках указаны номера соответствующих требований, содержащихся в ~~приложении~~ **добавлении IC**.

- ADA_005 ~~Записывающее—оборудование~~ **Контрольное устройство** любого транспортного средства, оснащенное адаптером, должно соответствовать всем положениям настоящего ~~приложения~~ **подраздела**, за исключением случаев, когда в настоящем ~~приложении~~ **подразделе** указано иное.
- ADA_006 В случае установки адаптера в состав ~~записывающего—оборудования~~ **контрольного устройства** входят кабели, адаптер (включая датчик движения) и БУ [01].
- ADA_007 Функция ~~записывающего—оборудования~~ **контрольного устройства** по обнаружению событий и/или неисправностей изменяется следующим образом:
- событие «прекращение питания» отображается БУ, за исключением режима калибровки, в случае прекращения питания встроенного датчика движения в течение более 200 миллисекунд [79];
 - «ошибка датчика движения» отображается в БУ в случае нарушения нормального потока данных между встроенным датчиком движения и бортовым устройством и/или в случае ошибки, указывающей на нарушение целостности или аутентичности данных в процессе передачи данных датчиком движения в БУ [83];
 - событие «попытка нарушения системы защиты» отображается БУ в случае любого другого события, оказывающего воздействие на безопасность встроенного датчика движения, за исключением режима калибровки [85];
 - неисправность ~~записывающего—оборудования~~ **«контрольного устройства»** отображается БУ, за исключением режима калибровки, в случае любой неисправности встроенного датчика движения [88].
- ADA_008 Неисправности адаптера, которые может обнаружить ~~записывающее~~ **оборудование контрольное устройство**, — это неисправности, которые связаны со встроенным датчиком движения [88].
- ADA_009 Функция калибровки БУ позволяет автоматически соединять встроенный датчик движения с БУ [202, 204].

4. Требования к конструкции и функциям адаптера

4.1 Обеспечение сопряжения и адаптация входящих импульсов скорости

- ADA_011 Входной интерфейс адаптера принимает импульсы частоты, отражающие скорость транспортного средства и пройденное расстояние. Электрические характеристики входящих импульсов: подлежат определению изготовителем. Корректировки, доступные только для изготовителя адаптера и уполномоченной мастерской, выполняющей установку адаптера, позволяют обеспечить, в случае применимости,

правильное сопряжение адаптера с транспортным средством через интерфейс.

- ADA_012 Входной интерфейс адаптера способен, в случае применимости, умножать или делить импульсы частоты входящих импульсов скорости на определенный коэффициент в целях адаптации сигнала к диапазону изменения коэффициента k , как описано в настоящем ~~приложении~~ **добавлении** (24000–25000 имп./км). Этот фиксированный коэффициент может быть запрограммирован только изготовителем адаптера и уполномоченной мастерской, которая устанавливает адаптер.

4.2 Индуцирование поступающих импульсов на встроенный датчик движения

- ADA_013 Входящие импульсы возбуждения, по возможности адаптированные, как описано выше, передаются на встроенный датчик движения, который позволяет ему реагировать на каждый поступающий импульс.

4.3 Встроенный датчик движения

- ADA_014 Встроенный датчик движения возбуждается под воздействием поступающих импульсов, приобретая тем самым способность генерировать данные о движении, точно отражающие перемещение транспортного средства, как если бы он был механически соединен с соответствующей движущейся частью транспортного средства.
- ADA_015 Идентификационные данные встроенного датчика движения позволяют идентифицировать адаптер [95].
- ADA_016 Считается, что монтажные данные, хранящиеся во встроенном датчике движения, отражают данные установки адаптера [122].

4.4 Требования безопасности

- ADA_017 Корпус адаптера выполнен таким образом, чтобы его нельзя было вскрыть. На него накладываются пломбы, что позволяет легко обнаружить попытки нарушения его физической целостности (например, в ходе визуального осмотра; см. ADA_035). Пломбы соответствуют тем же требованиям, что и пломбы датчиков движения [398-406].
- ADA_018 Встроенный датчик движения невозможно изъять из адаптера, не повредив пломбу(ы) корпуса адаптера или пломбу между датчиком и корпусом адаптера (см. ADA_034).
- ADA_019 Адаптер обеспечивает возможность обработки и получения данных о движении только на входе адаптера.

4.5 Эксплуатационные характеристики

- ADA_020 Адаптер полностью работоспособен в диапазоне температур, указанном изготовителем.
- ADA_021 Адаптер полностью работоспособен в диапазоне влажности 10–90 % [214].
- ADA_022 Адаптер защищен от бросков напряжения, несоблюдения полярности источника питания и короткого замыкания [216].

ADA_023 Адаптер либо:

- реагирует на магнитное поле, нарушающее функцию реагирования на движение транспортного средства. В подобных обстоятельствах бортовое устройство регистрирует и хранит запись о неисправности датчика (требование 88); либо
- оснащается чувствительным элементом, защищенным от магнитных полей или не реагирующим на них.

ADA_024 Адаптер соответствует Правилам ЕЭК № 10, регламентирующим электромагнитную совместимость, и защищен от электростатических разрядов и помех, вызванных переходными процессами [218].

4.6 Материалы

ADA_025 Адаптер соответствует уровню защиты (по усмотрению изготовителя в зависимости от местоположения при монтаже) [220, 221].

ADA_026 Цвет корпуса адаптера — желтый.

