



**Экономический  
и Социальный Совет**

Distr.: General  
17 January 2018  
Russian  
Original: English, French and  
Russian

---

**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)

Семнадцатая сессия

Женева, 19 февраля 2018 года

Пункт 2 b) предварительной повестки дня

Программа работы

**Добавление 1С**

**Представленно правительством Эстонии\***

Этот документ содержит Приложение 1С к Регламенту (ЕС) 2016/799. Документ следует использовать вместе с предложениями по поправкам, включенными в документ ECE/TRANS/SC.1/GE.21/2018/1.

---

\* Документ воспроизводит переданный текст без изменений.

GE.18-00678 (R)



\* 1 8 0 0 6 7 8 \*

Просьба отправить на вторичную переработку



**RU**

*Дополнение IC*  
*Требования к конструированию, тестированию, установке и*  
*проверкам*

<b>ВВЕДЕНИЕ .....</b>	<b>8</b>
<b>1 ОПРЕДЕЛЕНИЯ .....</b>	<b>10</b>
<b>2 ОБЩИЕ ХАРАКТЕРИСТИКИ И ФУНКЦИИ ЗАПИСЫВАЮЩЕГО ОБОРУДОВАНИЯ .....</b>	<b>17</b>
<b>2.1 Общие характеристики .....</b>	<b>17</b>
<b>2.2 Функции .....</b>	<b>17</b>
<b>2.3 Режимы работы .....</b>	<b>18</b>
<b>2.4 Защита .....</b>	<b>19</b>
<b>3 ТРЕБОВАНИЯ К КОНСТРУКЦИИ И ФУНКЦИЯМ ЗАПИСЫВАЮЩЕГО ОБОРУДОВАНИЯ .....</b>	<b>20</b>
<b>3.1 Контроль за вводом и извлечением карточек .....</b>	<b>20</b>
<b>3.2 Измерение скорости, местоположения и пробега.....</b>	<b>20</b>
3.2.1 Измерение пройденного расстояния .....	21
3.2.2 Измерение скорости .....	21
3.2.3 Определение местоположения.....	22
<b>3.3 Измерение времени .....</b>	<b>22</b>
<b>3.4 Контроль за деятельностью водителя.....</b>	<b>22</b>
<b>3.5 Контроль за статусом управления .....</b>	<b>23</b>
<b>3.6 Записи водителей.....</b>	<b>23</b>
3.6.1 Ввод данных о местах, в которых начинаются и/или заканчиваются дневные периоды работ	23
3.6.2 Ручной ввод данных о деятельности водителя и согласия водителя для интерфейса ИТС .....	23
3.6.3 Ввод данных об особых условиях .....	25
<b>3.7 Реагирование на блокировку, установленную предприятием .....</b>	<b>25</b>
<b>3.8 Мониторинг деятельности контроля .....</b>	<b>26</b>
<b>3.9 Обнаружение событий и/или неисправностей.....</b>	<b>26</b>
3.9.1 Событие «Ввод недействительной карточки».....	26
3.9.2 Событие «несовместимость карточек» .....	26
3.9.3 Событие «Нестыковка во времени» .....	27
3.9.4 Событие «Управление без соответствующей карточки» .....	27
3.9.5 Событие «Ввод карточки во время управления» .....	27
3.9.6 Событие «Неправильное завершение последнего сеанса использования карточки» .....	27
3.9.7 Событие «Превышение скорости» .....	27
3.9.8 Событие «Прекращение электропитания» .....	28
3.9.9 Событие «Ошибка связи со средством удалённой связи» .....	28
3.9.10 Событие «Отсутствие информации о местоположении из приёмника ГНСС» .....	28
3.9.11 Событие «Ошибка связи с внешним устройством ГНСС» .....	28
3.9.12 Событие «Ошибочные данные о движении» .....	28
3.9.13 Событие «Противоречивая информация о движении транспортного средства» .....	29
3.9.14 Событие «Попытка нарушения системы защиты» .....	29
3.9.15 Событие «Противоречивая информация о времени» .....	29
3.9.16 Неисправность «Карточка».....	29
3.9.17 Неисправность «Записывающее оборудование» .....	29
<b>3.10 Встроенные проверки и самопроверки.....</b>	<b>29</b>
<b>3.11 Считывание данных из блока памяти .....</b>	<b>30</b>

<b>3.12</b>	<b>Регистрация и хранение данных в блоке памяти .....</b>	<b>30</b>
3.12.1	Идентификационные данные аппаратуры .....	30
3.12.1.1	Идентификационные данные бортового устройства .....	30
3.12.1.2	Идентификационные данные датчика движения .....	31
3.12.1.3	Идентификационные данные глобальных навигационных спутниковых систем .....	31
3.12.2	Ключи и сертификаты .....	32
3.12.3	Данные о вводе и извлечении карточек водителя или мастерской .....	32
3.12.4	Данные о деятельности водителя .....	32
3.12.5	Места и положения, в которых начинаются и заканчиваются дневные периоды работы и/или достигается 3-часовой предел непрерывного управления .....	33
3.12.6	Данные одометра .....	33
3.12.7	Подробные данные о скорости .....	33
3.12.8	Данные о событиях .....	33
3.12.9	Данные о неисправностях .....	37
3.12.10	Данные калибровки .....	37
3.12.11	Данные корректировки времени .....	38
3.12.12	Данные о контрольных действиях .....	38
3.12.13	Данные блокировки, установленной предприятием .....	38
3.12.14	Данные о действиях загрузки .....	38
3.12.15	Данные об особых условиях .....	39
3.12.16	Данные карточек тахографов .....	39
<b>3.13</b>	<b>Считывание данных с карточек тахографов .....</b>	<b>39</b>
<b>3.14</b>	<b>Регистрация и хранение данных на карточках тахографов .....</b>	<b>39</b>
3.14.1	Регистрация и хранение данных на карточках тахографа первого поколения .....	40
3.14.2	Регистрация и хранение данных на карточках тахографа второго поколения .....	40
<b>3.15</b>	<b>Отображение .....</b>	<b>41</b>
3.15.1	Вид дисплея с исходными настройками .....	41
3.15.2	Отображение предупреждения .....	42
3.15.3	Доступ к меню .....	42
3.15.4	Другие отображаемые данные .....	42
<b>3.16</b>	<b>Печать .....</b>	<b>43</b>
<b>3.17</b>	<b>Предупреждения .....</b>	<b>44</b>
<b>3.18</b>	<b>Загрузка данных на внешние носители .....</b>	<b>45</b>
<b>3.19</b>	<b>Удалённая связь для целевых придорожных проверок .....</b>	<b>45</b>
<b>3.20</b>	<b>Вывод данных на дополнительные внешние устройства .....</b>	<b>45</b>
<b>3.21</b>	<b>Калибровка .....</b>	<b>46</b>
<b>3.22</b>	<b>Придорожные проверки калибровки .....</b>	<b>47</b>
<b>3.23</b>	<b>Корректировка времени .....</b>	<b>47</b>
<b>3.24</b>	<b>Рабочие характеристики .....</b>	<b>47</b>
<b>3.25</b>	<b>Материалы .....</b>	<b>48</b>
<b>3.26</b>	<b>Маркировка .....</b>	<b>48</b>
<b>4</b>	<b>ТРЕБОВАНИЯ К КОНСТРУКЦИИ И ФУНКЦИЯМ КАРТОЧЕК ТАХОГРАФОВ .....</b>	<b>49</b>
4.1	Видимые данные .....	49



<b>4.2</b>	<b>Защита .....</b>	<b>53</b>
<b>4.3</b>	<b>Стандарты .....</b>	<b>53</b>
<b>4.4</b>	<b>Спецификации по условиям окружающей среды и электромагнитной совместимости.....</b>	<b>53</b>
<b>4.5</b>	<b>Хранение данных.....</b>	<b>53</b>
4.5.1	Элементарные файлы для идентификации и управления карточками .....	54
4.5.2	Идентификационные данные карточки с интегральной схемой .....	54
4.5.2.1	Идентификационные данные микросхемы.....	54
4.5.2.2	DIR (только на карточках тахографа второго поколения) .....	55
4.5.2.3	Информация ATR (условно, только на карточках тахографа второго поколения).....	55
4.5.2.4	Расширенная информация (условно, только на карточках тахографа второго поколения) .....	55
4.5.3	Карточка водителя .....	55
4.5.3.1	Приложение тахографа (доступно для бортовых устройств первого и второго поколений).....	55
4.5.3.1.1	Идентификационные данные приложения .....	55
4.5.3.1.2	Ключи и сертификаты .....	55
4.5.3.1.3	Идентификационные данные карточки.....	55
4.5.3.1.4	Идентификационные данные владельца карточки .....	55
4.5.3.1.5	Загрузка данных карточки.....	55
4.5.3.1.6	Информация о водительском удостоверении .....	56
4.5.3.1.7	Данные о событиях .....	56
4.5.3.1.8	Данные о неисправностях .....	56
4.5.3.1.9	Данные о деятельности водителя .....	57
4.5.3.1.10	..... Данные об используемых транспортных средствах	57
4.5.3.1.11	..... Места, в которых начинаются и/или заканчиваются дневные периоды работы	58
4.5.3.1.12	..... Данные о сеансе использования карточки	58
4.5.3.1.13	..... Данные о контрольных действиях	58
4.5.3.1.14	..... Данные об особых условиях	58
4.5.3.2	Приложение тахографа второго поколения (недоступно для бортовых устройств первого поколения).....	59
4.5.3.2.1	Идентификационные данные приложения .....	59
4.5.3.2.2	Ключи и сертификаты .....	59
4.5.3.2.3	Идентификационные данные карточки.....	59
4.5.3.2.4	Идентификационные данные владельца карточки .....	59
4.5.3.2.5	Загрузка данных карточки.....	59
4.5.3.2.6	Информация о водительском удостоверении .....	59
4.5.3.2.7	Данные о событиях .....	59
4.5.3.2.8	Данные о неисправностях .....	60
4.5.3.2.9	Данные о деятельности водителя .....	61
4.5.3.2.10	..... Данные об используемых транспортных средствах	61
4.5.3.2.11	..... Места и положения, в которых начинаются и/или заканчиваются дневные периоды работы.....	61
4.5.3.2.12	..... Данные о сеансе использования карточки	62
4.5.3.2.13	..... Данные о контрольных действиях	62
4.5.3.2.14	..... Данные об особых условиях	62
4.5.3.2.15	..... Данные используемых бортовых устройств	62
4.5.3.2.16	..... Данные о местоположении при трёхчасовом непрерывном управлении	62
4.5.4	Карточка мастерской .....	63
4.5.4.1	Приложение тахографа (доступно для бортовых устройств первого и второго поколений).....	63
4.5.4.1.1	Идентификационные данные приложения .....	63

4.5.4.1.2	Ключи и сертификаты .....	63
4.5.4.1.3	Идентификационные данные карточки.....	63
4.5.4.1.4	Идентификационные данные владельца карточки .....	63
4.5.4.1.5	Загрузка данных карточки.....	63
4.5.4.1.6	Данные о калибровке и корректировке времени.....	63
4.5.4.1.7	Данные о событиях и неисправностях .....	64
4.5.4.1.8	Данные о деятельности водителя .....	64
4.5.4.1.9	Данные об используемых транспортных средствах .....	64
4.5.4.1.10	.....Данные о начале и/или окончании дневных периодов работы	64
4.5.4.1.11	..... Данные о сеансе использования карточки	64
4.5.4.1.12	..... Данные о контрольных действиях	64
4.5.4.1.13	.....Данные об особых условиях	65
4.5.4.2	Приложение тахографа второго поколения (недоступно для бортовых устройств первого поколения).....	65
4.5.4.2.1	Идентификационные данные приложения .....	65
4.5.4.2.2	Ключи и сертификаты .....	65
4.5.4.2.3	Идентификационные данные карточки.....	65
4.5.4.2.4	Идентификационные данные владельца карточки .....	65
4.5.4.2.5	Загрузка данных карточки.....	65
4.5.4.2.6	Данные о калибровке и корректировке времени.....	65
4.5.4.2.7	Данные о событиях и неисправностях .....	66
4.5.4.2.8	Данные о деятельности водителя .....	66
4.5.4.2.9	Данные об используемых транспортных средствах .....	66
4.5.4.2.10	.....Данные о начале и/или окончании дневных периодов работы	66
4.5.4.2.11	..... Данные о сеансе использования карточки	66
4.5.4.2.12	..... Данные о контрольных действиях	66
4.5.4.2.13	..... Данные используемых бортовых устройств	67
4.5.4.2.14	.....Данные о местоположении при трёхчасовом непрерывном управлении	67
4.5.4.2.15	.....Данные об особых условиях	67
4.5.5	Контрольная карточка .....	67
4.5.5.1	Приложение тахографа (доступно для бортовых устройств первого и второго поколений).....	67
4.5.5.1.1	Идентификационные данные приложения .....	67
4.5.5.1.2	Ключи и сертификаты .....	67
4.5.5.1.3	Идентификационные данные карточки.....	67
4.5.5.1.4	Идентификационные данные владельца карточки .....	67
4.5.5.1.5	Данные о контрольных действиях.....	68
4.5.5.2	Приложение тахографа второго поколения (недоступно для бортовых устройств первого поколения).....	68
4.5.5.2.1	Идентификационные данные приложения .....	68
4.5.5.2.2	Ключи и сертификаты .....	68
4.5.5.2.3	Идентификационные данные карточки.....	68
4.5.5.2.4	Идентификационные данные владельца карточки .....	68
4.5.5.2.5	Данные о контрольных действиях.....	68
4.5.6	Карточка предприятия.....	69
4.5.6.1	Приложение тахографа (доступно для бортовых устройств первого и второго поколений).....	69
4.5.6.1.1	Идентификационные данные приложения .....	69
4.5.6.1.2	Ключи и сертификаты .....	69
4.5.6.1.3	Идентификационные данные карточки.....	69
4.5.6.1.4	Идентификационные данные владельца карточки .....	69
4.5.6.1.5	Данные о деятельности предприятия .....	69
4.5.6.2	Приложение тахографа второго поколения (недоступно для бортовых устройств первого поколения).....	69

4.5.6.2.1	Идентификационные данные приложения .....	69
4.5.6.2.2	Ключи и сертификаты .....	70
4.5.6.2.3	Идентификационные данные карточки.....	70
4.5.6.2.4	Идентификационные данные владельца карточки .....	70
4.5.6.2.5	Данные о деятельности предприятия .....	70
<b>5</b>	<b>УСТАНОВКА ЗАПИСЫВАЮЩЕГО ОБОРУДОВАНИЯ.....</b>	<b>71</b>
5.1	Установка .....	71
5.2	Установочная табличка .....	72
5.3	Пломбирование.....	73
<b>6</b>	<b>ПРОВЕРКИ, ИНСПЕКЦИИ И РЕМОНТНЫЕ РАБОТЫ .....</b>	<b>73</b>
6.1	Утверждение монтажников, мастерских и производителей транспортных средств .....	74
6.2	Проверка новых или отремонтированных приборов .....	74
6.3	Инспекция установки.....	74
6.4	Регулярные проверки.....	74
6.5	Измерение погрешностей.....	75
6.6	Ремонтные работы .....	75
<b>7</b>	<b>ВЫДАЧА КАРТОЧЕК .....</b>	<b>76</b>
<b>8</b>	<b>УТВЕРЖДЕНИЕ ТИПА ЗАПИСЫВАЮЩЕГО ОБОРУДОВАНИЯ И КАРТОЧЕК ТАХОГРАФОВ ..</b>	<b>76</b>
8.1	Общие вопросы.....	76
8.2	Сертификат защиты .....	77
8.3	Сертификат функциональности.....	77
8.4	Сертификат эксплуатационной совместимости.....	78
8.5	Сертификат утверждения типа .....	79
8.6	Исключительная процедура: первые сертификаты эксплуатационной совместимости для записывающего оборудования и карточек тахографов второго поколения .....	79

## ВВЕДЕНИЕ

Система тахографов первого поколения эксплуатируется с 1 мая 2006 г. Она может использоваться до окончания срока службы на внутренних перевозках. В области международных перевозок в течение 15 лет с момента вступления в силу настоящего регламента Комиссии все транспортные средства должны быть оборудованы соответствующим требованиям «умным» тахографом, как предусмотрено в настоящем регламенте.

В настоящем дополнении содержатся требования к записывающему оборудованию и карточкам тахографов второго поколения.

Начиная с даты ввода, записывающее оборудование второго поколения устанавливается на транспортных средствах, регистрируемых впервые, и выдаются карточки тахографов второго поколения. Чтобы способствовать беспрепятственному вводу системы тахографов второго поколения,

- карточки тахографов второго поколения создаются таким образом, чтобы их можно было использовать в бортовых устройствах первого поколения,
- замены действительных карточек тахографов первого поколения в день ввода новой системы не требуется.

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

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

В настоящем дополнении представлены все требования, связанные с совместимостью систем тахографов первого и второго поколений.

В приложении 15 содержатся дополнительные подробности управления сосуществованием двух систем.

### Перечень приложений

- Приложение 1: СЛОВАРЬ ДАННЫХ
- Приложение 2: СПЕЦИФИКАЦИЯ КАРТОЧЕК ТАХОГРАФОВ
- Приложение 3: ПИКТОГРАММЫ
- Приложение 4: РАСПЕЧАТКИ
- Приложение 5: ОТОБРАЖЕНИЕ
- Приложение 6: ПЕРЕДНИЙ СОЕДИНИТЕЛЬ ДЛЯ КАЛИБРОВКИ И ЗАГРУЗКИ
- Приложение 7: ПРОТОКОЛЫ ЗАГРУЗКИ ДАННЫХ
- Приложение 8: ПРОТОКОЛ КАЛИБРОВКИ
- Приложение 9: УТВЕРЖДЕНИЕ ТИПА И ПЕРЕЧЕНЬ ОБЯЗАТЕЛЬНЫХ ИСПЫТАНИЙ
- Приложение 10: ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ
- Приложение 11: ОБЩИЕ МЕХАНИЗМЫ ЗАЩИТЫ
- Приложение 12: ОПРЕДЕЛЕНИЕ МЕСТОПОЛОЖЕНИЯ ПРИ ПОМОЩИ ГЛОБАЛЬНОЙ НАВИГАЦИОННОЙ СПУТНИКОВОЙ СИСТЕМЫ (ГНСС)

Приложение 13: ИНТЕРФЕЙС ИТС

Приложение 14: ФУНКЦИЯ УДАЛЁННОЙ СВЯЗИ

Приложение 15: МИГРАЦИЯ: УПРАВЛЕНИЕ СОСУЩЕСТВОВАНИЕМ ОБОРУДОВАНИЯ РАЗНЫХ ПОКОЛЕНИЙ

Приложение 16: АДАПТЕР ДЛЯ ТРАНСПОРТНЫХ СРЕДСТВ КАТЕГОРИЙ M1 И N1

## Определения

В настоящем дополнении:

- a) активизация:**  
фаза, во время которой тахограф полностью вводится в эксплуатацию и выполняет все функции, включая функции безопасности, при помощи карточки мастерской;
- b) опознавание:**  
функция, предназначенная для установления и удостоверения заявленной личности;
- c) подлинность:**  
свойство, означающее, что информация поступает от стороны, личность которой можно проверить;
- d) встроенный контроль:**  
испытания, проводимые по требованию, которые запускает оператор или внешнее оборудование;
- e) календарный день:**  
сутки с 00:00 часов до 24:00 часов. Все календарные дни определяются по системе всемирного координированного времени (UTC);
- f) калибровка «умного» тахографа:**  
обновление или подтверждение параметров транспортного средства, которые должны храниться в блоке памяти. К параметрам транспортных средств относятся идентификационные данные транспортного средства (VIN, VRN и государство-член регистрации) и характеристики транспортного средства (w, k, l, диаметр покрышки, установки устройства ограничения скорости (если есть), текущее время UTC, текущее показание одометра); во время калибровки записывающего оборудования в блоке памяти также сохраняются типы и идентификаторы всех имеющихся пломб утверждения типа; любое обновление или подтверждение времени UTC считается уточнением времени, а не калибровкой, при условии, что это не противоречит требованию 409;  
*калибровка записывающего оборудования требует использования карточки мастерской;*
- g) номер карточки:**  
номер в виде 16 буквенно-цифровых знаков, который однозначно идентифицирует карточку тахографа в данном государстве-члене. Номер карточки включает в себя порядковый индекс (при необходимости), индекс замены и индекс возобновления; таким образом карточка однозначно идентифицируется с помощью кода выдавшего её государства-члена и номера карточки;
- h) порядковый индекс карточки:**  
14-й буквенно-цифровой знак номера карточки, который используется для дифференциации различных карточек, выданных 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:**  
16-й буквенно-цифровой знак номера карточки, который увеличивается в каждом случае возобновления карточки;
- j) индекс замены карточки:**

15-й буквенно-цифровой знак номера карточки, который увеличивается в каждом случае замены карточки;

**к) характеристический коэффициент транспортного средства:**

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

**л) карточка предприятия:**

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

**м) постоянная величина записывающего оборудования:**

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);

**п) непрерывное время вождения рассчитывается внутри записывающего оборудования следующим образом<sup>1</sup>:**

непрерывное время вождения вычисляется как текущее суммарное время вождения определённого водителя с окончания последнего периода его ДОСТУПНОСТИ или ПЕРЕРЫВА/ОТДЫХА или НЕИЗВЕСТНО<sup>2</sup> длиной 45 минут или более (такой период может быть разделён в соответствии с Регламентом (ЕС) № 561/2006). В процессе расчёта при необходимости учитываются данные о прошлых видах деятельности, записанных на карточке водителя. Если водитель не вставил карточку, расчёт производится на основе данных, записанных в блоке памяти и относящихся к текущему периоду, в течение которого карточка вставлена не была, и к соответствующему временному интервалу.

**о) контрольная карточка:**

карточка тахографа, выданная органами государства-члена национальному компетентному контролирующему органу, который назначает орган контроля и, возможно, лицо, ответственное за контроль, и предоставляет доступ к данным, хранящимся в блоке памяти или на карточках водителя, а также, возможно, на карточках мастерских для считывания, печати и/или загрузки; Он также предоставляет доступ к функции придорожной проверки калибровки и к данным устройства, считывающего показания средства удалённой связи для раннего обнаружения.

**р) суммарная продолжительность перерывов рассчитывается внутри записывающего оборудования следующим образом<sup>1</sup>:**

<sup>1</sup> Такой способ вычисления непрерывного времени вождения и суммарной продолжительности перерывов помогает записывающему оборудованию вычислять предупреждение, касающееся непрерывного времени вождения. Он никак не предопределяет юридического толкования этих отрезков времени. Если представленные определения устарели из-за изменений других значимых правовых актов, можно использовать альтернативные методы вычисления непрерывного времени вождения и суммарной продолжительности перерывов.

<sup>2</sup> НЕИЗВЕСТНЫЕ периоды соответствуют периодам, когда карточка водителя не была вставлена в записывающее оборудование и когда действия водителя не вводились вручную.

суммарная продолжительность перерывов от вождения вычисляется как текущее суммарное время ДОСТУПНОСТИ или ПЕРЕРЫВА/ОТДЫХА или НЕИЗВЕСТНО<sup>2</sup> длиной 15 минут или более определённого водителя с окончания последнего периода его ДОСТУПНОСТИ или ПЕРЕРЫВА/ОТДЫХА или НЕИЗВЕСТНО<sup>2</sup> длиной 45 минут или более (такой период может быть разделён в соответствии с Регламентом (ЕС) № 561/2006).

В процессе расчёта при необходимости учитываются данные о прошлых видах деятельности, записанных на карточке водителя. Периоды, за которые нет данных и продолжительность которых отображается знаком «минус» (начало периода, за который нет данных, наступившее раньше завершения этого же периода), что обусловлено нестыковкой во времени между двумя различными записывающими устройствами, в процессе расчёта не учитываются.

Если водитель не вставил карточку, расчёт производится на основе данных, записанных в блоке памяти и относящихся к текущему периоду, в течение которого карточка вставлена не была, и к соответствующему временному интервалу.

**q) блок памяти:**

электронное устройство хранения данных, встроенное в записывающее оборудование;

**r) цифровая подпись:**

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

**s) загрузка:**

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 изменяет или не удаляет никакие хранящиеся данные;

Производители бортовых устройств, оснащённых «умными» тахографами, и производители оборудования для загрузки файлов данных предпринимают все разумные меры для обеспечения того, чтобы загрузка таких данных осуществлялась транспортными предприятиями или водителями с минимальной задержкой.

Загрузка подробного файла скорости может быть необязательной, чтобы установить соответствие Регламенту (ЕС) № 561/2006, но она может быть полезной для других целей, например, при расследовании аварии.