4.7 Маркировка

ADA_027 На адаптер крепится табличка с указанием следующих данных:

- название и адрес изготовителя адаптера;
- номер части, присвоенный изготовителем, и год изготовления адаптера;
- знак официального утверждения типа адаптера или типа записывающего оборудования, включая адаптер;
- дата установки адаптера;
- идентификационный номер транспортного средства, на котором он установлен.

ADA_028 Табличка с данными также содержит следующие сведения (если их нельзя прочитать непосредственно на внешней поверхности встроенного датчика движения):

- название изготовителя встроенного датчика движения;
- номер части, присвоенный изготовителем, и год изготовления встроенного датчика движения;
- знак официального утверждения встроенного датчика движения.

5. Требования к записывающему оборудованию контрольному устройству в случае установки адаптера

5.1 Установка

ADA_029 Адаптеры, подлежащие установке на транспортных средствах, устанавливаются только изготовителями транспортных средств или официально утвержденные мастерские, уполномоченные устанавливать, активировать и калибровать цифровые тахографы и смарт-тахографы.

ADA_030 Такая официально утвержденная мастерская, устанавливающая адаптер, настраивает входной интерфейс и выбирает коэффициент деления входного сигнала (в случае применимости).

ADA_031 Такая официально утвержденная мастерская, устанавливающая адаптер, налагает на корпус адаптера соответствующую пломбу.

- ADA_032 Адаптер устанавливают как можно ближе к той части транспортного средства, которая передает входящие импульсы.
- ADA_033 Электропроводка, обеспечивающая питание адаптера, имеет красный (положительная клемма) и черный цвет (заземление).

5.2 Наложение пломб

- ADA_034 Применяются следующие дополнительные требования:
- корпус адаптера пломбируется (см. ADA_017);
 - корпус встроенного датчика должен быть герметично соединен с корпусом адаптера, за исключением случаев, когда извлечь датчик из корпуса адаптера без нарушения уплотнения (уплотнений) корпуса адаптера невозможно (см. ADA_018);
 - корпус адаптера плотно крепится к транспортному средству;
 - соединение между адаптером и оборудованием, которое генерирует на его входе импульсы, герметизируется с обоих концов (в той степени, в какой это в достаточной степени приемлемо).

6. Проверка, инспекция и ремонт

6.1 Периодические инспекции

- ADA_035 При использовании адаптера каждая периодическая инспекция (под периодическими инспекциями понимаются проверки в соответствии с требованиями [409]–[413] ~~Приложения добавления 1С) записывающего оборудования контрольного устройства~~ включает следующие проверки с целью удостовериться:

- что на адаптер нанесена надлежащая маркировка, указывающая на официальное утверждение типа,
- что уплотнения на адаптере и его соединениях не повреждены,
- что адаптер установлен так, как указано на установочной табличке,
- что адаптер установлен в соответствии с требованиями изготовителя адаптера и/или транспортного средства,
- что установка адаптера на проверяемом транспортном средстве разрешена.

- ADA_036 Эти инспекции включают в себя калибровку и замену всех пломб вне зависимости от их состояния.

7. Требования к ~~записывающему оборудованию~~ контрольному устройству в случае использования адаптера

7.1 Общие положения

- ADA_037 ~~Записывающее оборудование~~ **Контрольное устройство** представляется на официальное утверждение типа в полной комплектации, вместе с адаптером [425].
- ADA_038 Любой адаптер можно представить на официальное утверждение типа в качестве отдельного устройства или на официальное утверждение типа в

качестве компонента ~~записывающего~~ ~~оборудования~~ **контрольного устройства**.

ADA_039 Такое официальное утверждение типа включает в себя функциональные испытания вместе с адаптером. Положительные результаты каждого из этих испытаний подтверждаются соответствующим сертификатом [426].

7.2 Сертификат функциональности

ADA_040 Сертификат функциональности адаптера или ~~записывающего оборудования~~ **контрольного устройства** в комплекте с адаптером, изготовителю адаптера выдается только после того, как будут успешно проведены следующие минимальные функциональные испытания.

<i>№</i>	<i>Испытание</i>	<i>Описание</i>	<i>Соответствующие требования</i>
1.	Административная проверка		
1.1	Документация	Правильность документации на адаптер	
2.	Визуальный осмотр		
2.1	Соответствие адаптера документации		
2.2	Идентификация/маркировка адаптера		ADA_027, ADA_028
2.3	Материалы адаптера		[219]–[223] ADA_026
2.4	Наложение пломб		ADA_017, ADA_018, ADA_034
3.	Функциональные испытания		
3.1	Индукцирование входящих импульсов скорости на встроенный датчик движения		ADA_013
3.2	Обеспечение сопряжения и адаптация входящих импульсов скорости		ADA_011, ADA_012
3.3	Точность измерения движения		[30]–[35], [217]
4.	Испытание на воздействие внешних факторов		
4.1	Результаты испытаний, проведенных изготовителем	Результаты испытаний на воздействие внешних факторов, проведенных изготовителем	ADA_020, ADA_021, ADA_022, ADA_024
5.	EMC		
5.1	Излучение и восприимчивость	Проверка на соответствие Директивы ЕЭК ООН 2006/28/ЕС Правилам ЕЭК ООН 10	ADA_024
5.2	Результаты испытаний, проведенных изготовителем	Результаты испытаний на воздействие условий окружающей среды, проведенных изготовителем	ADA_024