**t) карточка водителя:**

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

**u) эффективная окружность колёс:**

среднее значение расстояний, пройденных каждым из колёс, приводящих в движение транспортное средство (ведущими колесами) за один полный оборот. Эти расстояния измеряются при стандартных условиях испытания в соответствии с требованием 414 и выражаются как « $l = \dots$  мм». Производители транспортных средств могут использовать вместо фактического измерения этого расстояния теоретический метод расчёта, который учитывает распределение веса на оси транспортного средства в нормальных условиях эксплуатации без груза<sup>3</sup>. Методы такого теоретического расчёта должны быть утверждены компетентным органом государства-члена и могут применяться только до активизации тахографа;

---

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



- v) событие:**  
сбой в работе, обнаруженный «умным» тахографом, который может быть вызван попыткой мошенничества;
- w) внешняя ГНСС:**  
система, состоящая из приёмника ГНСС, когда бортовое устройство не является одноэлементной единицей, и других компонентов, необходимых для защиты передачи данных о местоположении в другие элементы бортового устройства;
- x) неисправность:**  
сбой в работе, обнаруженный «умным» тахографом, который может быть вызван сбоем или поломкой оборудования;
- y) приёмник ГНСС:**  
электронное устройство, принимающее сигналы одной или нескольких глобальных навигационных спутниковых систем (ГНСС) и производящее их цифровую обработку, чтобы предоставить информацию о местоположении, скорости и времени.
- z) установка:**  
установка тахографа на транспортном средстве;
- aa) эксплуатационная совместимость:**  
способность систем и основных деловых процессов обмениваться данными и делиться информацией;
- bb) интерфейс:**  
средство, обеспечивающее возможность связи и взаимодействия между системами;
- cc) местоположение:**  
географические координаты транспортного средства в определённый момент времени;
- dd) датчик движения:**  
деталь тахографа, подающая сигнал, который отображает скорость транспортного средства и/или пройденное расстояние;
- ee) недействительная карточка:**  
карточка, которая определена как неисправная или которую не удалось идентифицировать, или срок действия которой еще не наступил, или срок действия которой уже истёк;
- ff) открытый стандарт:**  
стандарт, указанный в документе спецификации стандартов, находящемся в свободном доступе или доступном за символическую плату, который можно копировать, распространять или использовать бесплатно или за символическую плату.
- gg) вне области применения:**  
когда использование записывающего оборудования не требуется в соответствии с положениями Регламента (ЕС) № 561/2006.
- hh) превышение скорости:**  
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 определённых категорий моторных транспортных средств в Сообществе<sup>4</sup>, с последними поправками;

**ii) периодическая проверка:**

ряд действий, производимых для проверки должной работы тахографа, соответствия его установок параметрам транспортного средства и отсутствия средства манипулирования, прикреплённых к тахографу;

**jj) печатающее устройство:**

компонент записывающего оборудования, который позволяет распечатывать хранящиеся данные;

**kk) удалённая связь для раннего обнаружения:**

связь между средством удалённой связи для раннего обнаружения и считывающим устройством удалённой связи для раннего обнаружения во время целевых придорожных проверок с целью удалённого обнаружения возможного манипулирования или неправомерного использования записывающего оборудования;

**ll) средство удалённой связи:**

оборудование бортового устройства, используемое для проведения целевых придорожных проверок;

**mm) считывающее устройство удалённой связи для раннего обнаружения:**

система, используемая сотрудниками контроля для целевых придорожных проверок.

**nn) возобновление:**

выдача новой карточки тахографа, когда срок действия используемой карточки подходит к концу или когда она обнаруживает сбой в работе и возвращена выдавшему её органу. Возобновление всегда однозначно указывает на то, что две действительные карточки одновременно использоваться не могут;

**oo) ремонт:**

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

**pp) замена карточки:**

выдача карточки тахографа взамен действительной карточки, которая утеряна, украдена или неисправна и не возвращена выдавшему её органу. Замена всегда предполагает риск того, что могут одновременно использоваться две действительные карточки;

**qq) сертификация безопасности:**

процедура органа сертификации по общим критериям для удостоверения того, что записывающее оборудование (или компонент) или карточка тахографа, в отношении которой проводится расследование, отвечает требованиям безопасности, установленным в соответствующих описаниях защиты;

**rr) самопроверка:**

проверки, производимые на цикличной основе и в автоматическом режиме записывающим оборудованием на предмет обнаружения неисправностей;

**ss) замеры времени:**

постоянная цифровая запись координированных универсальных даты и времени (UTC);

---

<sup>4</sup> ОЖ L 057, 2.3.1992, стр. 27 и 28.

- tt) корректировка времени:**  
автоматическое регулирование текущего времени через регулярные промежутки времени и при максимальном допуске в одну минуту, или корректировка во время калибровки;
- uu) размер шины:**  
определённые размеры шин (внешних ведущих колёс) в соответствии с Директивой 92/23/ЕЭС от 31 марта 1992 г.<sup>5</sup>, с последними поправками;
- vv) идентификационные признаки транспортного средства:**  
идентификационные номера транспортного средства: регистрационный номер транспортного средства (VRN) с указанием государства-члена регистрации и идентификационный номер транспортного средства (VIN)<sup>6</sup>;
- ww) в целях вычисления в записывающем оборудовании – неделя:**  
период с 00:00 часов UTC в понедельник до 24:00 часов UTC в воскресенье;
- xx) карточка мастерской:**  
карточка тахографа, выданная органами государства-члена назначенным сотрудникам производителя тахографов, установщика, производителя транспортных средств или мастерской, апробированных данным государством-членом, по которой устанавливается личность владельца карточки и которая позволяет проводить испытания, калибровку и активизацию тахографов и/или загружать из них данные;
- уу) адаптер:**  
устройство, передающее сигнал, постоянно отражающий скорость транспортного средства и/или пройденное расстояние, кроме сигнала, используемого для обнаружения независимого движения, которое:
- устанавливается и эксплуатируется только на транспортных средствах типов M1 и N1 (в соответствии с приложением II к Директиве Совета 2007/46/ЕС, с последними поправками), эксплуатируемых с 1 мая 2006 г.,
  - устанавливается, если механически невозможно установить никакие другие датчики движения, которые в остальном соответствуют положениям настоящего дополнения и его приложений 1-15,
  - устанавливается между бортовым устройством и встроенными датчиками или альтернативными интерфейсами, в которых генерируются импульсы скорости/расстояния,
  - со стороны бортового устройства ведут себя так же, как если бы к бортовому устройству был подключён датчик движения, в соответствии с положениями настоящего дополнения и его приложений 1-16;
- использование такого адаптера в описанных выше транспортных средствах делает возможными установку и правильную эксплуатацию бортового устройства в соответствии со всеми требованиями настоящего дополнения,  
в таких транспортных средствах в состав «умного» тахографа входят кабели, адаптер и бортовое устройство;
- zz) целостность данных:**  
точность и согласованность хранящихся данных, выражающиеся в отсутствии любых изменений данных между двумя обновлениями записи. Целостность предполагает, что данные являются точной копией оригинальной версии, т.е. что в процессе записи и считывания на карточке тахографа или в специальном оборудовании или во время передачи любыми каналами связи данные не нарушены;

<sup>5</sup> ОЖ L 129, 14/05/1992, стр. 95.

<sup>6</sup> Директива 76/114/ЕЭС, 18/12/1975; ОЖ L 024, 30/01/1976, стр. 1-5.

**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;

**bbb) система «умного» тахографа:**

записывающее 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 удалённой связи и любое другое оборудование для загрузки и анализа данных, калибровки, генерирования, контроля или введения элементов безопасности и проч.;

**ccc) дата ввода:**

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

*Это дата, после которой впервые регистрируемые транспортные средства:*

- снабжаются тахографом, соединённым с сервисом установления местоположения на основе спутниковой навигационной системы,
- могут передавать данные для целевых придорожных проверок компетентным контролирующим органам во время движения транспортного средства,
- и могут быть оснащены стандартизированными интерфейсами, позволяющими использовать данные, записанные или произведённые тахографами, в оперативном режиме на внешних устройствах.

**ddd) описание защиты:**

документ, используемый в рамках процедуры сертификации в соответствии с общими критериями, представляющий собой независимую от внедрения спецификацию требований обеспечения информационной безопасности;

**eee) точность ГНСС:**

в контексте регистрации местоположения при помощи глобальной навигационной спутниковой системы (ГНСС) на тахографах – это значение показателя снижения точности при определении положения в горизонтальной плоскости (HDOP), вычисляемое как минимум значений HDOP, собранных из имеющихся ГНСС.

## 2 Общие характеристики и функции записывающего оборудования

### 2.1 Общие характеристики

Цель записывающего оборудования состоит в регистрации, хранении, отображении, распечатке и генерации данных о деятельности водителя.

Любое транспортное средство, оснащённое записывающим оборудованием, удовлетворяющим положениям настоящего дополнения, должно быть оборудовано спидометром и одометром. Эти функции могут быть встроены в записывающее оборудование.

- 01) Записывающее оборудование включает в себя электропроводку, датчик движения и бортовое устройство.
- 02) Интерфейс между датчиками движения и бортовыми устройствами соответствует требованиям, указанным в приложении 11.
- 03) Бортовое устройство соединено с глобальной навигационной спутниковой системой (или системами), как указано в приложении 12.
- 04) Бортовое устройство поддерживает связь со считывающими устройствами удалённой связи для раннего обнаружения, как указано в приложении 14.
- 05) Бортовое устройство может включать в себя интерфейс ИТС, как указано в приложении 13. Записывающее оборудование может быть подключено к другим объектам через дополнительные интерфейсы и/или факультативный интерфейс ИТС.
- 06) Любое включение или подсоединение к записывающему оборудованию любой функции, устройства или устройств, сертифицированных или не сертифицированных, не должно создавать (или быть способным создавать) помехи, которые могут нарушить надлежащую и безопасную работу записывающего оборудования и положения настоящего регламента.

Пользователи записывающего оборудования вводят свои идентификационные данные в устройство с помощью карточек тахографа.

- 07) Записывающее оборудование предоставляет право селективного доступа к данным и функциям в зависимости от вида и/или идентификационных данных пользователя.

Записывающее оборудование регистрирует и хранит данные в блоке памяти, в устройстве удалённой связи и на карточках тахографов.

Это делается в соответствии с Директивой 95/46/ЕС от 24 октября 1995 г. защите лиц при обработке личных данных и о свободном движении таких данных<sup>7</sup>, Директивой 2002/58/ЕС от 12 июля 2002 г. об обработке личных данных и защите конфиденциальности в секторе электронных коммуникаций<sup>8</sup> и статьёй 7 Регламента (ЕС) № 165/2014.

### 2.2 Функции

- 08) Записывающее оборудование выполняет следующие функции:

<sup>7</sup> ОЖ L 281, 23/11/1995, стр. 31.

<sup>8</sup> ОЖ L 201, 31/07/2002, стр. 37.

- контроль за вводом и извлечением карточек,
- замеры скорости, расстояния и местоположения,
- измерение времени,
- контроль за деятельностью водителя,
- контроль за статусом водителя,
- ручной ввод данных водителем:
  - ввод данных о местах, в которых начинаются и/или заканчиваются дневные периоды работы,
  - ручной ввод данных о деятельности водителя,
  - ввод данных об особых условиях,
- реагирование на блокировку, установленную предприятием,
- контроль за деятельностью контроля,
- обнаружение событий и/или неисправностей,
- проведение 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,
- отображение,
- печать,
- предупреждение,
- загрузка данных на внешние носители,
- удалённая связь для целевых придорожных проверок,
- выходные данные в дополнительные устройства,
- калибровка,
- придорожные проверки калибровки,
- корректировка времени.

## 2.3 Режимы работы

- 09) Записывающее оборудование работает в четырёх режимах:
- рабочий режим,
  - режим контроля,
  - режим калибровки,
  - режим предприятия.
- 10) Записывающее оборудование переходит в следующий режим работы в соответствии с действующими карточками тахографа, вставленными в устройства интерфейса карточек. Для определения режима работы поколение карточки тахографа значения не имеет, при условии, что введённая карточка действительна. Карточка мастерской первого поколения всегда считается недействительной при вводе в бортовое устройство второго поколения.

Режим работы		Считывающее устройство водителя				
		Карточка не вставлена	Карточка водителя	Контрольная карточка	Карточка мастерской	Карточка предприятия
Считыва	Карточка не вставлена	Рабочий	Рабочий	Контроль	Калибровка	Предприятие

	Карточка водителя	Рабочий	Рабочий	Контроль	Калибровка	Предприятие
	Контрольная карточка	Контроль	Контроль	Контроль (*)	Рабочий	Рабочий
	Карточка мастерской	Калибровка	Калибровка	Рабочий	Калибровка (*)	Рабочий
	Карточка предприятия	Предприятие	Предприятие	Рабочий	Рабочий	Предприятие (*)

(\*) В подобных случаях записывающее оборудование использует только карточку тахографа, введённую в считывающее устройство водителя.

- 11) Записывающее устройство не принимает недействительные введённые карточки, за исключением отображения, печати или загрузки данных, хранящихся на истёкшей карте, которые остаются возможными.
- 12) Все функции, перечисленные в пункте 2.2, работают во всех режимах с учётом следующих исключений:
- функция калибровки доступна только в режиме калибровки,
  - функция придорожной проверки калибровки доступна только в режиме контроля,
  - функция реагирования на блокировку, установленную предприятием, доступна только в режиме предприятия,
  - функция контроля деятельности контроля доступна только в режиме контроля,
  - Функция загрузки недоступна в рабочем режиме (за исключением того, что предусмотрено в требовании 193) и за исключением загрузки карточки водителя, если в бортовое устройство не вставлены никакие другие карточки.
- 13) Записывающее оборудование может выводить любые данные на дисплей, печать или на внешние интерфейсы с учётом следующих исключений:
- в рабочем режиме любые личные идентификационные данные (фамилия и имя (имена), не соответствующие данным на вставленной карточке тахографа, гасятся, а любой номер карточки, не соответствующий данным на вставленной карточке тахографа, гасится частично (гасится каждый нечётный знак слева направо),
  - в режиме предприятия данные, касающиеся водителя (требования 102, 105 и 108), могут выводиться только за периоды, когда они не заблокированы или не заблокированы другим предприятием (идентифицируемым с помощью первых 13 цифр номера карточки предприятия),
  - когда в записывающее оборудование карточка не вставлена, данные, касающиеся водителя, могут выводиться только за текущий и восемь предыдущих календарных дней,
  - личные данные из бортового устройства не выводятся через интерфейс ИТС бортового устройства, если нет подтверждённого согласия водителя, с которым связаны данные,
  - бортовые устройства при нормальных условиях эксплуатации служат 15 лет с даты выдачи сертификата бортового устройства, но для загрузки данных бортовые устройства могут эксплуатироваться ещё 3 месяца дополнительно.

## 2.4 Защита

Система защиты имеет целью уберечь блок памяти от несанкционированного доступа к зарегистрированным данным и их манипуляции и регистрировать любые случаи таких попыток, сохранить целостность и подлинность данных, передаваемых между датчиком движения и бортовым устройством, сохранить целостность и подлинность данных, передаваемых между записывающим оборудованием и карточками тахографа, сохранить целостность и подлинность данных, передаваемых между записывающим оборудованием и внешней ГНСС, сохранить конфиденциальность, целостность и подлинность данных, передаваемых через систему удалённой связи для раннего предупреждения в целях контроля и проверять целостность и подлинность загружаемых данных.

- 14) Для обеспечения защиты системы следующие компоненты должны соответствовать требованиям безопасности, представленным в описаниях защиты согласно приложению 10:
- бортовое устройство,
  - карточка тахографа,
  - датчик движения,
  - внешняя ГНСС (данное описание необходимо и применимо только к внешней ГНСС).

### **3 Требования к конструкции и функциям записывающего оборудования**

#### **3.1 Контроль за вводом и извлечением карточек**

- 15) Записывающее оборудование контролирует интерфейс для считывания карточек в целях регистрации фактов ввода и извлечения карточки.
- 16) После ввода карточки записывающее оборудование устанавливает, является ли вставленная карточка действующей карточкой тахографа, и в таком случае определяет тип и поколение карточки. Если карточка с таким же номером карточки и более высоким индексом возобновления уже была введена в записывающее оборудование, карточка признаётся недействительной. Если карточка с таким же номером карточки и индексом возобновления и с более высоким индексом замены уже была введена в записывающее оборудование, карточка признаётся недействительной.
- 17) Карточки тахографов первого поколения признаются недействительными в записывающем оборудовании, после того как мастерская закрывает возможность использования карточек тахографа первого поколения в соответствии с приложением 15 (требование MIG003).
- 18) Карточки мастерской первого поколения, вводимые в записывающее оборудование второго поколения, признаются недействительными.
- 19) Записывающее оборудование 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 карточки тахографа возможно только в случае остановки транспортного средства и после записи соответствующих данных в память карточки. Извлечение 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 и указывает значение одометра, соответствующее полному расстоянию, пройденному транспортным средством, при помощи импульсов, генерируемых датчиком движения.
- 23) Данная функция обеспечивает постоянное измерение и указывает значение спидометра транспортного средства при помощи импульсов, генерируемых датчиком движения.
- 24) Функция измерения скорости также предоставляет информацию о том, что транспортное средство движется или остановлено. Транспортное средство считается движущимся в том случае, если эта функция обнаруживает сигнал величиной 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 (одометр), установленные на любом транспортном средстве, оснащённом записывающим оборудованием, соответствующим положениям настоящего регламента, удовлетворяют требованиям, касающимся максимальных допусков, указанных в настоящем дополнении (см. 3.2.1 и 3.2.2).
- 26) Для выявления манипуляций с данными движения информация из датчика движения проверяется по информации о движении транспортного средства из приёмника ГНСС и (необязательно) по другим источникам, не зависимым от датчика движения.
- 27) Эта функция замеряет местоположение транспортного средства, чтобы была возможность автоматически регистрировать:
- места, в которых водитель и/или второй водитель начинают свой дневной рабочий период;
  - места, в которых непрерывное время вождения достигает значения, кратного трём часам;
  - места, в которых водитель и/или второй водитель завершают свой дневной рабочий период.

### 3.2.1 Измерение пройденного расстояния

- 28) Пройденное расстояние может измеряться так:
- чтобы оно включало суммарное перемещение как вперёд, так и назад или
  - чтобы оно включало только перемещение вперёд.
- 29) Записывающее оборудование должно иметь возможность измерять расстояние от 0 до 9 999 999,9 км.
- 30) Пробег должен измеряться с соблюдением следующих допусков (расстояния не менее 1 000 м):
- $\pm 1\%$  до установки,
  - $\pm 2\%$  при установке и регулярных проверках,
  - $\pm 4\%$  в процессе эксплуатации.
- 31) Пробег должен измеряться с точностью не менее 0,1 км.

### 3.2.2 Измерение скорости

- 32) Записывающее оборудование должно иметь возможность измерять скорость от 0 до 220 км/ч.
- 33) В целях обеспечения максимального допуска на показываемую скорость на уровне  $\pm 6$  км/ч в процессе эксплуатации и с учётом:
- $\pm$  допуска 2 км/ч на разброс входных данных (разброс, обусловленный шинами, ...),
  - $\pm$  допуска 1 км/ч на измерения, производимые во время установки или регулярных проверок,
- записывающее оборудование должно обеспечивать, в диапазоне скоростей от 20 до 180 км/ч, и характеристических коэффициентов транспортного средства от 4 000 до 25 000 имп./км, измерение скорости с точностью  $\pm 1$  км/ч (при постоянной скорости).
- Примечание: точность хранения данных обуславливает дополнительный допуск на данные скорости, регистрируемой записывающим оборудованием, на уровне  $\pm 0,5$  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  $2 \text{ м/с}^2$ .
- 35) Скорость измеряется с точностью не менее 0,1 км/ч.

### **3.2.3 Определение местоположения**

- 36) Записывающее оборудование замеряет абсолютное местоположение транспортного средства при помощи приёмника ГНСС.
- 37) Абсолютное местоположение измеряется географическими координатами 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 (записи, обмен данными) и для всех распечаток, указанных в приложении 4 «Распечатки».
- 40) Для визуализации местного времени есть возможность изменения разницы в выводимом на дисплей времени с помощью получасовых интервалов. Никакие другие изменения в отрицательную или положительную стороны, кратные получасовым интервалам, не допускаются;
- 41) Отклонение времени не превышает  $\pm 2$  секунд в день в условиях, предусмотренных для официального утверждения типа, при отсутствии любых корректировок времени.
- 42) Время измеряется с точностью не менее 1 секунды.
- 43) Измерение времени не нарушается в результате прекращения электропитания от внешнего источника в течение менее 12 месяцев в условиях, предусмотренных для официального утверждения типа.

### **3.4 Контроль за деятельностью 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) Когда транспортное средство движется, в отношении водителя автоматически выбирается функция УПРАВЛЕНИЕ, а в отношении второго водителя автоматически выбирается функция ГОТОВНОСТЬ.
- 48) Когда транспортное средство останавливается, в отношении водителя автоматически выбирается функция РАБОТА.
- 49) Считается, что первое изменение вида деятельности в течение 120 секунд после автоматического переключения на функцию 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 УПРАВЛЕНИЕ регистрируется непосредственно до этой минуты и сразу же после неё, 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 места, в которых, по утверждению 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) Во время извлечения карточки водителя записывающее оборудование предлагает (второму) водителю ввести «место, в котором заканчивается дневной период работы».
- 59) Водитель вводит текущее местоположение транспортного средства, и это считается временной записью.
- 60) Места, в которых начинаются и/или заканчиваются дневные периоды работы, можно вводить при помощи команд в меню. Если в течение одной календарной минуты происходит ввод более чем одной такой записи, сохраняются только последняя запись места начала и последняя запись места окончания.

#### **3.6.2 Ручной ввод данных о деятельности водителя и согласия водителя для интерфейса ИТС**

- 61) При введении карточки водителя (или мастерской) и только тогда записывающее оборудование позволяет вручную вводить записи о деятельности. Ручной ввод данных о деятельности осуществляется с указанием значений местного времени и даты в часовом поясе (относительно UTC), указанном в данный момент в бортовом устройстве.

В момент ввода карточки водителя или мастерской владелец карточки получает напоминание:

- о дате и времени последнего извлечения карточки;
- (необязательно) о местном времени, установленном в настоящий момент в бортовом устройстве.

При первом вводе определённой карточки водителя или мастерской, в настоящее время неизвестной для бортового устройства, владельцу карточки предлагается выразить своё согласие на вывод личных данных, связанных с тахографом, через факультативный интерфейс ИТС.

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

Можно вводить данные о деятельности со следующими ограничениями:

- Вид деятельности отображается как УПРАВЛЕНИЕ, ГОТОВНОСТЬ или ПЕРЕРЫВ/ОТДЫХ;
- Время начала и окончания находится только в пределах периода между последним извлечением и текущим вводом карточки;
- Виды деятельности не должны дублироваться во времени.

При необходимости можно вводить записи 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 окончания каждой деятельности. В отношении любого отрезка времени между последним извлечением карточки и текущим её вводом владелец карточки может не указывать никакого вида деятельности.

При ручном вводе записей, связанных с вводом карточки, если применимо, владелец карточки может указать:

- место, в котором завершился предыдущий дневной период работы, связанный с определённым временем (и таким образом переписать запись, сделанную при последнем извлечении карточки),
- место, в котором начинается текущий дневной период работы, связанное с определённым временем.

Если владелец карточки не вводит никакого места, в котором начинается или кончается период работы, при ручном вводе записей, связанных с введением карточки, такие действия считаются декларацией того, что его период работы с последнего извлечения карточки не изменился. Следующая запись места, в котором заканчивается предыдущий дневной период работы, записывается поверх временной записи, сделанной при последнем извлечении карточки.

Если место введено, оно записывается на соответствующей карточке тахографа.

Ручные записи прерываются, если:

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

Допускаются дополнительные перерывы, например, перерыв после определённого периода бездействия пользователя. Если ручной ввод записи прерывается, записывающее оборудование подтверждает все завершённые записи места и вида деятельности (если указано недвусмысленное место и время или вид деятельности, время начала и время окончания).

Если во время ручного ввода записей о деятельности на уже введённой карточке вводится карточка второго водителя или мастерской, ручные записи первой карточки можно завершить, прежде чем начинать ручной ввод для второй карточки.

Владелец карточки может вводить записи вручную согласно следующей минимальной процедуре:

- Вручную в хронологическом порядке ввести виды деятельности за последний период между последним извлечением карточки и текущим её вводом.
- Время начала первой деятельности совпадает со временем извлечения карточки. Для каждой последующей записи время начала устанавливается заранее непосредственно сразу после времени окончания предыдущей записи. Вид деятельности и время окончания выбираются для каждого вида деятельности.

Процедура заканчивается, когда время завершения деятельности, введённой вручную, соответствует времени ввода карточки. После этого записывающее оборудование даёт владельцу карточки возможность изменить любые данные о деятельности, введённые вручную, до их подтверждения с помощью выбранной конкретной команды. После этого никакие изменения невозможны.

### 3.6.3 Ввод данных об особых условиях

- 62) Записывающее оборудование даёт водителю возможность в режиме реального времени вводить следующие два особых условия:
- НЕПРИМЕНИМО (начало, конец)
  - ПАРОМ/Ж/Д ПЕРЕЕЗД (начало, конец)

Функция ПАРОМ/Ж/Д ПЕРЕЕЗД может не открыться, если открыта функция НЕПРИМЕНИМО. Открытая функция НЕПРИМЕНИМО должна автоматически закрыться записывающим оборудованием в случае ввода или извлечения карточки водителя.

Открытая функция НЕПРИМЕНИМО блокирует следующие события и предупреждения:

- Управление без соответствующей карточки,
- Предупреждения, связанные с непрерывным временем вождения.

Пометка начала функции ПАРОМ/Ж/Д ПЕРЕЕЗД устанавливается перед выключением двигателя на пароме/поезде.

Открытая функция ПАРОМ/Ж/Д ПЕРЕЕЗД заканчивается в любом из следующих случаев:

- Водитель вручную закрывает функцию ПАРОМ/Ж/Д ПЕРЕЕЗД
- Водитель извлекает свою карточку

Открытая функция ПАРОМ/Ж/Д ПЕРЕЕЗД заканчивается, если она более недействительна в соответствии с правилами, изложенными в Регламенте (ЕС) № 561/2006.

## 3.7 Реагирование на блокировку, установленную предприятием

- 63) Данная функция позволяет управлять установленной предприятием блокировкой в целях ограничения доступа к данным в режиме работы предприятия только для самого предприятия.
- 64) Функция блокировки предприятием заключается в указании даты/времени начала (блокировка) и даты/времени завершения (разблокировка) 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 всё ещё находится в положении «включено».

### 3.8 Мониторинг деятельности контроля

- 69) Данная функция предусмотрена для осуществления контроля за операциями ВЫВОД НА ДИСПЛЕЙ, ПЕЧАТЬ, БОРТОВОЕ УСТРОЙСТВО, ЗАГРУЗКА и ПРИДОРОЖНАЯ КАЛИБРОВКА, производимых в режиме контроля.
- 70) Данная функция также контролирует операцию КОНТРОЛЬ ЗА ПРЕВЫШЕНИЕМ СКОРОСТИ при работе в режиме контроля. Считается, что контроль за превышением скорости производится в том случае, если в режиме контроля на принтер или дисплей выведено сообщение «превышение скорости» или если из блока памяти данных бортового устройства загружаются данные «события и неисправности».

### 3.9 Обнаружение 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, если введена любая недействительная карточка, если введена карточка водителя, которая уже была заменена и/или если истекает срок действия введённой карточки.

#### 3.9.2 Событие «несовместимость карточек»

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

Несовместимость карточек		Считывающее устройство водителя				
		Карточка не вставлена	Карточка водителя	Контрольная карточка	Карточка мастерской	Карточка предприятия
Считывающее устройство	Карточка не вставлена					
	Карточка водителя				X	
	Контрольная карточка			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 предшествует дате/времени последнего извлечения карточки водителя, считываемым с карточки.

### 3.9.4 Событие «Управление 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 (или недействительная карточка)	Карточка водителя	Контрольная карточка	Карточка мастерской	Карточка предприятия
Считывающее устройство	Карточка не вставлена (или недействительная карточка)	X		X		X
	Карточка водителя	X		X	X	X
	Контрольная карточка	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 вставляется 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 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 касается только 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 мс. Предельное значения прерванного питания устанавливает производитель. В случае падения напряжения в результате запуска двигателя транспортного средства данное событие отображаться не должно.

### **3.9.9 Событие «Ошибка связи со средством удалённой связи»**

- 80) Данное событие отображается, за исключением режима калибровки, когда средство удалённой связи не подтверждает успешного получения данных удалённой связи, отправленных из бортового устройства, более чем с трёх попыток.

### **3.9.10 Событие «Отсутствие информации о местоположении из приёмника ГНСС»**

- 81) Данное событие отображается, за исключением режима калибровки, в случае отсутствия информации о местоположении из приёмника ГНСС (внутреннего или внешнего) в течение более трёх часов суммарного времени управления.

### **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 подлинности данных в процессе передачи данных между датчиком движения и бортовым устройством.

### **3.9.13 Событие «Противоречивая информация о движении транспортного средства»**

- 84) Данное событие отображается, за исключением режима калибровки, в случае, если информации о движении, полученной из датчика движения, противоречит информация, полученная из внутреннего устройства ГНСС или внешнего устройства ГНСС и, возможно, из других независимых источников, как указано в приложении 12. Данное событие не отображается во время переправы на пароме/поезде, при активной функции НЕПРИМЕНИМО или если нет информации о местоположении из приёмника 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 10, за исключением режима калибровки.

### 3.9.15 Событие «Противоречивая информация о времени»

- 86) Данное событие отображается, за исключением режима калибровки, если бортовое устройство обнаруживает несоответствие длиной более 1 минуты между временем функции замера времени бортового устройства и временем приёмника ГНСС. 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, бортовое устройство не будет генерировать другие события такого же характера в течение следующих 12 часов. Данное событие не отображается в тех случаях, когда приёмник ГНСС не обнаруживает действительного сигнала ГНСС в течение последних 30 дней. Однако если информация о местоположении из приёмника ГНСС появляется снова, производится автоматическая корректировка времени.

### 3.9.16 Неисправность «Карточка»

- 87) Данное уведомление отображается в случае неисправности карточки тахографа, возникшей в процессе работы.

### 3.9.17 Неисправность «Записывающее оборудование»

- 88) 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 приёмника ГНСС или внешнего устройства ГНСС
  - Неисправность средства удалённой связи

## 3.10 Встроенные проверки и самопроверки

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

Подсистема проверки	Самопроверка	Встроенная система проверок
Программное обеспечение		Целостность
Блок памяти	Доступ	Доступ, целостность данных
Устройство интерфейса карточек	Доступ	Доступ
Клавиатура		Ручная проверка
Принтер	(устанавливается производителем)	Распечатка
Дисплей		Визуальная проверка
Загрузка (осуществляется только в процессе загрузки)	Нормальная эксплуатация	

Датчик	Нормальная эксплуатация	Нормальная эксплуатация
Средство удалённой связи	Нормальная эксплуатация	Нормальная эксплуатация
Устройство ГНСС	Нормальная эксплуатация	Нормальная эксплуатация

### 3.11 Считывание данных из блока памяти

- 90) Записывающее оборудование способно считывать любые данные, содержащиеся в его блоке памяти.

### 3.12 Регистрация и хранение данных в блоке памяти

В настоящем пункте:

- 365 дней – 365 календарных суток усреднённой продолжительности деятельности водителя на транспортном средстве. Усреднённая суточная продолжительность деятельности на транспортном средстве определяется исходя, по крайней мере, из 6 водителей или вторых водителей, 6 циклов ввода и извлечения карточки и 256 изменений вида деятельности. Таким образом, 365 дней включают в себя не менее 2190 (вторых) водителей, 2190 циклов ввода и извлечения карточки и 93440 изменений вида деятельности,
  - среднее суточное число мест определяется как, по крайней мере, 6 мест, в которых начинается дневной период работы, 6 мест, в которых непрерывное время управления водителем достигает значения, кратного трём часам, и 6 мест, в которых дневной период работы заканчивается, так что 365 дней включают в себя 6570 мест,
  - время регистрируется с точностью до одной минуты, если не предусмотрено иначе,
  - показания одометра регистрируются с точностью до 1 км,
  - скорость регистрируется с точностью 1 км/ч,
  - местоположение (широта и долгота) регистрируется в градусах и минутах с точностью 1/10 минуты с учётом соответствующей точности ГНСС и времени получения.
- 91) Данные, хранящиеся в блоке памяти, не страдают в результате прекращения электропитания от внешнего источника в течение менее 12 месяцев в условиях, предусмотренных для официального утверждения типа. Кроме того, данные, хранящиеся во внешнем устройстве удалённой связи, как указано в приложении 14, не страдают в результате прекращения электропитания в течение менее 28 дней.
- 92) Записывающее оборудование способно самостоятельно или по команде регистрировать и хранить в своей памяти следующие данные:

#### 3.12.1 Идентификационные данные аппаратуры

##### 3.12.1.1 Идентификационные данные бортового устройства

- 93) Записывающее оборудование способно хранить в своей памяти следующие идентификационные данные бортового устройства:
- название производителя,
  - адрес производителя,
  - номер детали,
  - серийный номер,
  - поколение БУ,
  - возможность использовать карточки тахографов первого поколения,
  - номер версии программного обеспечения,
  - дата установки версии программного обеспечения,
  - год изготовления устройства,
  - номер официального утверждения.

- 94) Идентификационные данные бортового устройства регистрируются и хранятся раз и навсегда производителем бортового устройства, за исключением даты и номера официального утверждения программного обеспечения, которые могут быть изменены в случае перехода на улучшенную 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 производителя,
  - серийный номер,
  - номер официального утверждения,
  - идентификатор встроенного компонента защиты (например, номер встроенной интегральной схемы/процессора),
  - идентификатор операционной системы (например, номер версии программного обеспечения).
- 96) Идентификационные данные датчика движения регистрируются и хранятся раз и навсегда в памяти датчика движения производителем.
- 97) Бортовое устройство способно регистрировать и хранить в своей памяти следующие данные, связанные с 20 последними подсоединениями датчиков движения (если в течение одного календарного дня имеется несколько подсоединений, сохраняется информация только о первом и последнем за указанный день).

Для каждого такого подсоединения 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 производителя,
  - серийный номер,
  - номер официального утверждения,
  - идентификатор встроенного компонента защиты (например, номер встроенной интегральной схемы/процессора),
  - идентификатор операционной системы (например, номер версии программного обеспечения).
- 99) Идентификационные данные регистрируются и хранятся раз и навсегда в памяти внешнего устройства ГНСС производителем внешнего устройства ГНСС.
- 100) Бортовое устройство способно регистрировать и хранить в своей памяти следующие данные, связанные с 20 последними соединениями внешних устройств ГНСС (если в течение одного календарного дня имеется несколько соединений, сохраняется информация только о первом и последнем соединениях дня).

Для каждого такого соединения регистрируются следующие данные:

- идентификационные данные внешнего устройства ГНСС:
  - серийный номер,
  - номер официального утверждения,
- данные о соединениях внешних устройств ГНСС:

- дата соединения

### 3.12.2 Ключи и сертификаты

- 101) Записывающее оборудование способно хранить ряд криптографических ключей и сертификатов, как указано в частях А и Б приложения 11.

### 3.12.3 Данные о вводе и извлечении карточек водителя или мастерской

- 102) В отношении каждого цикла ввода и извлечения карточки водителя или мастерской записывающее оборудование регистрирует и хранит в своей памяти следующие данные:
- фамилия и имя (имена) владельца карточки, записанные в блоке памяти карточки,
  - номер карточки, название выдавшего её государства-члена и дата окончания срока действия, записанные в блоке памяти карточки,
  - поколение карточки,
  - дата и время ввода,
  - показание одометра транспортного средства в момент ввода карточки,
  - считывающее устройство, в которое вставляется карточка,
  - дата и время извлечения,
  - показание одометра транспортного средства в момент извлечения карточки,
  - следующая информация о предыдущем транспортном средстве, которым пользовался водитель, записанная в блоке памяти карточки:
    - номер транспортного средства VRN и государство-член регистрации,
    - поколение БУ (если есть),
    - дата и время извлечения карточки,
  - метка, указывающая на момент ввода карточки, ввёл ли владелец карточки данные о своей деятельности вручную или нет.
- 103) Блок памяти способен хранить эти данные в течение не менее 365 дней.
- 104) Когда объём памяти заполнен, новые данные записываются поверх самых старых данных.

### 3.12.4 Данные о деятельности водителя

- 105) Записывающее оборудование регистрирует и хранит в своей памяти все факты изменения деятельности водителя и/или второго водителя и/или все случаи изменения статуса управления и/или 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 не вставлена никакая карточка).

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

- 106) Блок памяти способен хранить данные о деятельности водителя в течение не менее 365 дней.
- 107) Когда объём памяти заполнен, новые данные записываются поверх самых старых данных.

### **3.12.5 Места и положения, в которых начинаются и заканчиваются дневные периоды работы и/или достигается 3-часовой предел непрерывного управления**

- 108) Записывающее оборудование в своём блоке памяти регистрирует и хранит следующие данные:
- места и положения, в которых водитель и/или второй водитель начинает свой дневной рабочий период;
  - места, в которых непрерывное время вождения достигает значения, кратного трём часам;
  - места и положения, в которых водитель и/или второй водитель завершает свой дневной рабочий период.
- 109) Если положение транспортного средства в эти моменты времени из приёмника ГНСС неизвестно, записывающее оборудование использует данные последнего записанного места и соответствующие дату и время.
- 110) Вместе с каждым местом или положением записывающее оборудование в своём блоке памяти регистрирует и хранит следующие данные:
- номер карточки (второго) водителя и государство-член, выдавшее карточку,
  - поколение карточки,
  - дата и время ввода,
  - тип ввода (начало, окончание или 3-часовой отрезок непрерывного управления),
  - соответствующие точность, дата и время ГНСС, если применимо;
  - показания одометра транспортного средства.
- 111) Блок памяти способен хранить места и положения, в которых начинаются и заканчиваются дневные периоды работы и/или достигается 3-часовой предел непрерывного управления, в течение не менее 365 дней.
- 112) Когда объём памяти заполнен, новые данные записываются поверх самых старых данных.

### **3.12.6 Данные одометра**

- 113) Записывающее оборудование в своём блоке памяти регистрирует показания одометра транспортного средства и соответствующую дату в полночь каждого календарного дня.
- 114) Блок памяти способен хранить полуночные данные одометра в течение не менее 365 дней.
- 115) Когда объём памяти заполнен, новые данные записываются поверх самых старых данных.

### **3.12.7 Подробные данные о скорости**

- 116) Записывающее оборудование в своём 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 эксплуатировалось.

### **3.12.8 Данные о событиях**

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

- 117) Записывающее оборудование в своём блоке памяти регистрирует и хранит следующие данные по каждому обнаруженному событию в соответствии с указанными ниже правилами хранения:

Событие	Правила хранения	Данные по каждому событию, подлежащие регистрации
Ввод недействительной карточки	- 10 последних событий.	<ul style="list-style-type: none"> <li>- дата и время события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, в отношении которой произошло событие.</li> <li>- число аналогичных событий за указанный день</li> </ul>
Несовместимость карточек	- 10 последних событий.	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение обеих карточек, в отношении которых возникла несовместимость.</li> </ul>
Управление без соответствующей карточки	<ul style="list-style-type: none"> <li>- самое продолжительное событие за каждые последние 10 дней данного случая,</li> <li>- 5 самых продолжительных событий за последние 365 дней.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- число аналогичных событий за указанный день.</li> </ul>
Ввод карточки во время управления	- последнее событие за каждые последние 10 дней данного случая,	<ul style="list-style-type: none"> <li>- дата и время события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение,</li> <li>- число аналогичных событий за указанный день</li> </ul>
Неправильное завершение последнего сеанса использования карточки	- 10 последних событий.	<ul style="list-style-type: none"> <li>- дата и время ввода карточки,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение,</li> <li>- дата последнего сеанса использования, записанная на карточке: <ul style="list-style-type: none"> <li>- дата и время ввода карточки,</li> <li>- VRN, государство-член регистрации и поколение БУ.</li> </ul> </li> </ul>

Превышение скорости (1)	<ul style="list-style-type: none"> <li>- самое серьёзное событие за каждые последние 10 дней данного случая (т.е. самая высокая средняя скорость),</li> <li>- 5 самых серьёзных событий за последние 365 дней.</li> <li>- первое событие, наступившее после последней калибровки</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- максимальная скорость, измеренная во время события,</li> <li>- средняя арифметическая скорость, измеренная во время события,</li> <li>- тип и номер карточки, выдавшее её государство-член и поколение карточки водителя (если применимо),</li> <li>- число аналогичных событий за указанный день.</li> </ul>
Прекращение электропитания (2)	<ul style="list-style-type: none"> <li>- самое продолжительное событие за каждые последние 10 дней данного случая,</li> <li>- 5 самых продолжительных событий за последние 365 дней.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- число аналогичных событий за указанный день.</li> </ul>
Ошибка связи со средством удалённой связи	<ul style="list-style-type: none"> <li>- самое продолжительное событие за каждые последние 10 дней данного случая,</li> <li>- 5 самых продолжительных событий за последние 365 дней.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- число аналогичных событий за указанный день.</li> </ul>
Отсутствие информации о местоположении из приёмника ГНСС	<ul style="list-style-type: none"> <li>- самое продолжительное событие за каждые последние 10 дней данного случая,</li> <li>- 5 самых продолжительных событий за последние 365 дней.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- число аналогичных событий за указанный день.</li> </ul>

Ошибочные данные о движении	<ul style="list-style-type: none"> <li>- самое продолжительное событие за каждые последние 10 дней данного случая,</li> <li>- 5 самых продолжительных событий за последние 365 дней.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- число аналогичных событий за указанный день.</li> </ul>
Противоречивые данные о движении транспортного средства	<ul style="list-style-type: none"> <li>- самое продолжительное событие за каждые последние 10 дней данного случая,</li> <li>- 5 самых продолжительных событий за последние 365 дней.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- число аналогичных событий за указанный день.</li> </ul>
Попытка нарушения системы защиты	<ul style="list-style-type: none"> <li>- 10 последних событий по типу события.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события (если актуально),</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- тип события.</li> </ul>
Противоречивые данные о времени	<ul style="list-style-type: none"> <li>- самое продолжительное событие за каждые последние 10 дней данного случая,</li> <li>- 5 самых продолжительных событий за последние 365 дней.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время в записывающем оборудовании</li> <li>- дата и время ГНСС,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- число аналогичных событий за указанный день.</li> </ul>

(1) Записывающее оборудование в своём 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 этом время может 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 в своём блоке памяти стремится регистрировать и хранить следующие данные по каждой обнаруженной неисправности в соответствии с указанными ниже правилами хранения:

Неисправность	Правила хранения	Данные по каждой неисправности, подлежащие регистрации
Неисправность карточки	- 10 последних неисправностей карточки водителя.	- дата и время начала неисправности, - дата и время окончания неисправности, - тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение.
Неисправность записывающего оборудования	- 10 последних неисправностей по типу неисправности, - первая неисправность после последней калибровки.	- дата и время начала неисправности, - дата и время окончания неисправности, - тип неисправности, - тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце неисправности.

### 3.12.10 Данные калибровки

119) Записывающее оборудование в своём блоке памяти регистрирует и хранит следующие данные:

- известные параметры калибровки в момент включения,
- первая калибровка после включения,
- первая калибровка на данном транспортном средстве (идентифицируемом с помощью его опознавательного номера VIN),
- последние 20 калибровок (если последние калибровки производятся в течение одного календарного дня, сохраняются данные только о последней калибровке в указанный день).

120) Для каждой такой калибровки регистрируются следующие данные:

- цель калибровки (активация, первая установка, установка, регулярная проверка),
- название и адрес мастерской,
- номер карточки мастерской, выдавшее карточку государство-член и дата истечения срока действия карточки,
- идентификационные данные транспортного средства,
- обновлённые или подтверждённые параметры: w, k, l, размер шин, регулировка устройства ограничения скорости, одометр (старые и новые показания), дата и время (старые и новые значения),
- типы и идентификаторы всех имеющихся пломб.

121) Кроме того, записывающее оборудование в своём блоке памяти регистрирует и хранит данные о своей способности использовать карточки тахографов первого поколения (всё ещё активные или уже нет).

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

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

- 123) Внешнее устройство ГНСС в своём блоке памяти регистрирует и хранит следующие данные об установке:
- первое соединение с БУ (дата, время, номер официального утверждения БУ, серийный номер БУ),
  - последнее соединение с БУ (дата, время, номер официального утверждения БУ, серийный номер БУ).

### 3.12.11 Данные корректировки времени

- 124) Записывающее оборудование в своём блоке памяти регистрирует и хранит данные, связанные с корректировкой времени, выполненной в режиме калибровки вне рамок регулярной калибровки (определение в пункте f):

- последняя корректировка времени,
- 5 крупнейших корректировок времени.

- 125) Для каждой такой корректировки времени регистрируются следующие данные:

- дата и время, старое значение,
- дата и время, новое значение,
- название и адрес мастерской,
- номер карточки мастерской, выдавшее карточку государство-член, поколение карточки и дата истечения срока действия карточки.

### 3.12.12 Данные о контрольных действиях

- 126) Записывающее оборудование в своём блоке памяти регистрирует и хранит следующие данные о 20 последних контрольных действиях:

- дата и время контроля,
- номер контрольной карточки, выдавшее карточку государство-член 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 придорожная проверка калибровки).

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

### 3.12.13 Данные блокировки, установленной предприятием

- 128) Записывающее оборудование в своём блоке памяти регистрирует и хранит следующие данные о 255 последних блокировках предприятием:

- дата и время блокировки,
- дата и время разблокировки,
- номер карточки предприятия, выдавшее карточку государство-член и поколение карточки,
- название и адрес предприятия.

Данные, ранее заблокированные посредством блокировки, не сохранённой в памяти из-за превышения установленного предела, считаются незаблокированными.

### 3.12.14 Данные о действиях загрузки

- 129) Записывающее оборудование в своём блоке памяти регистрирует и хранит 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, выдавшее карточку государство-член и поколение карточки,
- название предприятия или мастерской.

### **3.12.15 Данные об особых условиях**

- 130) Записывающее оборудование в своём блоке памяти регистрирует и хранит следующие данные об особых условиях:
- дата и время ввода,
  - тип особых условий.
- 131) Блок памяти данных способен хранить данные об особых условиях не менее 365 дней (при предположении, что в среднем ежедневно открывается и закрывается одна позиция, указывающая на особое условие). Когда объём памяти заполнен, новые данные записываются поверх самых старых данных.

### **3.12.16 Данные карточек тахографов**

- 132) Записывающее оборудование способно хранить следующие данные, связанные с различными карточками тахографов, использовавшихся в БУ:
- номер и серийный номер карточки тахографа,
  - производитель карточки тахографа,
  - тип карточки тахографа,
  - версия карточки тахографа.

- 133) Записывающее оборудование способно хранить не менее 88 таких записей.

## **3.13 Считывание данных с карточек тахографов**

- 134) Записывающее оборудование в определённых условиях способно считывать с карточек тахографов первого и второго поколений необходимые данные, чтобы:
- установить тип карточки, владельца карточки, ранее эксплуатировавшееся транспортное средство, дату и время последнего извлечения карточки и вид деятельности, выбранный в тот момент,
  - проверить правильность завершения последнего сеанса использования карточки,
  - вычислить непрерывное время управления транспортным средством водителем, совокупное время перерывов и совокупное время управления за предыдущую и текущую недели,
  - 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 производит очередную попытку (максимум три раза) выполнения той же команды считывания данных, после чего, если считать данные не удалось, сообщает, что карточка неисправна и недействительна.

## **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 регистрирует и хранит данные так же, как и записывающее оборудование первого поколения.
- 137) Записывающее оборудование записывает «данные о сеансе использования карточки» на карточке водителя или мастерской сразу же после её ввода.
- 138) Записывающее оборудование обновляет данные, хранящиеся на действительных карточках водителя, мастерской и/или контроля, со всеми необходимыми данными, относящимися к периоду, в течение которого карточка была вставлена в устройство, и к владельцу карточки. Данные, хранящиеся на этих карточках, указаны в главе 4.
- 139) Записывающее оборудование 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 учётом данных о виде деятельности и месте, введённых владельцем карточки вручную.
- 140) Все события, не определённые для записывающего оборудования первого поколения, на карточках водителя и мастерской не хранятся.
- 141) Порядок обновления данных на карточках тахографа таков, чтобы в случае необходимости и с учётом фактического объёма памяти хранения последние данные записывались поверх самых старых данных.
- 142) В случае ошибки при записи записывающее оборудование производит очередную попытку (максимум три раза) выполнения той же команды записи данных, после чего, если записать данные не удалось, сообщает, что карточка неисправна и недействительна.
- 143) До высвобождения карточки водителя и после сохранения на ней всех соответствующих данных записывающее оборудование 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 прикладными программами, первая из которых точно такая же, как программа TACHO для карточек тахографов первого поколения, а вторая – TACHO\_G2, как описано в главе 4 и приложении 2.
- 145) Записывающее оборудование записывает «данные о сеансе использования карточки» на карточке водителя или мастерской сразу же после её ввода.
- 146) Записывающее оборудование обновляет данные, хранящиеся в 2 приложениях действительных карточек водителя, мастерской и/или контроля, со всеми необходимыми данными, относящимися к периоду, в течение которого карточка была вставлена в устройство, и к владельцу карточки. Данные, хранящиеся на этих карточках, указаны в главе 4.
- 147) Записывающее оборудование обновляет данные о деятельности водителя и местах и положениях (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 учётом данных о виде деятельности и месте, введённых владельцем карточки вручную.

- 148) Порядок обновления данных на карточках тахографа таков, чтобы в случае необходимости и с учётом фактического объёма памяти хранения последние данные записывались поверх самых старых данных.
- 149) В случае ошибки при записи записывающее оборудование производит очередную попытку (максимум три раза) выполнения той же команды записи данных, после чего, если записать данные не удалось, сообщает, что карточка неисправна и недействительна.
- 150) До высвобождения карточки водителя и после сохранения в 2 её приложениях всех соответствующих данных записывающее оборудование приводит «данные о сеансе использования карточки» в исходное состояние.

### **3.15 Отображение**

- 151) Отображаемое сообщение включает в себя не менее 20 знаков.
- 152) Минимальный размер знака – 5 мм в высоту и 3,5 мм в ширину.
- 153) Дисплей поддерживает знаки, указанные в главе 4 «Наборы знаков» приложения 1. На дисплее могут использоваться упрощённые наборные знаки (например, ударные знаки могут отображаться без знака удара или строчные буквы могут отображаться в виде заглавных).
- 154) Дисплей оснащён надлежащей неослепляющей подсветкой.
- 155) Отображение зрительно воспринимается со стороны, вне записывающего оборудования.
- 156) Записывающее оборудование способно отображать следующие данные:
- данные исходных настроек,
  - данные о предупреждениях,
  - данные о доступе к меню,
  - другие данные, запрашиваемые пользователем.

Записывающее оборудование может выводить на дисплей дополнительную информацию при условии, что её можно чётко отличить от информации, требуемой выше.

- 157) Дисплей записывающего оборудования использует пиктограммы или комбинации пиктограмм, перечисленные в приложении 3. На дисплей могут также выводиться дополнительные пиктограммы или комбинации пиктограмм при условии, что их можно чётко отличить от пиктограмм или комбинаций пиктограмм, упомянутых выше.
- 158) Когда транспортное средство находится в процессе движения, дисплей всегда находится во включённом состоянии.
- 159) Записывающее оборудование может быть оснащено ручной или автоматической функцией, позволяющей отключать дисплей, когда транспортное средство остановлено.

Формат отображения данных указан в приложении 5.

#### **3.15.1 Вид дисплея с исходными настройками**

- 160) Когда иную информацию на дисплей выводить не требуется, записывающее оборудование отображает по умолчанию следующие данные:

- местное время (время UTC плюс корректировка, 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 совокупная продолжительность перерывов.

- 161) Отображение данных, относящихся к каждому водителю, должно быть чётким, полным и однозначным. В том случае, если информацию, относящуюся к водителю и второму водителю, нельзя вывести на дисплей одновременно, записывающее оборудование по умолчанию отображает информацию, относящуюся к водителю, и даёт пользователю возможность выводить на дисплей информацию, относящуюся ко второму водителю.
- 162) В том случае, если ширина дисплея не позволяет по умолчанию отображать режим работы, записывающее оборудование выводит на дисплей кратковременное сообщение с указанием нового режима работы в момент его изменения.
- 163) Записывающее оборудование выводит на дисплей кратковременное сообщение с указанием фамилии владельца карточки в момент её ввода.
- 164) Когда открывается позиция НЕПРИМЕНИМО, на дисплее по умолчанию с использованием соответствующей пиктограммы отображается тот факт, что эта позиция открыта (при этом допускается, что текущий вид деятельности водителя может в это время не отображаться).

### 3.15.2 Отображение предупреждения

- 165) Записывающее оборудование выводит на дисплей предупреждающую информацию прежде всего с помощью пиктограмм, указанных в приложении 3, дополненных, в случае необходимости, дополнительной информацией в виде числового кода. Кроме того, может быть включено текстовое описание предупреждения на языке, выбранном водителем.

### 3.15.3 Доступ к меню

- 166) Записывающее оборудование содержит необходимые команды, подаваемые с использованием соответствующего меню.

### 3.15.4 Другие отображаемые данные

- 167) По соответствующей команде на дисплее на выборочной основе можно выводить следующие данные:
- дата и время UTC с корректировкой на местное время,
  - содержание любой из шести распечаток в том же формате, что и сами распечатки,
  - продолжительность непрерывного управления и совокупное время перерывов водителя,
  - продолжительность непрерывного управления и совокупное время перерывов второго водителя,
  - совокупное время управления водителем за предыдущую и текущую недели,
  - совокупное время управления вторым водителем за предыдущую и текущую недели,

необязательно:

- продолжительность текущей деятельности второго водителя (с момента выбора этой функции),

- совокупное время управления водителем за текущую неделю,
- совокупное время управления вторым водителем за текущий дневной период работы,
- совокупное время управления водителем за текущий дневной 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.

### **3.16 Печать**

169) Записывающее оборудование 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.
- история данных карточки тахографа в связи с данным БУ (см. главу 3.12.16)

Детальный формат и содержание этих распечаток представлены в приложении 4.

В конце распечаток могут содержаться дополнительные данные.

Записывающим оборудованием могут также выдаваться дополнительные распечатки, если они чётко 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» выдаётся только в том случае, если в записывающее оборудование вставлена карточка водителя или мастерской. До выдачи распечатки записывающее оборудование обновляет данные, содержащиеся в памяти соответствующей карточки.

171) Чтобы сделать «ежедневную распечатку данных о деятельности водителя, записанных на карточке» или «распечатку данных о событиях и неисправностях, записанных на карточке», записывающее оборудование:

- 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 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 «Наборы знаков» приложения 1.

175) Принтеры сконструированы таким образом, чтобы могли выдавать эти распечатки такой разрешающей способности, которая исключала бы всякое 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 утверждённой бумаге, используемой записывающим оборудованием, нанесён соответствующий знак официального утверждения типа и указание типа (типов) записывающего оборудования, 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 хотя бы тестовым спецификациям, представленным в приложении 9.
- 180) Кроме того, предусматривается возможность включения в эти документы примечаний, написанных от руки, например, подписи водителя.
- 181) Если во время распечатки кончается бумага, записывающее оборудование возобновляет печать после перезагрузки бумаги с начала распечатки или продолжает печать с чёткой ссылкой на ту часть, которая была выдана на печать ранее.

### **3.17 Предупреждения**

- 182) Записывающее оборудование 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 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 чётко распознаются пользователем, располагаются в поле визуального восприятия водителя и удобочитаемы как в дневное, так и в ночное время.
- 187) Визуальные предупреждения могут быть встроены в записывающее оборудование и/или удалены от него.
- 188) В последнем случае имеется пометка в виде буквы T.
- 189) Предупреждения подаются в течение как минимум 30 секунд, если только пользователь не нажимает на любую клавишу или несколько клавиш записывающего устройства, для подтверждения того, что он принял предупреждение к сведению. Это первое подтверждение не влечёт за собой удаления выведенной на дисплей причины, указанной в следующем пункте.
- 190) Причина предупреждения выводится на дисплей записывающего оборудования и остаётся видимой до тех пор, пока пользователь не введёт специальный код или команду на записывающем оборудовании.
- 191) Могут предусматриваться дополнительные предупреждения, если они не вводят водителей в заблуждение по поводу предупреждений, определённых выше.



### **3.18 Загрузка данных на внешние носители**

- 192) Записывающее оборудование способно по команде загружать данные из своей памяти или с карточки водителя на внешние носители через разъём калибровки/загрузки. До начала загрузки записывающее оборудование обновляет данные, содержащиеся в памяти соответствующей карточки.
- 193) В дополнение и в качестве факультативной функции записывающее оборудование в любом режиме работы может загружать данные в базу данных предприятия, идентифицированного по этому каналу связи, через любой другой разъём. В подобном случае к этой операции загрузки применяются права доступа к данным в режиме предприятия.
- 194) Загрузка не приводит к изменению или удалению любых сохранённых данных.
- 195) Электрический интерфейс разъёма калибровки/загрузки представлен в приложении 6.
- 196) Протоколы загрузки данных представлены в приложении 7.

### **3.19 Удалённая связь для целевых придорожных проверок**

- 197) При включённом зажигании бортовое устройство в устройстве удалённой связи каждые 60 секунд сохраняет новейшие данные для целевых придорожных проверок. Такие данные зашифрованы и защищены подписью, как описано в приложениях 11 и 14.
- 198) Данные, которые проверяются на удалении, передаются в считывающие устройства удалённой связи при помощи беспроводных средств, как описано в приложении 14.
- 199) Данные, необходимые для целевых придорожных проверок:
- 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 корректировки времени,
  - данные калибровки, включая даты двух последних сохранённых записей калибровки,
  - регистрационный номер транспортного средства,
  - скорость, зарегистрированная тахографом.

### **3.20 Вывод данных на дополнительные внешние устройства**

- 200) Записывающее оборудование также может быть оснащено стандартизированными интерфейсами, позволяющими использовать данные, записанные или произведённые тахографами, в оперативном режиме на внешних устройствах.

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

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

- эти данные представляют собой набор отдельных существующих данных из словаря данных тахографов (приложение 1),
- 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,
- В любой момент согласие водителя можно активизировать или отменить при помощи команд в меню, при условии что введена карточка водителя,
- множество и подмножество данных передаётся через протокол беспроводной связи блютуз в радиусе кабины транспортного средства с частотой обновления 1 минута,
- соединение внешнего устройства с интерфейсом ИТС защищено отдельным случайным 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 может нарушать надлежащее функционирование и безопасность бортового устройства или влиять на них.

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

Записывающее оборудование уведомляет другие внешние устройства о согласии водителя.

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

- 201) Интерфейс последовательного канала, как указано в дополнении 1В к регламенту (ЕЭС) № 3821/85 с последними поправками, может и далее предусматриваться в тахографах, чтобы обеспечить дополнительную совместимость. В любом случае при передаче личных данных согласие водителя всё равно необходимо.

### **3.21 Калибровка**

202) Функция калибровки позволяет:

- автоматически подсоединять датчик движения к БУ,
- автоматически подсоединять внешнее устройство ГНСС к БУ, если применимо,
- в цифровой форме приводить постоянную величину записывающего оборудования (k) в соответствие с характеристическим коэффициентом транспортного средства (w),
- корректировать текущее время в рамках срока действия введённой карточки мастерской,
- корректировать текущие показания одометра,
- обновлять идентификационные данные датчика движения, записанные в блоке памяти,
- в соответствующих случаях обновлять идентификационные данные внешнего устройства ГНСС, записанные в блоке памяти,
- обновлять типы и идентификаторы всех имеющихся пломб,
- обновлять или подтверждать другие параметры, заложенные в записывающем оборудовании: идентификация транспортного средства, показатели w и l, размер шин и регулировка устройства ограничения скорости (в случае применимости).

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

204) Подсоединение датчика движения к БУ заключается как минимум в:

- обновлении данных установки датчика движения, содержащихся в памяти датчика движения (при необходимости),

- копировании необходимых идентификационных данных датчика движения и блока памяти датчика движения в блок памяти БУ.

- 205) Подсоединение внешнего устройства ГНСС к БУ заключается как минимум в:
- обновлении данных об установке внешнего устройства ГНСС, содержащихся в 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 проводится проверка информации ГНСС о местоположении.

- 206) Функция калибровки способна обеспечивать ввод необходимых данных через разъём калибровки/загрузки в соответствии с протоколом калибровки, определённым в приложении 8. Функция калибровки может также обеспечивать ввод необходимых данных с помощью других разъёмов.

### **3.22 Придорожные проверки калибровки**

- 207) Функция придорожной проверки калибровки позволяет считывать серийный номер датчика движения (возможно, встроенный в адаптер) и серийный номер внешнего устройства ГНСС (если применимо), связанного с бортовым устройством, в момент запроса.
- 208) Такое считывание возможно, по крайней мере, с дисплея бортового устройства с помощью команд в меню.
- 209) Функция придорожной проверки калибровки также позволяет контролировать выбор режима калибровки I/O сигнальной линии калибровки I/O, как указано в приложении 6, через интерфейс К-линии. Это осуществляется через ECUAdjustmentSession, как описано в приложении 8, раздел 7 «Контроль тестовых импульсов. Функциональная контрольная единица ввода-вывода».

### **3.23 Корректировка времени**

- 210) Функция корректировки времени позволяет автоматически корректировать текущее время. В записывающем оборудовании для корректировки времени используются два источника времени: 1) внутренние часы БУ, 2) приёмник ГНСС.
- 211) Установка времени на внутренних часах БУ автоматически корректируется с интервалами не более 12 часов. По истечении интервала и при отсутствии сигнала ГНСС установка времени осуществляется, как только БУ получает доступ к действительному времени, обеспечиваемому приёмником ГНСС, с учётом условий зажигания транспортного средства. Привязка ко времени для автоматической установки времени на внутренних часах БУ берётся из приёмника ГНСС. Событие противоречивой информации о времени происходит в том случае, если текущее время отличается от информации о времени, поставляемой приёмником ГНСС, более чем на одну (1) минуту.
- 212) Функция корректировки времени также позволяет произвести синхронизированную корректировку текущего времени в режиме калибровки.

### **3.24 Рабочие характеристики**

- 213) Бортовое устройство полностью работоспособно в диапазоне температур от -20°C до 70°C, а датчик движения в диапазоне температур от -40°C до 135°C. Содержание блока памяти сохраняется при температурах до -40°C.
- 214) Тахограф полностью работоспособен в диапазоне влажности от 10% до 90%.

- 215) Пломбы «умного» тахографа выдерживают такие же условия, как пломбы компонентов тахографа.
- 216) Записывающее оборудование должно быть защищено от перепадов напряжения, несоблюдения полярности источника питания и короткого замыкания.
- 217) Датчики движения:
- реагируют на магнитное поле, нарушающее распознавание движения транспортного средства. В подобных обстоятельствах бортовое устройство регистрирует и хранит неисправность датчика (требование 88) или
  - снабжается чувствительным элементом, защищённым от магнитных полей или не реагирующим на них.
- 218) Записывающее оборудование и внешнее устройство ГНСС соответствуют международному регламенту ЭЖ ООН Р10 и защищены от электростатических разрядов и переходных процессов.

### **3.25 Материалы**

- 219) Все составные части записывающего оборудования изготовлены 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 соответствует применимым техническим спецификациям, регламентирующим параметры эргономичности.
- 223) Записывающее оборудование защищено от случайного повреждения.

### **3.26 Маркировка**

- 224) Если записывающее оборудование выводит на дисплей показания одометра транспортного средства и скорости, на дисплее должны отображаться следующие детали:
- около цифры, указывающей на расстояние, единица измерения расстояния, обозначаемая с помощью сокращения «км»,
  - около цифры, указывающей на скорость, сокращение «км/ч».

Записывающее оборудование может также переключаться в режим отображения скорости в милях в час; в этом случае единица измерения скорости указывается с помощью сокращения «м/ч». Записывающее оборудование может также переключаться в режим отображения расстояния в милях; в этом случае единица измерения расстояния – «мили».

- 225) К каждому отдельному компоненту записывающего оборудования прикреплена поясняющая табличка с указанием следующих данных:
- название и адрес производителя оборудования,
  - номер детали, присвоенный производителем, и год изготовления оборудования,
  - серийный номер оборудования,
  - знак официального утверждения типа устройства.
- 226) Если на табличке физически не хватает места для указания вышеупомянутых данных, на ней следует указать хотя бы название или логотип производителя и номер детали устройства.

#### 4 Требования к конструкции и функциям карточек тахографов

##### 4.1 Видимые данные

На первой странице указываются:

- 227) слова «Карточка водителя» или «Контрольная карточка», или «Карточка мастерской», или «Карточка предприятия», напечатанные заглавными буквами на официальном языке или языках государства-члена, выдавшего карточку, в соответствии с типом карточки.
- 228) название государства-члена, выдавшего карточку (необязательно);
- 229) отличительный знак государства-члена, выдавшего карточку, напечатанный в виде негатива в синем прямоугольнике в окружении 12 жёлтых звёзд. Отличительные знаки:

B	Бельгия	LV	Латвия
BG	Болгария	L	Люксембург
CZ	Чехия	LT	Литва
CY	Кипр	П	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	Соединённое Королевство
I	Италия		

- 230) конкретная информация, касающаяся выданной карточки, под следующими номерами:

	Карточка водителя	Контрольная карточка	Карточка предприятия или мастерской
1.	фамилия водителя	название контрольного органа	название предприятия или мастерской
2.	имя (имена) водителя	фамилия контролёра (если применимо)	фамилия владельца карточки (если применимо)
3.	дата рождения водителя	имя (имена) контролёра (если применимо)	имя (имена) владельца карточки (если применимо)
4.a	дата начала срока действия карточки		
4.b	дата истечения срока действия карточки		
4.c	название органа, выдавшего карточку (может быть напечатано на стр. 2)		
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 контролёра (факультативно)	фотография установщика (факультативно)-
7.	Подпись владельца (факультативно)		
8.	Обычное место жительства или почтовый адрес владельца (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:

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

233) с письменного согласия владельца 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,
- контрольная карточка: синий,
- карточка мастерской: красный,
- карточка предприятия: жёлтый.

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,
- на месте фотографии – фоновый защитный рисунок, который перекрывает фотография,
- по крайней мере одна двухцветная линия – микропринт.

## COMMUNITY MODEL TACHOGRAPH CARDS

FRONT		REVERSE	
A	<p style="text-align: center;"><b>DRIVER CARD</b> MEMBER STATE</p>  <p>1. 2. 3. 4a. 4b. 4c. (4d.) 5a. 5b. 6. 7. G2 (8.)</p>	B	<p style="text-align: center;">1. Surname 2. First name(s) 3. Birth date 4a. Date of start of validity of card 4b. Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5a. Driving license number 5b. Card number 6. Photograph 7. Signature (8.) Address</p> <p style="text-align: center;">Please return to: NAME OF AUTHORITY AND ADDRESS</p>
A	<p style="text-align: center;"><b>CONTROL CARD</b> MEMBER STATE</p>  <p>1. (2.) (3.) 4a. (4b.) 4c. (4d.) 5b. (6.) (7.) G2 8.</p>	B	<p style="text-align: center;">1. Control Body (2.) Surname (3.) First name(s) 4a. Date of start of validity of card (4b.) Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5b. Card number (6.) Photograph (7.) Signature 8. Address</p> <p style="text-align: center;">Please return to: NAME OF AUTHORITY AND ADDRESS</p>
A	<p style="text-align: center;"><b>WORKSHOP CARD</b> MEMBER STATE</p>  <p>1. (2.) (3.) 4a. 4b. 4c. (4d.) 5b. (7.) G2 8.</p>	B	<p style="text-align: center;">1. Workshop Name (2.) Surname (3.) First name(s) 4a. Date of start of validity of card 4b. Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5b. Card number (7.) Signature 8. Address</p> <p style="text-align: center;">Please return to: NAME OF AUTHORITY AND ADDRESS</p>
A	<p style="text-align: center;"><b>COMPANY CARD</b> MEMBER STATE</p>  <p>1. (2.) (3.) 4a. 4b. 4c. (4d.) 5b. (7.) G2 8.</p>	B	<p style="text-align: center;">1. Company Name (2.) Surname (3.) First name(s) 4a. Date of start of validity of card 4b. Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5b. Card number (7.) Signature 8. Address</p> <p style="text-align: center;">Please return to: NAME OF AUTHORITY AND ADDRESS</p>

## ОБРАЗЕЦ КАРТОЧЕК ТАХОГРАФА СООБЩЕСТВА

## ЛИЦЕВАЯ СТОРОНА

## ОБРАТНАЯ СТОРОНА

КАРТОЧКА ВОДИТЕЛЯ ГОСУДАРСТВО-ЧЛЕН

1. Фамилия 2. Имя (имена) 3. Дата рождения  
4a. Действительна с  
4b. Административный срок действия  
4c. Орган, выдавший карточку  
(4d.) № для национальных административных целей

<p>КОНТРОЛЬНАЯ КАРТОЧКА ГОСУДАРСТВО-ЧЛЕН</p>	<p>5а. № водительского удостоверения 5б. № карточки 6. Фотография 7. Подпись (8.) Адрес</p>
	<p>Подлежит возврату: НАЗВАНИЕ И АДРЕС ОРГАНА</p>
	<p>1. Контрольный орган (2.) Фамилия 3. Имя (имена)</p>
	<p>4а. Действительна с</p>
	<p>(4б.) Административный срок действия</p>
	<p>4с. Орган, выдавший карточку</p>
	<p>(4d.) № для национальных административных целей</p>
	<p>5б. № карточки</p>
	<p>(6.) Фотография</p>
	<p>(7.) Подпись 8. Адрес</p>
<p>КАРТОЧКА МАСТЕРСКОЙ ГОСУДАРСТВО-ЧЛЕН</p>	<p>Подлежит возврату: НАЗВАНИЕ И АДРЕС ОРГАНА</p>
	<p>1. Название мастерской (2.) Фамилия (3.) Имя (имена)</p>
	<p>4а. Действительна с</p>
	<p>4б. Административный срок действия</p>
	<p>4с. Орган, выдавший карточку</p>
	<p>(4d.) № для национальных административных целей</p>
	<p>5б. № карточки</p>
	<p>(7.) Подпись 8. Адрес</p>
	<p>Подлежит возврату: НАЗВАНИЕ И АДРЕС ОРГАНА</p>
	<p>1. Название предприятия (2.) Фамилия (3.) Имя (имена)</p>
<p>4а. Действительна с</p>	
<p>4б. Административный срок действия</p>	
<p>4с. Орган, выдавший карточку</p>	
<p>(4d.) № для национальных административных целей</p>	
<p>5б. № карточки</p>	
<p>КАРТОЧКА ПРЕДПРИЯТИЯ ГОСУДАРСТВО-ЧЛЕН</p>	<p>(7.) Подпись 8. Адрес</p>
	<p>Подлежит возврату: НАЗВАНИЕ И АДРЕС ОРГАНА</p>

236) По согласованию с Комиссией государства-члены могут включать цвета или маркировку, например, национальные символы и элементы защиты без ущерба для других положений настоящего дополнения.

237) Временные карточки, указанные в статье 26.4 Регламента (ЕС) № 165/2014, соответствуют положениям настоящего дополнения.



## 4.2 Защита

Цель системы защиты – предохранить целостность и подлинность данных, передаваемых между карточками и записывающим оборудованием, предохранить целостность и подлинность данных, загружаемых с карточки, предоставлять возможность производить некоторые операции по записи данных на карточку только записывающим оборудованием, исключить любую возможность фальсификации данных, хранящихся на карточках, предотвратить фальсификацию и обнаруживать любые попытки такого рода.

- 238) Для обеспечения защиты системы карточка тахографа должны соответствовать требованиям безопасности, изложенным в приложениях 10 и 11.
- 239) Карточки тахографа должны считываться другими устройствами, например, персональными компьютерами.

## 4.3 Стандарты

- 240) Карточки тахографов соответствуют следующим стандартам:
- ISO/IEC 7810 Идентификационные карточки – физические характеристики,
  - ISO/IEC 7816 Идентификационные карточки – карточки с интегральными микросхемами:
    - 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 с интегральными микросхемами с контактами и связанные с ними устройства интерфейса.

## 4.4 Спецификации по условиям окружающей среды и электромагнитной совместимости

- 241) Карточки тахографа способны надлежащим образом работать в любых климатических условиях, которые обычно встречаются на территории Сообщества, как минимум в диапазоне температур от  $-25^{\circ}\text{C}$  до  $+70^{\circ}\text{C}$  с нерегулярными пиковыми значениями до  $+85^{\circ}\text{C}$ ; 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 полностью 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 по условиям окружающей среды и электромагнитной совместимости.
- 244) В процессе работы карточки тахографа соответствуют Правилам ЕЭК № 10, касающимся электромагнитной совместимости, и защищены от электростатических разрядов.

## 4.5 Хранение данных

В настоящем пункте:

- время регистрируется с точностью до одной минуты, если не предусмотрено иначе,
- показания одометра регистрируются с точностью до 1 км,

- скорость регистрируется с точностью 1 км/ч,
- местоположение (широта и долгота) регистрируется в градусах и минутах с точностью 1/10 минуты.

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

Если не указано иначе, хранение данных на карточках тахографов организуется таким образом, чтобы новые данные заменяли собой самые старые данные, если исчерпан предусмотренный объём памяти для определённых записей.

- 245) В настоящем пункте определяется минимальный объём памяти хранения различных файлов данных соответствующих приложений. Карточки тахографа способны передавать записывающему оборудованию данные о фактическом объёме памяти хранения данных этих файлов.
- 246) Любые дополнительные данные, которые могут храниться на карточках тахографов, связанные с другими приложениями, которые могут быть записаны на карточке, хранятся в соответствии с Директивой 95/46/ЕС от 24 октября 1995 г. о защите лиц при обработке личных данных и о свободном движении таких данных<sup>8</sup> и Директивой 2002/58/ЕС от 12 июля 2002 г. об обработке личных данных и защите конфиденциальности в секторе электронных коммуникаций<sup>9</sup> и статьёй 7 Регламента (ЕС) № 165/2014.
- 247) Каждый главный файл (MF) на любой карточке тахографа включает в себя до пяти элементарных файлов (EF) для управления карточкой, приложений и идентификации при помощи микросхемы и два назначенных файла (DF):
- DF Tachograph с приложением, доступным для бортовых устройств первого поколения и присутствующим также на карточках тахографов первого поколения,
  - DF Tachograph\_G2 с приложением, доступным только для бортовых устройств второго поколения и присутствующим только на карточках тахографов второго поколения.

Подробная информация о структуре карточек тахографов представлена в приложении 2.

#### **4.5.1 Элементарные файлы для идентификации и управления карточками**

#### **4.5.2 Идентификационные данные карточки с интегральной схемой**

- 248) Карточки тахографа способны хранить следующие идентификационные данные карточки с интегральной схемой:
- остановка часов,
  - серийный номер карточки (включая исходные заводские данные),
  - номер официального утверждения типа карточки,
  - идентификатор учреждения, персонализирующего карточку (ИД),
  - ИД монтажного предприятия,
  - идентификатор ИС.

##### **4.5.2.1 Идентификационные данные микросхемы**

- 249) Карточки тахографа способны хранить следующие идентификационные данные интегральной схемы:
- серийный номер ИС,
  - исходные заводские данные ИС.

---

<sup>8</sup> ОЖ L 281, 23/11/1995, стр. 31.

<sup>9</sup> ОЖ L 201, 31/07/2002, стр. 37.

#### **4.5.2.2 DIR (только на карточках тахографа второго поколения)**

250) Карточки тахографа способны хранить идентификационные данные приложений, как указано в приложении 2.

#### **4.5.2.3 Информация ATR (условно, только на карточках тахографа второго поколения)**

251) Карточки тахографа способны хранить следующие объекты данных расширенной информации:

- в случае, если карточка тахографа поддерживает поля расширенной информации, объекты данных расширенной информации, указанные в приложении 2.

#### **4.5.2.4 Расширенная информация (условно, только на карточках тахографа второго поколения)**

252) Карточки тахографа способны хранить следующие объекты данных расширенной информации:

- в случае, если карточка тахографа поддерживает поля расширенной информации, объекты данных расширенной информации, указанные в приложении 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 11.

##### ***4.5.3.1.3 Идентификационные данные карточки***

255) Карточка водителя способна хранить следующие идентификационные данные карточки:

- номер карточки,
- выдавшее её государство-член, название выдавшего компетентного органа, дата выдачи,
- дата начала срока действия карточки, дата истечения срока действия карточки.

##### ***4.5.3.1.4 Идентификационные данные владельца карточки***

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

- фамилия владельца,
- имя (имена) владельца,
- дата рождения,
- предпочитаемый язык.

##### ***4.5.3.1.5 Загрузка данных карточки***

257) Карточка водителя способна хранить следующие данные, связанные с загрузкой 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 данные о водительском удостоверении:

- выдавшее его государство-член, 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, касающиеся соответствующих событий, обнаруженных записывающим оборудованием со вставленной в него карточкой:

- 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,
- ошибочные данные о движении,
- попытка нарушения системы защиты.

261) Карточка водителя способна хранить следующие данные об этих событиях:

- 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 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 текущего транспортного средства,
- данные о транспортном средстве соответствуют используемому 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 применительно к неправильно завершённом сеансу её использования,
- дата и время окончания события соответствуют дате и времени ввода карточки применительно к сеансу использования, во время которого зафиксировано 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 событиях).

#### **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 со вставленной в него карточкой:
- неисправность карточки (в тех случаях, когда причиной этого события является данная карточка),
  - неисправность записывающего оборудования.
- 264) Карточка водителя способна хранить следующие данные об этих неисправностях:
- код неисправности,
  - дата и время начала неисправности (или ввода карточки, если в данный момент неисправность ещё не устранена),
  - дата и время окончания неисправности (или извлечения карточки, если в данный момент неисправность ещё не устранена),
  - VRN и государство-член регистрации транспортного средства, к которому относится неисправность.
- 265) Карточка водителя способна хранить данные о двенадцати последних неисправностях каждого типа (т.е. 24 неисправностях).

#### **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 внёс данные о своей деятельности, карточка водителя способна хранить следующие данные:
- дата,
  - счётчик 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 вставляет 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 усреднённой деятельности водителя определяется в качестве 93 изменений видов деятельности в день).
- 268) Данные, перечисленные в рамках требований 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 одометра транспортного средства в это время,
  - дата и время последнего использования транспортного средства (т.е. последнее извлечение карточки за этот период использования транспортного средства или 23:59 часов, если в этот момент данный период использования продолжается),
  - показание одометра транспортного средства в это время,
  - VRN и государство-член 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, введённые 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),
  - введённое название страны и региона,
  - показания одометра 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 её использования:
- дата и время начала сеанса (т.е. ввода карточки) с точностью до одной секунды,
  - VRN и государство-член регистрации.

#### ***4.5.3.1.13 Данные о контрольных действиях***

- 274) Карточка водителя способна хранить следующие данные, связанные с контрольными действиями:
- дата и время контроля,
  - номер контрольной карточки и государство-член, выдавшее 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 регистрации транспортного средства, к которому относится контроль.

Примечание: загрузка данных карточки регистрируется только в том случае, если она осуществляется через записывающее оборудование.

- 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, введённых в то время, когда карточка была вставлена в записывающее оборудование (независимо от считывающего устройства):
- дата и время ввода,
  - 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)**

### **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.

### **4.5.3.2.2 Ключи и сертификаты**

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

### **4.5.3.2.3 Идентификационные данные карточки**

- 280) Карточка водителя способна хранить следующие идентификационные данные карточки:
- номер карточки,
  - выдавшее её государство-член, название выдавшего компетентного органа, дата выдачи,
  - дата начала срока действия карточки, дата истечения срока действия карточки.

### **4.5.3.2.4 Идентификационные данные владельца карточки**

- 281) Карточка водителя способна хранить следующие идентификационные данные владельца карточки:
- фамилия владельца,
  - имя (имена) владельца,
  - дата рождения,
  - предпочитаемый язык.

### **4.5.3.2.5 Загрузка данных карточки**

- 282) Карточка водителя способна хранить следующие данные, связанные с загрузкой 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 данные о водительском удостоверении:
- выдавшее его государство-член, 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 соответствующих событий, обнаруженных записывающим оборудованием со вставленной в него карточкой:
- 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 связи со средством удалённой связи,

- Отсутствие информации о местоположении из приёмника ГНСС,
- Ошибка связи с внешним устройством ГНСС
- Ошибочные данные о движении,
- Противоречивые данные о движении транспортного средства,
- Попытка нарушения системы защиты,
- Противоречивые данные о времени.

286) Карточка водителя способна хранить следующие данные об этих событиях:

- 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 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 текущего транспортного средства,
- данные о транспортном средстве соответствуют используемому 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 применительно к неправильно завершённой сессии её использования,
- дата и время окончания события соответствуют дате и времени ввода карточки применительно к сессии использования, во время которого зафиксировано событие (текущий сеанс),
- данные о транспортном средстве соответствуют транспортному средству, на котором сеанс использования карточки был завершён неправильно.

287) Карточка водителя способна хранить данные о шести последних событиях каждого типа (т.е. 66 событиях).

#### **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 со вставленной в него карточкой:

- неисправность карточки (в тех случаях, когда причиной этого события является данная карточка),
- неисправность записывающего оборудования.

289) Карточка водителя способна хранить следующие данные об этих неисправностях:

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



- 290) Карточка водителя способна хранить данные о двенадцати последних неисправностях каждого типа (т.е. 24 неисправностях).

#### **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 внёс данные о своей деятельности, карточка водителя способна хранить следующие данные:
- дата,
  - счётчик 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 вставляет 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 28 дней (показатель усреднённой деятельности водителя определяется в качестве 93 изменений видов деятельности в день).
- 293) Данные, перечисленные в рамках требований 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 одометра транспортного средства во время первого использования,
  - дата и время последнего использования транспортного средства (т.е. последнее извлечение карточки за этот период использования транспортного средства или 23:59 часов, если в этот момент данный период использования продолжается),
  - показание одометра транспортного средства во время последнего использования,
  - VRN и государство-член регистрации транспортного средства,
  - VIN транспортного средства.
- 295) Карточка водителя способна хранить не менее 84 таких записей.

#### **4.5.3.2.11 Места и положения, 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, введённые 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),
- введённое название страны и региона,
- показания одометра транспортного средства,
- положение транспортного средства,
- точность ГНСС, дата и время определения положения.

297) Блок памяти карточки водителя способен хранить не менее 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 её использования:

- дата и время начала сеанса (т.е. ввода карточки) с точностью до одной секунды,
- VRN и государство-член регистрации.

#### **4.5.3.2.13 Данные о контрольных действиях**

299) Карточка водителя способна хранить следующие данные, связанные с контрольными действиями:

- дата и время контроля,
- номер контрольной карточки и государство-член, выдавшее 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 регистрации транспортного средства, к которому относится контроль.

Примечание: требования безопасности означают, что загрузка данных карточки регистрируется только в том случае, если она осуществляется через записывающее оборудование.

300) Карточка водителя способна хранить одну такую запись.

#### **4.5.3.2.14 Данные об особых условиях**

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

- дата и время ввода,
- тип особых условий.

302) Карточка водителя способна хранить не менее 56 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 карточка:

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

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

#### **4.5.3.2.16 Данные о местоположении при трёхчасовом непрерывном управлении**

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

- дата и время, когда непрерывное время вождения достигает значения, кратного трём часам,

- местоположение транспортного средства.
- точность ГНСС, дата и время определения положения.

306) Карточка водителя способна хранить не менее 252 таких записей.

## **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***

308) Карточка мастерской способна хранить ряд криптографических ключей и сертификатов, как указано в части А приложения 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 её государство-член, название выдавшего компетентного органа, дата выдачи,
  - дата начала срока действия карточки, дата истечения срока действия карточки.

#### ***4.5.4.1.4 Идентификационные данные владельца карточки***

- 311) Карточка мастерской способна хранить следующие идентификационные данные владельца карточки:
- название мастерской,
  - адрес мастерской,
  - фамилия владельца,
  - имя (имена) владельца,
  - предпочитаемый язык.

#### ***4.5.4.1.5 Загрузка данных карточки***

312) Карточка мастерской способна хранить записанные данные 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 записанные данные о калибровке и/или корректировке времени, произведённой в то время, когда карточка была вставлена в записывающее оборудование.
- 314) Каждая запись калибровки способна хранить следующие данные:
- цель калибровки (активация, первая установка, установка, регулярная проверка),
  - идентификационные данные транспортного средства,

- обновлённые или подтверждённые параметры (w, k, l, размер шин, регулировка устройства ограничения скорости, одометр (новые и старые показания), дата и время (новые и старые значения)),
- идентификационные данные записывающего оборудования (номер детали БУ, серийный номер БУ, серийный номер датчика движения).

315) Карточка мастерской способна хранить не менее 88 таких записей.

316) На карточке мастерской есть счётчик, указывающий на число калибровок, произведённых на карточке.

317) На карточке мастерской есть счётчик, указывающий на число калибровок, произведённых с момента последней загрузки данных.

#### ***4.5.4.1.7 Данные о событиях и неисправностях***

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

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

#### ***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 не менее чем за 1 день средней деятельности водителя.

#### ***4.5.4.1.9 Данные об используемых транспортных средствах***

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

323) Карточка мастерской способна хранить не менее 4 таких записей.

#### ***4.5.4.1.10 Данные о начале и/или окончании дневных периодов работы***

324) Карточка мастерской способна хранить записанные данные о начале и/или окончании дневных периодов работы таким же образом, как и карточка водителя.

325) Карточка мастерской способна хранить не менее 3 пар таких записей.

#### ***4.5.4.1.11 Данные о сеансе использования карточки***

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

#### ***4.5.4.1.12 Данные о контрольных действиях***

327) Карточка мастерской способна хранить записанные данные о контрольных действиях таким же образом, как и карточка водителя.

#### **4.5.4.1.13 Данные об особых условиях**

- 328) Карточка мастерской способна хранить записанные данные об особых условиях таким же образом, как и карточка водителя.
- 329) Карточка мастерской способна хранить не менее 2 таких записей.

#### **4.5.4.2 Приложение тахографа второго поколения (недоступно для бортовых устройств первого поколения)**

##### **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.

##### **4.5.4.2.2 Ключи и сертификаты**

- 331) Карточка мастерской способна хранить ряд криптографических ключей и сертификатов, как указано в части Б приложения 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 её государство-член, название выдавшего компетентного органа, дата выдачи,
  - дата начала срока действия карточки, дата истечения срока действия карточки.

##### **4.5.4.2.4 Идентификационные данные владельца карточки**

- 334) Карточка мастерской способна хранить следующие идентификационные данные владельца карточки:
- название мастерской,
  - адрес мастерской,
  - фамилия владельца,
  - имя (имена) владельца,
  - предпочитаемый язык.

##### **4.5.4.2.5 Загрузка данных карточки**

- 335) Карточка мастерской способна хранить записанные данные 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 записанные данные о калибровке и/или корректировке времени, произведённой в то время, когда карточка была вставлена в записывающее оборудование.
- 337) Каждая запись калибровки способна хранить следующие данные:
- цель калибровки (активация, первая установка, установка, регулярная проверка),
  - идентификационные данные транспортного средства,

- обновлённые или подтверждённые параметры (w, k, l, размер шин, регулировка устройства ограничения скорости, одометр (новые и старые показания), дата и время (новые и старые значения)),
- идентификационные данные записывающего оборудования (номер детали БУ, серийный номер БУ, серийный номер датчика движения, серийный номер средства удалённой связи и серийный номер внешнего устройства ГНСС, если применимо),
- тип и идентификатор всех имеющихся пломб,
- способность БУ работать с карточками тахографов первого поколения (есть или нет).

338) Карточка мастерской способна хранить не менее 88 таких записей.

339) На карточке мастерской есть счётчик, указывающий на число калибровок, произведённых на карточке.

340) На карточке мастерской есть счётчик, указывающий на число калибровок, произведённых с момента последней загрузки данных.

#### ***4.5.4.2.7 Данные о событиях и неисправностях***

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

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

#### ***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 не менее чем за 1 день средней деятельности водителя.

#### ***4.5.4.2.9 Данные об используемых транспортных средствах***

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

346) Карточка мастерской способна хранить не менее 4 таких записей.

#### ***4.5.4.2.10 Данные о начале и/или окончании дневных периодов работы***

347) Карточка мастерской способна хранить записанные данные о начале и/или окончании дневных периодов работы таким же образом, как и карточка водителя.

348) Карточка мастерской способна хранить не менее 3 пар таких записей.

#### ***4.5.4.2.11 Данные о сеансе использования карточки***

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

#### ***4.5.4.2.12 Данные о контрольных действиях***

350) Карточка мастерской способна хранить записанные данные о контрольных действиях таким же образом, как и карточка водителя.

#### **4.5.4.2.13 Данные используемых бортовых устройств**

- 351) Карточка мастерской способна хранить следующие данные, связанные с различными бортовыми устройствами, в которых использовалась карточка:
- дата и время начала периода использования бортового устройства (т.е. первый ввод карточки в бортовое устройство в течение рассматриваемого периода),
  - производитель бортового устройства,
  - тип бортового устройства,
  - номер версии программного обеспечения бортового устройства.
- 352) Карточка мастерской способна хранить не менее 4 таких записей.

#### **4.5.4.2.14 Данные о местоположении при трёхчасовом непрерывном управлении**

- 353) Карточка мастерской способна хранить следующие данные о местоположении транспортного средства, когда непрерывное время управления водителем достигает значения, кратного трём часам:
- дата и время, когда непрерывное время вождения достигает значения, кратного трём часам,
  - местоположение транспортного средства,
  - точность ГНСС, дата и время определения положения.
- 354) Карточка мастерской способна хранить не менее 18 таких записей.

#### **4.5.4.2.15 Данные об особых условиях**

- 355) Карточка мастерской способна хранить записанные данные об особых условиях таким же образом, как и карточка водителя.
- 356) Карточка мастерской способна хранить не менее 2 таких записей.

### **4.5.5 Контрольная карточка**

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

##### **4.5.5.1.1 Идентификационные данные приложения**

- 357) Контрольная карточка способна хранить следующие идентификационные данные приложения:
- идентификационные данные приложения тахографа,
  - идентификационные данные типа карточки тахографа.

##### **4.5.5.1.2 Ключи и сертификаты**

- 358) Контрольная карточка способна хранить ряд криптографических ключей и сертификатов, как указано в части А приложения 11.

##### **4.5.5.1.3 Идентификационные данные карточки**

- 359) Контрольная карточка способна хранить следующие идентификационные данные карточки:
- номер карточки,
  - выдавшее её государство-член, название выдавшего компетентного органа, дата выдачи,
  - дата начала срока действия карточки, дата истечения срока действия карточки (если есть).

##### **4.5.5.1.4 Идентификационные данные владельца карточки**

- 360) Контрольная карточка способна хранить следующие идентификационные данные владельца карточки:

- название контрольного органа,
- адрес контрольного органа,
- фамилия владельца,
- имя (имена) владельца,
- предпочитаемый язык.

#### **4.5.5.1.5 Данные о контрольных действиях**

361) Контрольная карточка способна хранить следующие данные о контрольных действиях:

- 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 придорожная проверка калибровки),
- период, за который загружаются данные (в соответствующих случаях),
- VRN и компетентный орган государства-члена, зарегистрировавший проверенное транспортное средство,
- номер проверенной карточки водителя и выдавшее её государство-член.

362) Контрольная карточка способна хранить не менее 230 таких записей.

### **4.5.5.2 Приложение тахографа второго поколения (недоступно для бортовых устройств первого поколения)**

#### **4.5.5.2.1 Идентификационные данные приложения**

363) Контрольная карточка способна хранить следующие идентификационные данные приложения:

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

#### **4.5.5.2.2 Ключи и сертификаты**

364) Контрольная карточка способна хранить ряд криптографических ключей и сертификатов, как указано в части Б приложения 11.

#### **4.5.5.2.3 Идентификационные данные карточки**

365) Контрольная карточка способна хранить следующие идентификационные данные карточки:

- номер карточки,
- выдавшее её государство-член, название выдавшего компетентного органа, дата выдачи,
- дата начала срока действия карточки, дата истечения срока действия карточки (если есть).

#### **4.5.5.2.4 Идентификационные данные владельца карточки**

366) Контрольная карточка способна хранить следующие идентификационные данные владельца карточки:

- название контрольного органа,
- адрес контрольного органа,
- фамилия владельца,
- имя (имена) владельца,
- предпочитаемый язык.

#### **4.5.5.2.5 Данные о контрольных действиях**

367) Контрольная карточка способна хранить следующие данные о контрольных действиях:

- 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 придорожная проверка калибровки)



- период, за который загружаются данные (в соответствующих случаях),
  - VRN и компетентный орган государства-члена, зарегистрировавший проверенное транспортное средство,
  - номер проверенной карточки водителя и выдавшее её государство-член.
- 368) Контрольная карточка способна хранить не менее 230 таких записей.

## **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***

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

#### ***4.5.6.1.3 Идентификационные данные карточки***

- 371) Карточка предприятия способна хранить следующие идентификационные данные карточки:
- номер карточки,
  - выдавшее её государство-член, название выдавшего компетентного органа, дата выдачи,
  - дата начала срока действия карточки, дата истечения срока действия карточки (если есть).

#### ***4.5.6.1.4 Идентификационные данные владельца карточки***

- 372) Карточка предприятия способна хранить следующие идентификационные данные владельца 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 действия,
  - тип действия (блокировка и/или разблокировка БУ и/или загрузка данных с БУ и/или загрузка с карточки),
  - период, за который загружаются данные (в соответствующих случаях),
  - VRN и компетентный орган государства-члена, зарегистрировавший транспортное средство,
  - номер карточки и выдавшее её государство-член (в случае загрузки данных с карточки).
- 374) Карточка предприятия способна хранить не менее 230 таких записей.

### **4.5.6.2 Приложение тахографа второго поколения (недоступно для бортовых устройств первого поколения)**

#### ***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.

#### **4.5.6.2.2 Ключи и сертификаты**

376) Карточка предприятия способна хранить ряд криптографических ключей и сертификатов, как указано в части Б приложения 11.

#### **4.5.6.2.3 Идентификационные данные карточки**

377) Карточка предприятия способна хранить следующие идентификационные данные карточки:

- номер карточки,
- выдавшее её государство-член, название выдавшего компетентного органа, дата выдачи,
- дата начала срока действия карточки, дата истечения срока действия карточки (если есть).

#### **4.5.6.2.4 Идентификационные данные владельца карточки**

378) Карточка предприятия способна хранить следующие идентификационные данные владельца 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 действия,
- тип действия (блокировка и/или разблокировка БУ и/или загрузка данных с БУ и/или загрузка с карточки),
- период, за который загружаются данные (в соответствующих случаях),
- VRN и компетентный орган государства-члена, зарегистрировавший транспортное средство,
- номер карточки и выдавшее её государство-член (в случае загрузки данных с карточки).

380) Карточка предприятия способна хранить не менее 230 таких записей.

## 5 Установка записывающего оборудования

### 5.1 Установка

- 381) Новое записывающее оборудование поставляется монтажникам или производителям транспортного средства неактивированным со всеми параметрами калибровки, перечисленными в главе 3.21, с установленными соответствующими и действительными значениями по умолчанию. Если не подходит никакое значение, буквенные параметры отображаются в виде строк из вопросительных знаков «?», а числовые параметры устанавливаются на ноль. Доставка деталей записывающего оборудования, имеющих отношение к обеспечению безопасности, может быть ограничена, если требуется, во время процедуры сертификации безопасности.
- 382) До активации записывающее оборудование обеспечивает доступ к функции калибровки, даже если оно не находится в режиме калибровки.
- 383) До активации записывающее оборудование не регистрирует и не хранит данные, указанные в пунктах 3.12.3, 3.12.9 и 3.12.12-3.12.15, включительно.
- 384) В процессе установки производители транспортных средств предварительно устанавливают все известные параметры.
- 385) Производители транспортных средств или монтажники активируют установленное записывающее оборудование не позднее начала эксплуатации транспортного средства, попадающего в область применения Регламента (ЕС) № 561/2006.
- 386) Активация записывающего оборудования происходит автоматически в результате первого ввода действительной карточки предприятия 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 соединению внешнего устройства ГНСС и бортового устройства, если таковые требуются, производятся автоматически до или во время активации.
- 389) После активации записывающее оборудование полностью обеспечивает выполнение функций и пользование правами доступа к данным.
- 390) После активации записывающее оборудование передаёт устройству удалённой связи защищённые данные, необходимые для целевых придорожных проверок.
- 391) Функции регистрации и хранения записывающего оборудования после его активации полностью работоспособны.
- 392) После установки производится калибровка. Первая калибровка не обязана включать в себя ввод регистрационного номера транспортного средства (VRN), если апробированной мастерской, которая проводит калибровку, он неизвестен. В подобных случаях владелец транспортного средства только в этот раз может ввести VRN при помощи своей карточки предприятия до начала эксплуатации транспортного средства, попадающего в область применения Регламента (ЕС) № 561/2006 (например, при помощи команд через соответствующее меню человеко-машинного интерфейса бортового устройства)<sup>10</sup>. Любые обновления или подтверждения такой записи возможны только с помощью карточки мастерской.

<sup>10</sup> ОЖ L 102, 11.4.2006, стр. 1.

- 393) Установка внешнего устройства ГНСС требует соединения с бортовым устройством и последующей проверки информации ГНСС о местоположении.
- 394) Записывающее оборудование должно быть установлено в транспортном средстве таким образом, чтобы водитель имел доступ ко всем необходимым функциям со своего места.

## 5.2 Установочная табличка

- 395) После проверки записывающего оборудования в процессе установки, на него прикрепляется установочная табличка с выгравированным или напечатанным нестираемым текстом, который чётко виден и удобочитаем. Если это невозможно, табличка прикрепляется к средней стойке транспортного средства, чтобы она была хорошо видна. Если в транспортном средстве средней стойки нет, установочная табличка прикрепляется к дверной раме со стороны водителя транспортного средства, чтобы быть хорошо заметной во всех случаях.

После каждой инспекции, проведённой уполномоченным монтажником или мастерской, на месте прежней таблички устанавливается новая.

- 396) На табличке указываются, по крайней мере, следующие сведения:
- название, адрес или фирменный знак уполномоченного монтажника или мастерской,
  - характеристический коэффициент транспортного средства в виде « $w = \text{имп./км}$ »,
  - постоянная величина записывающего оборудования в виде « $k = \dots \text{имп./км}$ »,
  - эффективная окружность шин колёс в виде « $d = \dots \text{мм}$ »,
  - размер шин,
  - дата определения характеристического коэффициента транспортного средства и измерения эффективной окружности шин колёс,
  - идентификационный номер транспортного средства,
  - наличие (или отсутствие) внешнего устройства ГНСС,
  - серийный номер внешнего устройства ГНСС,
  - серийный номер устройства удалённой связи,
  - серийный номер всех имеющихся пломб,
  - часть транспортного средства, в которой установлен адаптер (если он установлен),
  - часть транспортного средства, в которой установлен датчик движения, если он не соединён 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.

- 397) Только в случае транспортных средств категорий M1 и N1, на которых установлен адаптер в соответствии с Регламентом (ЕС) № 68/2009<sup>11</sup> с последними поправками, и если невозможно включить всю необходимую информацию, как указано в требовании 396, можно использовать вторую, дополнительную табличку. В подобных случаях на дополнительной табличке присутствует не менее четырёх пунктов, как описано в требовании 396.

Если используется такая вторая, дополнительная табличка, она закрепляется около или недалеко от первой основной таблички, как описано в требовании 396, и для неё обеспечивается такой же уровень защиты. Кроме того, на второй табличке также указываются название, адрес или фирменный знак уполномоченного монтажника или мастерской, установившей оборудование, и дата установки.

<sup>11</sup> ОЖ L 21, 24.1.2009, стр. 3.

### 5.3 Пломбирование

398) Пломбы накладываются на следующие части:

- Любое соединение, которое в случае рассоединения повлечёт 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);
- Установочная табличка, если она не прикреплена таким образом, что её нельзя снять, не повредив нанесённую на ней маркировку.

399) Указанные 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 продолжает функционировать надёжно и правильно и снова пломбируется уполномоченным монтажником 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 производителем. Это уникальный номер, отличный от любого другого номера пломбы, присвоенного другим производителем пломб.

Такой уникальный идентификационный номер составляется следующим образом: нестираемая маркировка ММ NNNNNN, где ММ – это уникальный идентификационный номер производителя (регистрация в базе данных, администрируемой ЕК), а NNNNNN – это буквенно-цифровой номер, уникальный для производителя.

402) На пломбах имеется свободное пространство, на котором уполномоченные монтажники, мастерские или производители транспортных средств могут поместить особую метку в соответствии со статьёй 22.3 Регламента (ЕС) № 165/2014.

Такая метка не загромождает идентификационный номер пломбы.

403) Производители пломб регистрируются в специальной базе данных и публикуют свои идентификационные номера пломб в соответствии с процедурой, установленной Европейской комиссией.

404) Уполномоченные мастерские и производители транспортных средств в рамках Регламента (ЕС) № 165/2014 используют пломбы только тех производителей пломб, которые перечислены в упомянутой базе данных.

405) Производители пломб и их распространители ведут записи, обеспечивающие полную отслеживаемость проданных пломб, используемых в рамках Регламента (ЕС) № 165/2014, и при необходимости готовы их предоставить компетентным национальным органам.

406) На установочной табличке видны уникальные идентификационные номера пломб.

### 6 Проверки, инспекции и ремонтные работы

Требования к обстоятельствам, при которых могут быть сняты пломбы, как указано в статье 22.5 Регламента (ЕС) № 165/2014, представлены в главе 5.3 настоящего дополнения.

## **6.1 Утверждение монтажников, мастерских и производителей транспортных средств**

Государства-члены утверждают, регулярно контролируют и аттестуют организации, которым поручены следующие задачи:

- установка,
- проверки,
- инспекции,
- ремонтные работы.

Карточки мастерской выдаются только монтажникам и/или мастерским, которые уполномочены активировать и/или калибровать записывающее оборудование в соответствии с настоящим дополнением и, если нет должного обоснования:

- которые не имеют права на карточку предприятия;
- и иная профессиональная деятельность которых не может поставить под угрозу общую защиту системы в соответствии с требованиями приложения 10.

## **6.2 Проверка новых или отремонтированных приборов**

- 407) Каждое отдельное устройство, новое или отремонтированное, проверяется на предмет его надлежащего функционирования и точности показаний и записей в пределах, изложенных в главах 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) Во время установки на транспортное средство весь сборочный узел, включая записывающее оборудование, соответствует положениям, регламентирующим максимальные допуски, указанные в главах 3.2.1, 3.2.2, 3.2.3 и 3.3.

## **6.4 Регулярные проверки**

- 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 20 минут, или в случае изменения VRN не реже одного раза в два года (24 месяца) после последней инспекции.
- 410) Такие инспекции включают в себя следующие проверки:
- что записывающее оборудование работает должным образом, включая функцию хранения данных на карточках тахографов и связь со считывающими устройствами удалённой связи,
  - что обеспечивается соблюдение положений глав 3.2.1 и 3.2.2 о максимальных допусках при установке,
  - что обеспечивается соблюдение положений глав 3.2.3 и 3.3,
  - что записывающее оборудование помечено знаком официального утверждения типа,
  - что установочная табличка, как описано в требовании 396, и описательная табличка, как описано в требовании 225, на месте,
  - размер шин и фактическая окружность шин колёс,

- что к оборудованию не прикреплены никакие средства манипулирования,
  - что пломбы правильно размещены, находятся в хорошем состоянии, что их идентификационные номера действительны (присвоены производителем пломб в базе данных ЕК) и что их идентификационные номера соответствуют меткам на установочной табличке (см. требование 401).
- 411) Если обнаруживается, что с момента последней инспекции произошло одно из событий, перечисленных в главе 3.9 (обнаружение событий и/или неисправностей), и производители тахографов и/или национальных органов считают, что оно может подвергнуть риску безопасность оборудования, мастерская:
- a. сравнивает идентификационные данные датчика движения, подключённого к коробке передач, с данными парного 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 напечатаны на корпусе датчика движения, информации, хранящейся в блоке памяти записывающего оборудования;
  - 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 отчётах об инспекциях хранят любые установленные факты о повреждённых пломбах или устройствах для манипулирования. Такие отчёты хранятся в мастерских не менее 2 лет и по требованию предоставляются компетентным органам.
- 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 снаряжённом состоянии без груза,
  - давление в шинах соответствует инструкциям производителя,
  - износ шин в пределах, допускаемых национальным законодательством,
  - движение транспортного средства:
  - транспортное средство движется вперёд на своем двигателе по прямой линии по ровной дороге на скорости  $50 \pm 5$  км/ч. Измеряемое расстояние составляет не менее 1 000 метров,
  - а для проведения этого испытания могут использоваться альтернативные методы, например, соответствующий испытательный стенд, при условии обеспечения сопоставимой точности.

## **6.6 Ремонтные работы**

- 415) Мастерские имеют возможность загружать данные с записывающего оборудования для их передачи соответствующему транспортному предприятию.
- 416) Утверждённые мастерские выдают транспортным предприятиям свидетельство, подтверждающее невозможность загрузки данных в том случае, когда неисправность записывающего оборудования не позволяет загрузить ранее записанные данные даже после ремонта, произведённого данной мастерской. Мастерские хранят копию каждого выданного свидетельства не менее двух лет.

## **7 Выдача карточек**

Порядок выдачи карточек, установленный государствами-членами, 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 заменённой 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 заменённая 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, или в соответствии с правилами первой выдачи карточки, если это происходит в другом государстве-члене.
- 423) Графа «фамилия владельца карточки» в случае неиндивидуальных карточек мастерской или контрольных карточек, заполняется названием мастерской или контрольного органа, или фамилией монтажника или контролёра, если государство-член приняло такое решение.
- 424) Государства-члены обмениваются данными в электронном виде, чтобы обеспечить уникальность карточек водителя, которые они выдают, в соответствии с Регламентом (ЕС) № 165/2014.

## **8 Утверждение типа записывающего оборудования и карточек тахографов**

### **8.1 Общие вопросы**

В настоящем разделе выражение «записывающее оборудование» означает «записывающее оборудование или его компоненты». Для кабеля (кабелей) соединения датчика движения с БУ, внешнего устройства ГНСС с БУ или устройства удалённой связи с БУ официальное утверждение типа не требуется. Бумага, используемая в записывающем оборудовании, считается компонентом записывающего оборудования.

Любой производитель может обращаться за официальным утверждением типа компонента с любым типом датчика движения, внешнего устройства ГНСС и наоборот, если каждый из этих компонентов соответствует требованиям настоящего дополнения. В противном случае производители также могут обращаться за официальным утверждением типа записывающего оборудования.

- 425) Записывающее оборудование представляется на официальное утверждение в сборе со всеми комплектующими дополнительными устройствами.
- 426) Официальное утверждение типа записывающего оборудования и карточек тахографа включает в себя испытания защиты, функциональные испытания, испытания на эксплуатационную совместимость.



Положительные результаты каждого из таких испытаний подтверждаются соответствующим сертификатом.

- 427) Органы официального утверждения типа государств-членов не выдают свидетельство об утверждении типа, если нет:
- сертификата защиты,
  - сертификата функциональности,
  - и сертификата эксплуатационной совместимости

в отношении записывающего оборудования или карточки тахографа, являющихся предметом заявки на утверждение типа.

- 428) Любое изменение программного обеспечения или аппаратного оборудования или характера материалов, использованных для его изготовления, в предварительном порядке доводится до сведения компетентного органа, который предоставил официальное утверждение типа оборудования. Такой орган подтверждает производителю факт продления действия утверждения типа или может потребовать обновления или подтверждения соответствующих сертификатов функциональности, безопасности и/или эксплуатационной совместимости.

- 429) Процедуры модернизации программного обеспечения записывающего оборудования на месте утверждаются органом, который предоставил утверждение типа записывающего оборудования. При модернизации программного обеспечения не должны изменяться или удаляться никакие данные о деятельности водителя, которые хранятся в памяти записывающего оборудования. Модернизация программного обеспечения может проводиться только под ответственность производителя оборудования.

- 430) Утверждение типа изменений программного обеспечения с целью модернизации записывающего оборудования ранее утверждённого типа не может быть отклонено, если такие изменения относятся только к функциям, не указанным в настоящем дополнении. Модернизация программного обеспечения записывающего оборудования может не охватывать введения новых наборов символов, если это технически неосуществимо.

## **8.2 Сертификат защиты**

- 431) Сертификат защиты выдаётся в соответствии с положениями приложения 10 настоящего дополнения. Подлежащие сертификации компоненты записывающего оборудования включают в себя бортовое устройство, датчик движения, внешнее устройство ГНСС и карточки тахографов.

- 432) В исключительных обстоятельствах, когда органы, сертифицирующие защиту, отказываются сертифицировать новое оборудование на основании устаревания механизмов защиты, утверждения типа остаётся действительным в таких особых и исключительных обстоятельствах, только если нет альтернативного решения, соответствующего регламенту.

- 433) В подобных случаях соответствующее государство-член незамедлительно информирует Европейскую комиссию, которая в течение двенадцати календарных месяцев после предоставления утверждения типа начинает процедуру восстановления уровня безопасности до исходного уровня.

## **8.3 Сертификат функциональности**

- 434) Каждый претендент на получение официального утверждения типа направляет компетентному органу государства-члена, предоставляющему официальное утверждение типа, все материалы и документацию, которые такой компетентный орган считает необходимыми.

- 435) Производители предоставляют соответствующие образцы изделий, претендующих на утверждение типа, и связанные с ними документы, требуемые лабораториями, назначенными ответственными за проведение

функциональных испытаний, в течение одного месяца с момента подачи заявки. Все расходы, связанные с заявкой, берёт на себя подающий её субъект. Лаборатории хранят конфиденциальность всей информации, представляющей собой коммерческую тайну.

- 436) Сертификат функциональности выдаётся производителю только по итогам всех успешно проведенных функциональных испытаний, предусмотренных, по крайней мере, в приложении 9.
- 437) Орган по утверждению типа выдаёт сертификат о функциональности. В таком сертификате, помимо названия его получателя и идентификационных данных образцы, даётся подробный перечень проведенных испытаний и полученных результатов.
- 438) Сертификат функциональности любого компонента записывающего оборудования также содержит номера официального утверждения типа компонентов другого совместимого записывающего оборудования утвержденного типа, прошедших испытания для получения настоящего сертификата.
- 439) Сертификат функциональности любого компонента записывающего оборудования также содержит ссылку на стандарт ISO или ЕКС, по которому сертифицирован функциональный интерфейс.

## **8.4 Сертификат эксплуатационной совместимости**

- 440) Испытания на эксплуатационную совместимость проводятся одной лабораторией под руководством и при ответственности Европейской комиссии.
- 441) Лаборатория регистрирует заявки на проведение проверок на эксплуатационную совместимость, подаваемые производителями, 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 эксплуатационной совместимости,
  - соответствующего сертификата защиты,
  - соответствующего сертификата функциональности,

Дата регистрации заявки доводится до сведения производителя.

- 443) Лаборатории не проводят испытаний эксплуатационной совместимости в отношении записывающего оборудования или карточек тахографов, которым не выданы сертификат защиты и сертификат функциональности, кроме случаев исключительных обстоятельств, указанных в требовании 432.
- 444) Любой производитель, подавший заявку на проведение испытаний на эксплуатационную совместимость, берёт на себя обязательство передать на хранение лаборатории, уполномоченной проводить эти испытания, весь комплект материалов и документов, которые он предоставил для проведения испытаний.
- 445) Испытания эксплуатационной совместимости проводятся в соответствии с положениями приложения 9 настоящего дополнения в отношении всех типов записывающего оборудования или карточек тахографов:
- для которых ещё действительно утверждение типа или
  - которые ожидают выдачи утверждения типа и имеют действительный сертификат эксплуатационной совместимости.

- 446) Испытания эксплуатационной совместимости охватывают все поколения записывающего оборудования или карточек тахографов, которые ещё используются.
- 447) Сертификат эксплуатационной совместимости выдаётся лабораторией производителю только по итогам всех успешно проведённых испытаний на эксплуатационную совместимость.
- 448) Если одна или несколько единиц записывающего оборудования или карточек тахографов не прошли испытания на эксплуатационную совместимость, сертификат эксплуатационной совместимости не выдаётся до тех пор, пока производитель, подавший заявку, не произведёт необходимые изменения и не проведёт успешные испытания на эксплуатационную совместимость. Лаборатория определяет причину проблемы с помощью производителей, которых касается данное несоответствие требованиям к эксплуатационной совместимости, и стремится оказать производителю, подавшему заявку, помощь в поиске соответствующего технического решения. Если производитель модифицировал своё изделие, он обязан удостовериться в соответствующих компетентных органах в том, что сертификат защиты и сертификат функциональности продолжают действовать.
- 449) Сертификат эксплуатационной совместимости действует в течение шести месяцев. Если производитель не получил соответствующего свидетельства об официальном утверждении типа, его срок действия в конце этого периода истекает. Производитель передаёт его компетентному органу государства-члена, выдающему утверждение типа, который выдал 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 утверждения типа**

- 451) Орган государства-члена, выдающий официальное утверждение типа, может выдавать свидетельство об официальном утверждении типа после получения всех трёх сертификатов.
- 452) Сертификат утверждения типа любого компонента записывающего оборудования также содержит номера официального утверждения типа компонентов другого совместимого записывающего оборудования утверждённого типа.
- 453) Копия свидетельства об официальном утверждении 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 публичный веб-сайт, на котором обновляется перечень образцов записывающего оборудования или карточек тахографов:
- в отношении которых зарегистрирована заявка на испытания на эксплуатационную совместимость,
  - которые получили сертификат эксплуатационной совместимости (хотя бы временный),
  - которые получили сертификат утверждения типа.

## **8.6 Исключительная процедура: первые сертификаты эксплуатационной совместимости для записывающего оборудования и карточек тахографов второго поколения**

- 455) До истечения четырёх месяцев после подтверждения эксплуатационной совместимости первой пары записывающего оборудования и карточек тахографов второго поколения (карточек водителя, мастерской, контрольной карточки и карточки предприятия), любой сертификат эксплуатационной совместимости (включая первые), выданный по заявкам, 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 эксплуатационной совместимости, находит причины проблем с помощью всех заинтересованных производителей 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 производителями и органами утверждения типа, выдавшими соответствующие сертификаты функциональности, устанавливает причины несоответствия требованиям эксплуатационной совместимости и принимает решение о том, какие изменения должен внести каждый заинтересованный производитель. 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, какому оборудованию и карточкам выдать постоянные сертификаты эксплуатационной совместимости, и указывает причины своего решения.
- 459) Любые заявки на испытания эксплуатационной совместимости, регистрируемые лабораторией с конца четырёхмесячного периода после выдачи первого временного сертификата эксплуатационной совместимости и даты решения Комиссии, указанного в требовании 455, откладываются до разрешения начальных проблем с эксплуатационной совместимостью. Впоследствии такие заявки обрабатываются в хронологическом порядке согласно их регистрации.

\*\*\*

**RU**

**Приложение 1. Словарь данных**

## СОДЕРЖАНИЕ

<b>1. ВВЕДЕНИЕ.....</b>	<b>90</b>
<b>1.1. Метод определения типов данных .....</b>	<b>90</b>
<b>1.2. Ссылки .....</b>	<b>90</b>
<b>2. ОПРЕДЕЛЕНИЯ ТИПОВ ДАННЫХ.....</b>	<b>92</b>
<b>2.1. ActivityChangeInfo .....</b>	<b>92</b>
<b>2.2. Address.....</b>	<b>93</b>
<b>2.3. AESKey .....</b>	<b>93</b>
<b>2.4. AES128Key .....</b>	<b>94</b>
<b>2.5. AES192Key .....</b>	<b>94</b>
<b>2.6. AES256Key .....</b>	<b>94</b>
<b>2.7. BCDString.....</b>	<b>95</b>
<b>2.8. CalibrationPurpose .....</b>	<b>95</b>
<b>2.9. CardActivityDailyRecord .....</b>	<b>96</b>
<b>2.10. CardActivityLengthRange .....</b>	<b>96</b>
<b>2.11. CardApprovalNumber.....</b>	<b>96</b>
<b>2.12. CardCertificate.....</b>	<b>96</b>
<b>2.13. CardChipIdentification.....</b>	<b>97</b>
<b>2.14. CardConsecutiveIndex.....</b>	<b>97</b>
<b>2.15. CardControlActivityDataRecord.....</b>	<b>97</b>
<b>2.16. CardCurrentUse.....</b>	<b>98</b>
<b>2.17. CardDriverActivity .....</b>	<b>98</b>
<b>2.18. CardDrivingLicenceInformation .....</b>	<b>99</b>
<b>2.19. CardEventData .....</b>	<b>99</b>
<b>2.20. CardEventRecord.....</b>	<b>99</b>
<b>2.21. CardFaultData.....</b>	<b>100</b>
<b>2.22. CardFaultRecord.....</b>	<b>100</b>
<b>2.23. CardIceIdentification.....</b>	<b>101</b>
<b>2.24. CardIdentification .....</b>	<b>101</b>
<b>2.25. CardMACertificate .....</b>	<b>101</b>
<b>2.26. CardNumber.....</b>	<b>102</b>
<b>2.27. CardPlaceDailyWorkPeriod.....</b>	<b>102</b>
<b>2.28. CardPrivateKey.....</b>	<b>102</b>

---

2.29.	CardPublicKey .....	103
2.30.	CardRenewalIndex.....	103
2.31.	CardReplacementIndex .....	103
2.32.	CardSignCertificate .....	103
2.33.	CardSlotNumber .....	103
2.34.	CardSlotsStatus .....	104
2.35.	CardSlotsStatusRecordArray .....	104
2.36.	CardStructureVersion .....	105
2.37.	CardVehicleRecord .....	105
2.38.	CardVehiclesUsed .....	106
2.39.	CardVehicleUnitRecord .....	107
2.40.	CardVehicleUnitsUsed .....	107
2.41.	Certificate.....	107
2.42.	CertificateContent .....	108
2.43.	CertificateHolderAuthorisation .....	108
2.44.	CertificateRequestID.....	109
2.45.	CertificationAuthorityKID .....	109
2.46.	CompanyActivityData.....	110
2.47.	CompanyActivityType .....	111
2.48.	CompanyCardApplicationIdentification .....	111
2.49.	CompanyCardHolderIdentification .....	111
2.50.	ControlCardApplicationIdentification.....	111
2.51.	ControlCardControlActivityData.....	112
2.52.	ControlCardHolderIdentification.....	112
2.53.	ControlType .....	113
2.54.	CurrentDateTime .....	113
2.55.	CurrentDateTimeRecordArray .....	114
2.56.	DailyPresenceCounter.....	114
2.57.	Datef.....	114
2.58.	DateOfDayDownloaded .....	114
2.59.	DateOfDayDownloadedRecordArray.....	115
2.60.	Distance .....	115
2.61.	DriverCardApplicationIdentification.....	115

---

2.62.	DriverCardHolderIdentification.....	116
2.63.	DSRCSecurityData.....	116
2.64.	EGFCertificate.....	117
2.65.	EmbedderIcAssemblerId.....	117
2.66.	EntryTypeDailyWorkPeriod .....	118
2.67.	EquipmentType .....	118
2.68.	EuropeanPublicKey .....	119
2.69.	EventFaultRecordPurpose .....	119
2.70.	EventFaultType .....	120
2.71.	ExtendedSealIdentifier .....	121
2.72.	ExtendedSerialNumber.....	122
2.73.	FullCardNumber .....	123
2.74.	FullCardNumberAndGeneration .....	123
2.75.	Generation.....	123
2.76.	GeoCoordinates .....	123
2.77.	GNSSAccuracy .....	124
2.78.	GNSSContinuousDriving.....	124
2.79.	GNSSContinuousDrivingRecord .....	124
2.80.	GNSSPlaceRecord .....	125
2.81.	HighResOdometer .....	125
2.82.	HighResTripDistance.....	125
2.83.	HolderName .....	125
2.84.	InternalGNSSReceiver.....	126
2.85.	K-ConstantOfRecordingEquipment.....	126
2.86.	KeyIdentifier.....	126
2.87.	KMWCKey .....	126
2.88.	Language .....	126
2.89.	LastCardDownload .....	127
2.90.	LinkCertificate.....	127
2.91.	L-TyreCircumference .....	127
2.92.	MAC .....	127
2.93.	ManualInputFlag.....	127
2.94.	ManufacturerCode.....	128



2.95.	ManufacturerSpecificEventFaultData .....	128
2.96.	MemberStateCertificate .....	128
2.97.	MemberStateCertificateRecordArray .....	128
2.98.	MemberStatePublicKey .....	129
2.99.	Name .....	129
2.100.	NationAlpha .....	129
2.101.	NationNumeric.....	129
2.102.	NoOfCalibrationRecords.....	129
2.103.	NoOfCalibrationsSinceDownload .....	130
2.104.	NoOfCardPlaceRecords.....	130
2.105.	NoOfCardVehicleRecords .....	130
2.106.	NoOfCardVehicleUnitRecords.....	130
2.107.	NoOfCompanyActivityRecords.....	130
2.108.	NoOfControlActivityRecords .....	130
2.109.	NoOfEventsPerType .....	131
2.110.	NoOfFaultsPerType .....	131
2.111.	NoOfGNSSCDRecords .....	131
2.112.	NoOfSpecificConditionRecords .....	131
2.113.	OdometerShort .....	131
2.114.	OdometerValueMidnight.....	131
2.115.	OdometerValueMidnightRecordArray .....	131
2.116.	OverspeedNumber.....	132
2.117.	PlaceRecord .....	132
2.118.	PreviousVehicleInfo .....	133
2.119.	PublicKey .....	133
2.120.	RecordType.....	134
2.121.	RegionAlpha .....	134
2.122.	RegionNumeric .....	135
2.123.	RemoteCommunicationModuleSerialNumber .....	136
2.124.	RSAPublicModulus.....	136
2.125.	RSAPrivateExponent .....	136
2.126.	RSAPublicExponent.....	136
2.127.	RtmData .....	136

---

2.128.	SealDataCard.....	136
2.129.	SealDataVu .....	137
2.130.	SealRecord .....	137
2.131.	SensorApprovalNumber .....	137
2.132.	SensorExternalGNSSApprovalNumber .....	138
2.133.	SensorExternalGNSSCoupledRecord .....	138
2.134.	SensorExternalGNSSIdentification .....	139
2.135.	SensorExternalGNSSInstallation.....	139
2.136.	SensorExternalGNSSOSIdentifier.....	140
2.137.	SensorExternalGNSSSCIIdentifier .....	140
2.138.	SensorGNSSCouplingDate .....	140
2.139.	SensorGNSSSerialNumber .....	140
2.140.	SensorIdentification .....	140
2.141.	SensorInstallation.....	141
2.142.	SensorInstallationSecData .....	141
2.143.	SensorOSIdentifier .....	141
2.144.	SensorPaired .....	142
2.145.	SensorPairedRecord.....	142
2.146.	SensorPairingDate.....	142
2.147.	SensorSCIIdentifier .....	142
2.148.	SensorSerialNumber .....	143
2.149.	Signature .....	143
2.150.	SignatureRecordArray .....	143
2.151.	SimilarEventsNumber.....	143
2.152.	SpecificConditionRecord .....	143
2.153.	SpecificConditions .....	144
2.154.	SpecificConditionType .....	144
2.155.	Speed.....	145
2.156.	SpeedAuthorised.....	145
2.157.	SpeedAverage.....	145
2.158.	SpeedMax .....	145
2.159.	TachographPayload .....	145
2.160.	TachographPayloadEncrypted .....	145

---

2.161.	TDesSessionKey .....	146
2.162.	TimeReal .....	146
2.163.	TyreSize.....	146
2.164.	VehicleIdentificationNumber .....	146
2.165.	VehicleIdentificationNumberRecordArray .....	146
2.166.	VehicleRegistrationIdentification .....	147
2.167.	VehicleRegistrationNumber .....	147
2.168.	VehicleRegistrationNumberRecordArray .....	147
2.169.	VuAbility .....	148
2.170.	VuActivityDailyData .....	148
2.171.	VuActivityDailyRecordArray .....	148
2.172.	VuApprovalNumber .....	149
2.173.	VuCalibrationData.....	149
2.174.	VuCalibrationRecord.....	150
2.175.	VuCalibrationRecordArray .....	151
2.176.	VuCardIWData .....	152
2.177.	VuCardIWRecord .....	152
2.178.	VuCardIWRecordArray.....	153
2.179.	VuCardRecord.....	153
2.180.	VuCardRecordArray .....	154
2.181.	VuCertificate.....	154
2.182.	VuCertificateRecordArray .....	154
2.183.	VuCompanyLocksData.....	155
2.184.	VuCompanyLocksRecord.....	155
2.185.	VuCompanyLocksRecordArray .....	156
2.186.	VuControlActivityData.....	156
2.187.	VuControlActivityRecord.....	157
2.188.	VuControlActivityRecordArray .....	157
2.189.	VuDataBlockCounter.....	158
2.190.	VuDetailedSpeedBlock.....	158
2.191.	VuDetailedSpeedBlockRecordArray .....	158
2.192.	VuDetailedSpeedData .....	158
2.193.	VuDownloadablePeriod .....	159

---

2.194.	VuDownloadablePeriodRecordArray .....	159
2.195.	VuDownloadActivityData.....	159
2.196.	VuDownloadActivityDataRecordArray .....	160
2.197.	VuEventData.....	160
2.198.	VuEventRecord .....	161
2.199.	VuEventRecordArray .....	162
2.200.	VuFaultData.....	163
2.201.	VuFaultRecord .....	163
2.202.	VuFaultRecordArray .....	164
2.203.	VuGNSSCDRecord .....	164
2.204.	VuGNSSCDRecordArray .....	165
2.205.	VuIdentification.....	165
2.206.	VuIdentificationRecordArray .....	166
2.207.	VuITSConsentRecord .....	166
2.208.	VuITSConsentRecordArray.....	167
2.209.	VuManufacturerAddress.....	167
2.210.	VuManufacturerName.....	167
2.211.	VuManufacturingDate .....	167
2.212.	VuOverSpeedingControlData .....	168
2.213.	VuOverSpeedingControlDataRecordArray .....	168
2.214.	VuOverSpeedingEventData .....	168
2.215.	VuOverSpeedingEventRecord .....	169
2.216.	VuOverSpeedingEventRecordArray .....	169
2.217.	VuPartNumber .....	170
2.218.	VuPlaceDailyWorkPeriodData .....	170
2.219.	VuPlaceDailyWorkPeriodRecord .....	170
2.220.	VuPlaceDailyWorkPeriodRecordArray.....	171
2.221.	VuPrivateKey.....	172
2.222.	VuPublicKey .....	172
2.223.	VuSerialNumber .....	172
2.224.	VuSoftInstallationDate .....	172
2.225.	VuSoftwareIdentification .....	172
2.226.	VuSoftwareVersion .....	172

2.227.	VuSpecificConditionData .....	172
2.228.	VuSpecificConditionRecordArray.....	173
2.229.	VuTimeAdjustmentData.....	173
2.230.	VuTimeAdjustmentGNSSRecord .....	173
2.231.	VuTimeAdjustmentGNSSRecordArray.....	174
2.232.	VuTimeAdjustmentRecord .....	174
2.233.	VuTimeAdjustmentRecordArray .....	175
2.234.	WorkshopCardApplicationIdentification .....	176
2.235.	WorkshopCardCalibrationData .....	177
2.236.	WorkshopCardCalibrationRecord .....	177
2.237.	WorkshopCardHolderIdentification .....	179
2.238.	WorkshopCardPIN .....	179
2.239.	W-VehicleCharacteristicConstant .....	179
2.240.	VuPowerSupplyInterruptionRecord .....	180
2.241.	VuPowerSupplyInterruptionRecordArray.....	180
2.242.	VuSensorExternalGNSSCoupledRecordArray.....	181
2.243.	VuSensorPairedRecordArray .....	181
3.	ОПРЕДЕЛЕНИЯ ДИАПАЗОНОВ ЗНАЧЕНИЙ И РАЗМЕРОВ .....	182
4.	НАБОРЫ СИМВОЛОВ.....	182
5.	КОДИРОВКА .....	182
6.	ИДЕНТИФИКАТОРЫ ОБЪЕКТОВ И ПРИЛОЖЕНИЙ .....	182
6.1.	Идентификаторы объектов .....	182
6.2.	Идентификаторы приложения .....	183

## 1. Введение

В настоящем приложении уточняются форматы данных, элементы данных и структуры данных, подлежащие использованию в записывающем оборудовании и карточках тахографа.

### 1.1. Метод определения типов данных

Для определения типов данных в настоящем приложении 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 данным.

Если какой-либо тип ASN.1 уже определён в качестве того или иного стандарта и если он подходит для использования в записывающем оборудовании, в данном приложении будет определён и этот тип ASN.1.

Для того, чтобы можно было использовать несколько типов правил кодирования, некоторые типы ASN.1 в настоящем приложении ограничиваются соответствующими идентификаторами диапазона значений. Идентификаторы диапазона значений определяются в пункте 3 и приложении 2.

### 1.2. Ссылки

В настоящем приложении используются следующие источники:

ISO 639	Код отображения названий языков. 1-е издание: 1988.
ISO 3166	Коды отображения названий стран и их частей. Часть 1: коды стран, 2013
ISO 3779	Дорожные транспортные средства. Оповестительный номер транспортного средства (VIN). Содержание и структура. 2009
ISO/IEC 7816-5	Идентификационные карточки – карточки с интегральными микросхемами. Часть 5: регистрация подателей заявок. 2-е издание: 2004.
ISO/IEC 7816-6	Идентификационные карточки – карточки с интегральными микросхемами. Часть 6: межотраслевые элементы данных для обмена, 2004 + техническая поправка 1: 2006
ISO/IEC 8824-1	Информационные технологии. Абстрактное описание синтаксиса версии 1 (ASN.1): спецификация базового описания. 2008 + техническая поправка 1: 2012 и техническая поправка 2: 2014.
ISO/IEC 8825-2	Информационные технологии. Правила кодирования ASN.1: спецификация правил компактного кодирования (PER). 2008.
ISO/IEC 8859-1	Информационные технологии. 8-битные однобайтовые кодированные наборы графических символов. Часть 1: латиница № 1. 1-е издание: 1998.
ISO/IEC 8859-7	Информационные технологии. 8-битные однобайтовые кодированные наборы графических символов. Часть 7: латиница/греческий алфавит. 2003.
ISO 16844-3	Дорожные транспортные средства. Системы тахографов. Интерфейс датчика движения. 2004 + техническая поправка 1: 2006.

TR-03110-3      Технические руководящие принципы BSI/ANSSI TR-03110-3, механизмы повышенной безопасности для машиночитываемых проездных документов и токенов eIDAS. Часть 3: общие спецификации, версия 2.20, 3. Февраль 2015 г.

## 2. Определения типов данных

В случае любого из следующих типов данных значение по умолчанию содержания «нет данных» или «неприменимо» определяется посредством заполнения соответствующего элемента данных с помощью байтов «FF».

Все типы данных используются для приложений первого и второго поколений, если не указано иначе.

### 2.1. ActivityChangeInfo

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 изменения вида деятельности и/или изменения статуса управления и/или изменения статуса карточки водителя или второго водителя. Данный тип данных связан с требованиями 105, 266, 291, 320, 321, 343 и 344 в приложении 1С.

ActivityChangeInfo ::= OCTET STRING (SIZE(2))

**Присвоение значения – выровненный октет:** ‘scpaatttttttt’В (16 бит)

Для записи данных в блок памяти (или состояние считывающего устройства):

‘s’В	Считывающее устройство: ‘0’В: DRIVER, ‘1’В: CO-DRIVER,
‘c’В	Статус управления: ‘0’В: SINGLE, ‘1’В: CREW,
‘p’В устройстве:	Статус карточки водителя (или мастерской) в соответствующем считывающем устройстве: ‘0’В: INSERTED, карточка вставлена, ‘1’В: NOT INSERTED, карточка не вставлена (или извлечена),
‘aa’В	Деятельность: ‘00’В: BREAK/REST, ‘01’В: AVAILABILITY, ‘10’В: WORK, ‘11’В: DRIVING,
‘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 (неактуально, если 'р'=1, за исключением примечания ниже):	
	'0'В: DRIVER,	
	'1'В: CO-DRIVER,	
'с'В (случай 'р'=1):	Статус управления (случай 'р'=0) или	Статус следующего вида деятельности
	'0'В: SINGLE,	'0'В: UNKNOWN
	'1'В: CREW,	'1'В: KNOWN (= введено вручную)
'р'В	Статус карточки:	
	'0'В: INSERTED, карточка вставлена в записывающее оборудование,	
	'1'В: NOT INSERTED, карточка не вставлена (или извлечена),	
'aa'В	Деятельность (неактуально, если 'р'=1 и 'с'=0, за исключением примечания ниже):	
	'00'В: BREAK/REST,	
	'01'В: AVAILABILITY,	
	'10'В: WORK,	
	'11'В: DRIVING,	
'tttttttt'В	Время изменения: число минут, начиная с 00:00 часов на данный день.	

#### Примечание на случай «извлечения карточки»:

Когда карточка извлечена:

- знак 's' применим и указывает на считывающее устройство, из которого извлечена карточка,
- 'с' должно быть установлено на 0,
- 'р' 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.

```
Address ::= SEQUENCE {
    codePage          INTEGER (0..255),
    address           OCTET STRING (SIZE (35))
}
```

**codePage** определяет набор символов, указанный в главе 4,

**address** представляет собой адрес, закодированный с помощью указанного набора символов.

## 2.3. AESKey

**Второе поколение:**

Ключ AES длиной 128, 192 или 256 бит.

```
AESKey ::= CHOICE {  
    aes128Key          AES128Key,  
    aes192Key          AES192Key,  
    aes256Key          AES256Key  
}
```

**Присвоение значения:** дополнительно не указывается.

## 2.4. AES128Key

**Второе поколение:**

Ключ AES128.

```
AES128Key ::= SEQUENCE {  
    length              INTEGER(0..255),  
    aes128Key          OCTET STRING (SIZE(16))  
}
```

**length** обозначает октетную длину ключа AES128.

**aes128Key** – ключ AES длиной 128 бит.

**Присвоение значения:**

значение длины – 16.

## 2.5. AES192Key

**Второе поколение:**

Ключ AES192.

```
AES192Key ::= SEQUENCE {  
    length              INTEGER(0..255),  
    aes192Key          OCTET STRING (SIZE(24))  
}
```

**length** обозначает октетную длину ключа AES192.

**aes192Key** – ключ AES длиной 192 бит.

**Присвоение значения:**

значение длины – 24.

## 2.6. AES256Key

**Второе поколение:**

Ключ AES256.

```
AES256Key ::= SEQUENCE {  
    length              INTEGER(0..255),  
    aes256Key          OCTET STRING (SIZE(32))  
}
```

**length** обозначает октетную длину ключа AES256.

**aes256Key** – ключ AES длиной 256 бит.

**Присвоение значения:**

значение длины – 32.

## 2.7. BCDString

BCDString используется для отображения десятичного числа в двоичном коде (BCD). Этот тип данных используется для отображения одного десятичного знака в полуоктете (4 бита). BCDString определяется в соответствии со стандартом ISO/IEC 8824-1 CharacterStringType.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
  identification ( WITH COMPONENTS {
    fixed PRESENT }) })
```

BCDString использует нотацию «hstring». Крайняя левая шестнадцатеричная цифра представляет собой самый значимый полуоктет первого октета. Для получения нескольких октетов после крайнего левого полуоктета первого октета по мере необходимости включается соответствующее число нулевых полуоктетов.

Допустимые цифры: 0, 1, .. 9.

## 2.8. CalibrationPurpose

Данный код указывает причину регистрации набора параметров калибровки. Данный тип данных связан с требованиями 097 и 098 приложения 1B и требованием 119 приложения 1C.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

### Присвоение значения:

Первое поколение:

- ‘00’H зарезервированное значение,
- ‘01’H активация: регистрация известных параметров калибровки в момент включения БУ,
- ‘02’H первая установка: первая калибровка БУ после его активации,
- ‘03’H установка: первая калибровка БУ на текущем транспортном средстве,
- ‘04’H регулярная проверка.

Второе поколение:

В дополнение к первому поколению, используются следующие значения:

- ‘05’H ввод VRN предприятием,
- ‘06’H корректировка времени без калибровки,
- от ‘07’H до ‘7F’H RFU, от ‘80’H до ‘FF’H зависит от производителя.

## 2.9. CardActivityDailyRecord

Информация, которая хранится на карточке, относится к деятельности водителя за конкретный календарный день. Данный тип данных связан с требованиями 266, 291, 320 и 343 в приложении 1С.

```
CardActivityDailyRecord ::= SEQUENCE {
    activityPreviousRecordLength    INTEGER(0..CardActivityLengthRange),
    activityRecordLength            INTEGER(0..CardActivityLengthRange),
    activityRecordDate              TimeReal,
    activityDailyPresenceCounter    DailyPresenceCounter,
    activityDayDistance             Distance,
    activityChangeInfo              SET SIZE(1..1440) OF ActivityChangeInfo
}
```

**activityPreviousRecordLength** – общая длина предыдущей ежедневной записи в байтах. Максимальное значение определяется в виде длины ОКТЕТНОЙ СТРОКИ, содержащей эти записи (см. CardActivityLengthRange приложение 2, пункт 4). Когда эта запись становится самой старой ежедневной записью, значение activityPreviousRecordLength должно устанавливаться на 0.

**activityRecordLength** – общая длина данной записи в байтах. Максимальное значение определяется в виде длины ОКТЕТНОЙ СТРОКИ, содержащей эти записи.

**activityRecordDate** – дата записи.

**activityDailyPresenceCounter** – счётчик ежедневного наличия карточки на данный день.

**activityDayDistance** – общее расстояние, пройденное за данный день.

**activityChangeInfo** – набор данных ActivityChangeInfo в отношении водителя на данный день. Он может содержать максимум 1 440 значений (изменение вида деятельности 1 раз в минуту). Этот набор данных всегда включает кодирование статуса водителя activityChangeInfo на 00:00 часов.

## 2.10. CardActivityLengthRange

Число байтов на карточке водителя или мастерской, которые предусмотрены для хранения записей, касающихся деятельности водителя.

```
CardActivityLengthRange ::= INTEGER(0..216-1)
```

**Присвоение значения:** см. приложение 2.

## 2.11. CardApprovalNumber

Номер официального утверждения типа карточки.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

**Присвоение значения:**

Номер официального утверждения указывается в соответствии с публикацией на соответствующем веб-сайте Европейской комиссии, например, с дефисами, если они есть. Номер официального утверждения смещён влево.

## 2.12. CardCertificate

Первое поколение:

Сертификат открытого ключа карточки.

```
CardCertificate ::= Certificate
```

## 2.13. *CardChipIdentification*

Информация, записанная на карточке, которая относится к идентификации интегральной схемы карточки (ИС) (требование 249 приложения 1С). `icSerialNumber` вместе с `icManufacturingReferences` представляют собой уникальный определитель микросхемы карточки. Один только `icSerialNumber` не является уникальным определителем микросхемы карточки.

```
CardChipIdentification ::= SEQUENCE {
    icSerialNumber          OCTET STRING (SIZE(4)),
    icManufacturingReferences OCTET STRING (SIZE(4))
}
```

**icSerialNumber** – серийный номер ИС.

**icManufacturingReferences** – конкретный идентификатор производителя ИС.

## 2.14. *CardConsecutiveIndex*

Порядковый индекс карточки (определение h)).

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

**Присвоение значения:** (см. приложение 1С, глава 7)

Порядок повышения: ‘0 , ..., 9, A , ... , Z , a , ... , z’

## 2.15. *CardControlActivityDataRecord*

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к последней проверке, которой подвергался водитель (приложение 1С, требования 274, 299, 327 и 350).

```
CardControlActivityDataRecord ::= SEQUENCE {
    controlType          ControlType,
    controlTime          TimeReal,
    controlCardNumber   FullCardNumber,
    controlVehicleRegistration VehicleRegistrationIdentification,
    controlDownloadPeriodBegin TimeReal,
    controlDownloadPeriodEnd TimeReal
}
```

**controlType** – тип контроля.

**controlTime** – дата и время контроля.

**controlCardNumber** – FullCardNumber контролёра, проводившего проверку.

**controlVehicleRegistration** – VRN и государство-член регистрации транспортного средства, к которому относится контроль.

**controlDownloadPeriodBegin** и **controlDownloadPeriodEnd** – период, за который загружаются данные, в случае загрузки.

## 2.16. *CardCurrentUse*

Информация о фактическом пользовании карточкой (приложение 1С, требования 273, 298, 326 и 349).

```
CardCurrentUse ::= SEQUENCE {
    sessionOpenTime           TimeReal,
    sessionOpenVehicle       VehicleRegistrationIdentification
}
```

**sessionOpenTime** – время, когда карточка была вставлена для текущего использования. При извлечении карточки данный элемент устанавливается на ноль.

**sessionOpenVehicle** – идентификация текущего используемого транспортного средства, установленная при вводе карточки. При извлечении карточки данный элемент устанавливается на ноль.

## 2.17. *CardDriverActivity*

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к деятельности водителя (приложение 1С, требования 267, 268, 292, 293, 321 и 344).

```
CardDriverActivity ::= SEQUENCE {
    activityPointerOldestDayRecord    INTEGER(0.. CardActivityLengthRange-1),
    activityPointerNewestRecord       INTEGER(0.. CardActivityLengthRange-1),
    activityDailyRecords              OCTET STRING (SIZE(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 обновлён с целью отразить новое место хранения самой давней полной дневной записи, а указатель *activityPreviousRecordLength* этой (новой) самой давней полной дневной записи должен быть установлен на ноль.

## 2.18. *CardDrivingLicenceInformation*

Информация, записанная на карточке водителя, которая относится к данным о водительском удостоверении владельца карточки (приложение 1С, требования 259 и 284).

```
CardDrivingLicenceInformation ::= SEQUENCE {
    drivingLicenceIssuingAuthority      Name,
    drivingLicenceIssuingNation         NationNumeric,
    drivingLicenceNumber                IA5String(SIZE(16))
}
```

**drivingLicenceIssuingAuthority** – орган, ответственный за выдачу водительского удостоверения.

**drivingLicenceIssuingNation** – национальная принадлежность органа, выдавшего водительское удостоверение.

**drivingLicenceNumber** – номер водительского удостоверения.

## 2.19. *CardEventData*

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к событиям, связанным с владельцем карточки (приложение 1С, требования 260, 285, 318 и 341).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
    cardEventRecords                SET SIZE(NoOfEventsPerType) OF CardEventRecord
}
```

**CardEventData** – последовательность записей *cardEventRecords*, записанная в порядке возрастания значения элемента *EventFaultType* (за исключением записей, касающихся нарушения защиты, которые группируются в последнем массиве данных последовательности).

**cardEventRecords** – набор записей о событиях данного типа (или категория событий, имеющих отношение к попыткам нарушения защиты).

## 2.20. *CardEventRecord*

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к событию, связанному с владельцем карточки (приложение 1С, требования 261, 286, 318 и 341).

```
CardEventRecord ::= SEQUENCE {
    eventType                        EventFaultType,
    eventBeginTime                   TimeReal,
    eventEndTime                     TimeReal,
    eventVehicleRegistration          VehicleRegistrationIdentification
}
```

**eventType** – тип события.

**eventBeginTime** – дата и время начала события.

**eventEndTime** – дата и время завершения события.

**eventVehicleRegistration** – VRN и государство-член регистрации транспортного средства, к которому относится событие.

## 2.21. *CardFaultData*

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к неисправностям, связанным с владельцем карточки (приложение 1С, требования 263, 288, 318 и 341).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {  
    cardFaultRecords                               SET SIZE(NoOfFaultsPerType) OF CardFaultRecord  
}
```

**CardFaultData** – последовательность совокупности записей, отражающих неисправности записывающего оборудования, за которой следует совокупность записей, отражающих сбои в работе карточек.

**cardFaultRecords** – совокупность записей о неисправностях, сгруппированных по данной категории неисправностей (записывающего оборудования или карточки).

## 2.22. *CardFaultRecord*

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к неисправности, связанной с владельцем карточки (приложение 1С, требования 264, 289, 318 и 341).

```
CardFaultRecord ::= SEQUENCE {  
    faultType                               EventFaultType,  
    faultBeginTime                          TimeReal,  
    faultEndTime                            TimeReal,  
    faultVehicleRegistration                VehicleRegistrationIdentification  
}
```

**faultType** – тип неисправности.

**faultBeginTime** – дата и время начала неисправности.

**faultEndTime** – дата и время окончания неисправности.

**faultVehicleRegistration** – VRN и государство-член регистрации транспортного средства, к которому относится неисправность.



## 2.23. *CardIccIdentification*

Информация, записанная на карточке, которая относится к идентификации интегральной схемы карточки (ИС) (требование 248 приложения 1С).

```
CardIccIdentification ::= SEQUENCE {
    clockStop                OCTET STRING (SIZE(1)),
    cardExtendedSerialNumber ExtendedSerialNumber,
    cardApprovalNumber      CardApprovalNumber,
    cardPersonaliserID      ManufacturerCode,
    embedderIcAssemblerId   EmbedderIcAssemblerId,
    icIdentifier             OCTET STRING (SIZE(2))
}
```

**clockStop** – режим остановки часов, определённый в приложении 2.

**cardExtendedSerialNumber** – уникальный серийный номер карточки с ИС, как указано далее для типа данных ExtendedSerialNumber.

**cardApprovalNumber** – номер официального утверждения типа карточки.

**cardPersonaliserID** – идентификационные данные персонализатора карточки, закодированные как ManufacturerCode.

**embedderIcAssemblerId** предоставляет информацию об установщике/сборщике ИС.

**icIdentifier** – идентификатор ИС на карточке и производителя ИС, как указано в стандарте ISO/IEC 7816-6.

## 2.24. *CardIdentification*

Информация, записанная на карточке, которая имеет отношение к идентификационным данным карточки (приложение 1С, требования 255, 280, 310, 333, 359, 365, 371 и 377).

```
CardIdentification ::= SEQUENCE {
    cardIssuingMemberState  NationNumeric,
    cardNumber              CardNumber,
    cardIssuingAuthorityName Name,
    cardIssueDate           TimeReal,
    cardValidityBegin       TimeReal,
    cardExpiryDate          TimeReal
}
```

**cardIssuingMemberState** – код государства-члена, выдавшего карточку.

**cardNumber** – номер карточки.

**cardIssuingAuthorityName** – название органа, выдавшего карточку.

**cardIssueDate** – дата выдачи карточки нынешнему владельцу.

**cardValidityBegin** – первая дата действия карточки.

**cardExpiryDate** – дата истечения срока действия карточки.

## 2.25. *CardMACertificate*

Второе поколение:

Сертификат открытого ключа карточки для взаимной проверки подлинности с БУ. Структура данного сертификата представлена в приложении 11.

CardMACertificate ::= Certificate

## 2.26. *CardNumber*

Номер карточки в соответствии с определением g.

```
CardNumber ::= CHOICE {
  SEQUENCE {
    driverIdentification          IA5String(SIZE(14)),
    cardReplacementIndex        CardReplacementIndex,
    cardRenewalIndex            CardRenewalIndex
  },
  SEQUENCE {
    ownerIdentification          IA5String(SIZE(13)),
    cardConsecutiveIndex        CardConsecutiveIndex,
    cardReplacementIndex        CardReplacementIndex,
    cardRenewalIndex            CardRenewalIndex
  }
}
```

**driverIdentification** – уникальная идентификация водителя в государстве-члене.

**ownerIdentification** – уникальная идентификация предприятия или мастерской или контрольного органа в государстве-члене.

**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, контрольной карточки и карточки предприятия.

## 2.27. *CardPlaceDailyWorkPeriod*

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к местам, где начинаются и/или заканчиваются дневные периоды работы (приложение 1С, требования 272, 297, 325 и 348).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
  placePointerNewestRecord      INTEGER(0 .. NoOfCardPlaceRecords-1),
  placeRecords                  SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

**placePointerNewestRecord** – индекс последней обновлённой записи данных о месте.

**Присвоение значения:** Число, соответствующее числовому показателю записи данных о месте, которое начинается с 0 в случае первой регистрации записей, касающихся места, в структуре.

**placeRecords** – совокупность записей, содержащих информацию о введённых названиях мест.

## 2.28. *CardPrivateKey*

Первое поколение:

Закрытый ключ карточки.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

## 2.29. *CardPublicKey*

Открытый ключ карточки.

`CardPublicKey ::= PublicKey`

## 2.30. *CardRenewalIndex*

Индекс возобновления карточки (определение i).

`CardRenewalIndex ::= IA5String(SIZE(1))`

**Присвоение значения:** (см. главу VII данного приложения).

‘0’ Первый выпуск.

Порядок повышения: ‘0 , ... , 9 , A , ... , Z’

## 2.31. *CardReplacementIndex*

Индекс замены карточки (определение j).

`CardReplacementIndex ::= IA5String(SIZE(1))`

**Присвоение значения:** (см. главу VII данного приложения).

‘0’ Оригинальная карточка.

Порядок повышения: ‘0 , ... , 9 , A , ... , Z’

## 2.32. *CardSignCertificate*

Второе поколение:

Сертификат открытого ключа карточки для подписания. Структура данного сертификата представлена в приложении 11.

`CardSignCertificate ::= Certificate`

## 2.33. *CardSlotNumber*

Код, позволяющий проводить различие между двумя считывающими устройствами бортового устройства.

```
CardSlotNumber ::= INTEGER {
    driverSlot                (0),
    co-driverSlot             (1)
}
```

**Присвоение значения:** дополнительно не указывается.

## 2.34. *CardSlotsStatus*

Код, указывающий тип карточек, вставленных в два считывающих устройства бортового устройства.

CardSlotsStatus ::= OCTET STRING (SIZE(1))

**Присвоение значения – выровненный октет:** ‘ccccddd’В

‘cccc’В Идентификационные данные типа карточки, вставленной в считывающее устройство второго водителя,

‘ddd’В Идентификационные данные типа карточки, вставленной в считывающее устройство водителя,

со следующими идентификационными кодами:

‘0000’В карточка не вставлена,

‘0001’В вставлена карточка водителя,

‘0010’В вставлена карточка мастерской,

‘0011’В вставлена контрольная карточка,

‘0100’В вставлена карточка предприятия.

## 2.35. *CardSlotsStatusRecordArray*

Второе поколение:

CardSlotsStatus и метаданные, используемые в протоколе загрузки.

```
CardSlotsStatusRecordArray ::= SEQUENCE {  
    recordType          RecordType,  
    recordSize          INTEGER(1..65535),  
    noOfRecords         INTEGER(0..65535),  
    records             SET SIZE(noOfRecords) OF CardSlotsStatus  
}
```

**recordType** указывает на тип записи (CardSlotsStatus). **Присвоение значения:** см. RecordType

**recordSize** – размер CardSlotsStatus в байтах.

**noOfRecords** – число записей в массиве.

**records** – массив записей CardSlotsStatus.

## 2.36. *CardStructureVersion*

Код, указывающий на версию реализованной структуры на карточке тахографа.

CardStructureVersion ::= OCTET STRING (SIZE(2))

**Присвоение значения:** ‘aabb’H:

- ‘aa’H индекс изменений структуры.
  - ‘00’H для приложений первого поколения
  - ‘01’H для приложений второго поколения
  
- ‘bb’H индекс изменений, касающийся использования элементов данных, определённых в структуре, заданной стартовым байтом.
  - ‘00’H для данной версии приложений первого поколения
  - ‘00’H для данной версии приложений второго поколения

## 2.37. *CardVehicleRecord*

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к периоду пользования транспортным средством в течение календарного дня (приложение 1С, требования 269, 294, 322 и 345).

Первое поколение:

```
CardVehicleRecord ::= SEQUENCE {
    vehicleOdometerBegin           OdometerShort,
    vehicleOdometerEnd            OdometerShort,
    vehicleFirstUse                TimeReal,
    vehicleLastUse                 TimeReal,
    vehicleRegistration            VehicleRegistrationIdentification,
    vuDataBlockCounter            VuDataBlockCounter
}
```

**vehicleOdometerBegin** – показания одометра транспортного средства на начало периода эксплуатации транспортного средства.

**vehicleOdometerEnd** – показания одометра 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 регистрации транспортного средства.

**vuDataBlockCounter** – значение VuDataBlockCounter на момент последнего извлечения периода эксплуатации транспортного средства.

Второе поколение:

```
CardVehicleRecord ::= SEQUENCE {  
    vehicleOdometerBegin           OdometerShort,  
    vehicleOdometerEnd           OdometerShort,  
    vehicleFirstUse              TimeReal,  
    vehicleLastUse               TimeReal,  
    vehicleRegistration          VehicleRegistrationIdentification,  
    vuDataBlockCounter          VuDataBlockCounter,  
    vehicleIdentificationNumber  VehicleIdentificationNumber  
}
```

В дополнение к первому поколению, используется следующий элемент данных:

**VehicleIdentificationNumber** – идентификационный номер транспортного средства, относящийся ко всему транспортному средству.

## 2.38. *CardVehiclesUsed*

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к транспортным средствам, эксплуатируемым владельцем карточки (приложение 1С, требования 270, 295, 323 и 346).

```
CardVehiclesUsed ::= SEQUENCE {  
    vehiclePointerNewestRecord    INTEGER(0..NoOfCardVehicleRecords-1),  
    cardVehicleRecords           SET SIZE(NoOfCardVehicleRecords) OF CardVehicleRecord  
}
```

**vehiclePointerNewestRecord** – индекс последней обновлённой записи, касающейся транспортного средства.

**Присвоение значения:** Число, соответствующее числовому показателю записи данных о транспортном средстве, которое начинается с 0 в случае первой регистрации регистрации записей, касающихся транспортного средства, в структуре.

**cardVehicleRecords** – совокупность записей, содержащих информацию об использованных транспортных средствах.

## 2.39. CardVehicleUnitRecord

Второе поколение:

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к используемым бортовым устройствам (приложение 1С, требования 303 и 351).

```
CardVehicleUnitRecord ::= SEQUENCE {
    timeStamp                TimeReal,
    manufacturerCode         ManufacturerCode,
    deviceID                 INTEGER(0..255),
    vuSoftwareVersion        VuSoftwareVersion
}
```

**timeStamp** – начало периода использования бортового устройства (т.е. первый ввод карточки в бортовое устройство в течение рассматриваемого периода).

**manufacturerCode** идентифицирует производителя бортового устройства.

**deviceID** идентифицирует тип бортового устройства производителя. Значение зависит от производителя.

**vuSoftwareVersion** – номер версии программного обеспечения бортового устройства.

## 2.40. CardVehicleUnitsUsed

Второе поколение:

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к бортовым устройствам, используемым владельцем карточки (приложение 1С, требования 306 и 352).

```
CardVehicleUnitsUsed := SEQUENCE {
    vehicleUnitPointerNewestRecord    INTEGER(0..NoOfCardVehicleUnitRecords-1),
    cardVehicleUnitRecords            SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

**vehicleUnitPointerNewestRecord** – индекс последней обновлённой записи, касающейся бортового устройства.

**Присвоение значения:** Число, соответствующее числовому показателю записи данных о бортовом устройстве, которое начинается с 0 в случае первой регистрации регистрации записей, касающихся бортового устройства, в структуре.

**cardVehicleUnitRecords** – совокупность записей, содержащих информацию об использованных бортовых устройствах.

## 2.41. Certificate

Сертификат открытого ключа, выданный сертификационным органом.

Первое поколение:

```
Certificate ::= OCTET STRING (SIZE(194))
```

**Присвоение значения:** цифровая подпись с частичным восстановлением CertificateContent в соответствии с общими механизмами защиты, описанными в приложении 11: Подпись (128 байт) || Остаток открытого ключа (58 байт) || Код сертификационного органа (8 байт).

Второе поколение:

Certificate ::= OCTET STRING (SIZE(204..341))

**Присвоение значения:** См. приложение 11

## 2.42. CertificateContent

Первое поколение:

(Ясное) содержание сертификата открытого ключа в соответствии с общими механизмами защиты, изложенными в приложении 11.

```
CertificateContent ::= SEQUENCE {
    certificateProfileIdentifier          INTEGER(0..255),
    certificationAuthorityReference      KeyIdentifier,
    certificateHolderAuthorisation       CertificateHolderAuthorisation,
    certificateEndOfValidity             TimeReal,
    certificateHolderReference           KeyIdentifier,
    publicKey                            PublicKey
}
```

**certificateProfileIdentifier** — версия соответствующего сертификата.

**Присвоение значения:** '01h' для данной версии.

**certificationAuthorityReference** идентифицирует сертификационный орган, выдавший сертификат. 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** — идентификатор держателя сертификата. Также включает в себя ссылку на его открытый ключ.

**publicKey** — открытый ключ, подтверждающий данный сертификат.

## 2.43. CertificateHolderAuthorisation

Идентификатор прав держателя сертификата.

```
CertificateHolderAuthorisation ::= SEQUENCE {
    tachographApplicationID            OCTET STRING(SIZE(6))
    equipmentType                       EquipmentType
}
```

Первое поколение:

**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, для которого предназначен сертификат.

**Присвоение значения:** в соответствии с типом данных EquipmentType. **0**, если это сертификат государства-члена.

Второе поколение:



**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 сертификат.

**Присвоение значения:** в соответствии с типом данных EquipmentType.

## 2.44. CertificateRequestID

Уникальный идентификатор заявки на получение сертификата. Также может использоваться в качестве идентификатора открытого ключа бортового устройства, если серийный номер бортового устройства, для которого предназначен данный ключ, в момент создания сертификата неизвестен.

```
CertificateRequestID ::= SEQUENCE{
    requestSerialNumber          INTEGER(0..232-1),
    requestMonthYear            BCDString(SIZE(2)),
    crIdentifier                 OCTET STRING(SIZE(1)),
    manufacturerCode            ManufacturerCode
}
```

**requestSerialNumber** – серийный номер заявки на сертификат, уникальный для данного производителя и относящийся к месяцу, указанному ниже.

**requestMonthYear** —идентификатор месяца и года заявки на сертификат.

**Присвоение значения:** код BCD месяца (две цифры) и года (две последние цифры).

**crIdentifier** —идентификатор, позволяющий проводить различие между заявкой на сертификат и расширенным серийным номером.

**Присвоение значения:** 'FFh'.

**manufacturerCode** – цифровой код производителя, подающего заявку на сертификат.

## 2.45. CertificationAuthorityKID

Идентификатор открытого ключа сертификационного органа (государства-члена или европейского сертификационного органа).

```
CertificationAuthorityKID ::= SEQUENCE{
    nationNumeric                NationNumeric,
    nationAlpha                  NationAlpha,
    keySerialNumber              INTEGER(0..255),
    additionalInfo                OCTET STRING(SIZE(2)),
    caIdentifier                  OCTET STRING(SIZE(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 (специально для сертификационного органа).

**caIdentifier** –идентификатор, позволяющий проводить различие между идентификатором ключа сертификационного органа и другими идентификаторами ключа.

**Присвоение значения:** ‘01h’.

## 2.46. *CompanyActivityData*

Информация, записанная на карточке предприятия, которая относится к действиям, проводимым с карточкой (приложение 1С, требования 373 и 379).

```
CompanyActivityData ::= SEQUENCE {
  companyPointerNewestRecord      INTEGER(0..NoOfCompanyActivityRecords-1),
  companyActivityRecords          SET SIZE(NoOfCompanyActivityRecords) OF
  companyActivityRecord           SEQUENCE {
    companyActivityType           CompanyActivityType,
    companyActivityTime           TimeReal,
    cardNumberInformation         FullCardNumber,
    vehicleRegistrationInformation VehicleRegistrationIdentification,
    downloadPeriodBegin          TimeReal,
    downloadPeriodEnd            TimeReal
  }
}
```

**companyPointerNewestRecord** –индекс последней обновлённой записи companyActivityRecord.

**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.

**companyActivityRecords** – совокупность всех записей действий, произведённых предприятием.

**companyActivityRecord** – последовательность информации, относящейся к одному действию, произведённому предприятием.

**companyActivityType** – тип действия предприятия.

**companyActivityTime** – дата и время действия предприятия.

**cardNumberInformation** – номер карточки и название государства-члена, выдавшего карточку с загруженными с неё данными, если применимо.

**vehicleRegistrationInformation** – VRN и государство-член регистрации транспортного средства, в отношении которого данные загружены, заблокированы или разблокированы.

**downloadPeriodBegin** и **downloadPeriodEnd** – период, за который в соответствующих случаях загружены данные с БУ.

## 2.47. *CompanyActivityType*

Код указывающей на действия, произведённые предприятием с использованием карточки предприятия.

```
CompanyActivityType ::= INTEGER {
  card downloading           (1),
  VU downloading           (2),
  VU lock-in                (3),
  VU lock-out               (4)
}
```

## 2.48. *CompanyCardApplicationIdentification*

Информация, записанная на карточке предприятия, которая относится к идентификации приложения карточки (приложение 1С, требования 369 и 375).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
  typeOfTachographCardId    EquipmentType,
  cardStructureVersion       CardStructureVersion,
  noOfCompanyActivityRecords NoOfCompanyActivityRecords
}
```

**typeOfTachographCardId** уточняет реализованный тип карточки.

**cardStructureVersion** уточняет версию структуры, реализованной на карточке.

**noOfCompanyActivityRecords** – число записей о действиях предприятия, которые могут храниться на карточке.

## 2.49. *CompanyCardHolderIdentification*

Информация, записанная на карточке предприятия, которая относится к идентификации владельца карточки (приложение 1С, требования 372 и 378).

```
CompanyCardHolderIdentification ::= SEQUENCE {
  companyName                Name,
  companyAddress              Address,
  cardHolderPreferredLanguage Language
}
```

**companyName** – название предприятия владельца.

**companyAddress** – адрес предприятия владельца.

**cardHolderPreferredLanguage** – предпочитаемый язык владельца карточки.

## 2.50. *ControlCardApplicationIdentification*

Информация, записанная на контрольной карточке, которая относится к идентификации приложения карточки (приложение 1С, требования 357 и 363).

```
ControlCardApplicationIdentification ::= SEQUENCE {
  typeOfTachographCardId    EquipmentType,
  cardStructureVersion       CardStructureVersion,
  noOfControlActivityRecords NoOfControlActivityRecords
}
```

**typeOfTachographCardId** уточняет реализованный тип карточки.

**cardStructureVersion** уточняет версию структуры, реализованной на карточке.

**noOfControlActivityRecords** – число записей о контрольных действиях, которые могут храниться на карточке.

## 2.51. ControlCardControlActivityData

Информация, записанная на контрольной карточке, которая относится к контрольным действиям, проводимым с карточкой (приложение 1С, требования 361 и 367).

```
ControlCardControlActivityData ::= SEQUENCE {
  controlPointerNewestRecord      INTEGER(0.. NoOfControlActivityRecords-1),
  controlActivityRecords          SET SIZE(NoOfControlActivityRecords) OF
  controlActivityRecord           SEQUENCE {
    controlType                   ControlType,
    controlTime                   TimeReal,
    controlledCardNumber          FullCardNumber,
    controlledVehicleRegistration VehicleRegistrationIdentification,
    controlDownloadPeriodBegin    TimeReal,
    controlDownloadPeriodEnd      TimeReal
  }
}
```

**controlPointerNewestRecord** —индекс последней обновлённой записи, касающейся контрольных действий.

**Присвоение значения:** Число, соответствующее числовому показателю записи данных о контрольной деятельности, которое начинается с 0 в случае первой регистрации записей, касающихся контрольной деятельности, в структуре.

**controlActivityRecords** – совокупность всех записей контрольных действий.

**controlActivityRecord** – последовательность информации, относящейся к одному контрольному действию.

**controlType** – тип контроля.

**controlTime** – дата и время контроля.

**controlledCardNumber** – номер карточки и название государства-члена, выдавшего контролируемую карточку.

**controlledVehicleRegistration** – VRN и государство-член регистрации транспортного средства, к которому относится контроль.

**controlDownloadPeriodBegin** и **controlDownloadPeriodEnd** – период, за который впоследствии загружаются данные.

## 2.52. ControlCardHolderIdentification

Информация, записанная на контрольной карточке, которая относится к идентификации владельца карточки (приложение 1С, требования 360 и 366).

```
ControlCardHolderIdentification ::= SEQUENCE {
  controlBodyName      Name,
  controlBodyAddress   Address,
  cardHolderName       HolderName,
  cardHolderPreferredLanguage Language
}
```

**controlBodyName** – название контрольного органа владельца карточки.

**controlBodyAddress** – адрес контрольного органа владельца карточки.

**cardHolderName** – фамилия и имя (имена) владельца контрольной карточки.

**cardHolderPreferredLanguage** – предпочитаемый язык владельца карточки.

## 2.53. ControlType

Код, указывающий на действия, проведённые в ходе проверки. Данный тип данных связан с требованиями 126, 274, 299, 327 и 350 в приложении 1С.

ControlType ::= OCTET STRING (SIZE(1))

Первое поколение:

**Присвоение значения** —выровненный октет: 'c'V (8 бит)

'с'В загрузка данных карточки:

'0'В: во время данной контрольной операции загрузка данных с карточки не произведена,  
'1'В: во время данной контрольной операции загрузка данных с карточки произведена

'v'В загрузка данных с БУ:

'0'В: во время данной контрольной операции загрузка данных с БУ не произведена,  
'1'В: во время данной контрольной операции загрузка данных с БУ произведена

'p'В печать:

'0'В: во время данной контрольной операции печать не произведена,  
'1'В: во время данной контрольной операции печать произведена

'd'В отображение:

'0'В: во время данной контрольной операции данные на дисплей не выводились,  
'1'В: во время данной контрольной операции данные на дисплей выводились

'xxxx'В не применяется.

Второе поколение:

**Присвоение значения** —выровненный октет: 'c'Vdexxx'В (8 бит)

'с'В загрузка данных карточки:

'0'В: во время данной контрольной операции загрузка данных с карточки не произведена,  
'1'В: во время данной контрольной операции загрузка данных с карточки произведена

'v'В загрузка данных с БУ:

'0'В: во время данной контрольной операции загрузка данных с БУ не произведена,  
'1'В: во время данной контрольной операции загрузка данных с БУ произведена

'p'В печать:

'0'В: во время данной контрольной операции печать не произведена,  
'1'В: во время данной контрольной операции печать произведена

'd'В отображение:

'0'В: во время данной контрольной операции данные на дисплей не выводились,  
'1'В: во время данной контрольной операции данные на дисплей выводились

'e'В придорожная проверка калибровки:

'0'В: во время данной контрольной операции параметры калибровки не проверялись,  
'1'В: во время данной контрольной операции параметры калибровки проверялись

'xxx'BRFU.

## 2.54. CurrentDateTime

Текущие дата и время записывающего оборудования.

CurrentDateTime ::= TimeReal

**Присвоение значения:** дополнительно не указывается.

## 2.55. *CurrentDateTimeRecordArray*

Второе поколение:

Текущие дата и время и метаданные, используемые в протоколе загрузки.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize         INTEGER(1..65535),
    noOfRecords        INTEGER(0..65535),
    records            SET SIZE(noOfRecords) OF CurrentDateTime
}
```

**recordType** указывает на тип записи (CurrentDateTime). **Присвоение значения:** см. RecordType

**recordSize** – размер CurrentDateTime в байтах.

**noOfRecords** – число записей в массиве.

**records** – массив записей текущих даты и времени.

## 2.56. *DailyPresenceCounter*

Показания счетчика, записанные на карточке водителя или предприятия, которые увеличиваются на единицу за каждый календарный день, в течение которого в БУ была вставлена карточка. Данный тип данных связан с требованиями 266, 299, 320 и 343 в приложении 1С.

DailyPresenceCounter ::= BCDString(SIZE(2))

**Присвоение значения:** порядковый номер с максимальным значением = 9 999, который снова начинается с 0. В момент первой выдачи номера карточки это число устанавливается на 0.

## 2.57. *Datef*

Дата, выраженная в числовом формате, которая может сразу выводиться на печать.

```
Datef ::= SEQUENCE {
    year          BCDString(SIZE(2)),
    month        BCDString(SIZE(1)),
    day          BCDString(SIZE(1))
}
```

**Присвоение значения:**

uuuu	год
mm	месяц
dd	день
'00000000'H	явно выражает отсутствие даты.

## 2.58. *DateOfDayDownloaded*

Второе поколение:

Дата и время загрузки.

DateOfDayDownloaded ::= TimeReal

**Присвоение значения:** дополнительно не указывается.

## 2.59. *DateOfDayDownloadedRecordArray*

Второе поколение:

Дата и время загрузки и метаданные, используемые в протоколе загрузки.

```
DateOfDayDownloadedRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize          INTEGER(1..65535),
    noOfRecords         INTEGER(0..65535),
    records             SET SIZE(noOfRecords) OF DateOfDayDownloaded
}
```

**recordType** указывает на тип записи (DateOfDayDownloaded). **Присвоение значения:** см. RecordType

**recordSize** – размер CurrentDateTime в байтах.

**noOfRecords** – число записей в массиве.

**records** – массив записей даты и времени загрузки.

## 2.60. *Distance*

Пройденное расстояние (результат расчёта разницы между двумя показаниями одометра транспортного средства в километрах).

Distance ::= INTEGER(0..216-1)

**Присвоение значения:** Двоичное значение без знака. Значение в км в рабочем диапазоне от 0 до 9 999 км.

## 2.61. *DriverCardApplicationIdentification*

Информация, записанная на карточке водителя, которая относится к идентификации приложения карточки (приложение 1С, требования 253 и 278).

Первое поколение:

```
DriverCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId      EquipmentType,
    cardStructureVersion         CardStructureVersion,
    noOfEventsPerType            NoOfEventsPerType,
    noOfFaultsPerType           NoOfFaultsPerType,
    activityStructureLength       CardActivityLengthRange,
    noOfCardVehicleRecords       NoOfCardVehicleRecords,
    noOfCardPlaceRecords         NoOfCardPlaceRecords
}
```

**typeOfTachographCardId** уточняет реализованный 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 транспортном средстве, которые могут храниться на карточке.

**noOfCardPlaceRecords** – число записей о местах, которые могут храниться на карточке.

Второе поколение:

```
DriverCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId           EquipmentType,
    cardStructureVersion              CardStructureVersion,
    noOfEventsPerType                 NoOfEventsPerType,
    noOfFaultsPerType                 NoOfFaultsPerType,
    activityStructureLength            CardActivityLengthRange,
    noOfCardVehicleRecords            NoOfCardVehicleRecords,
    noOfCardPlaceRecords              NoOfCardPlaceRecords,
    noOfGNSSCDRecords                NoOfGNSSCDRecords,
    noOfSpecificConditionRecords      NoOfSpecificConditionRecords
}
```

В дополнение к первому поколению, используются следующие элементы данных:

**noOfGNSSCDRecords** – число записей о непрерывном времени управления по ГНСС, которые могут храниться на карточке.

**noOfSpecificConditionRecords** – число записей об особых условиях, которые могут храниться на карточке.

## 2.62. *DriverCardHolderIdentification*

Информация, записанная на карточке водителя, которая относится к идентификации владельца карточки (приложение 1С, требования 256 и 281).

```
DriverCardHolderIdentification ::= SEQUENCE {
    cardHolderName                    HolderName,
    cardHolderBirthDate               Datef,
    cardHolderPreferredLanguage        Language
}
```

**cardHolderName** – фамилия и имя (имена) владельца карточки водителя.

**cardHolderBirthDate** – дата рождения владельца карточки водителя.

**cardHolderPreferredLanguage** – предпочитаемый язык владельца карточки.

## 2.63. *DSRCSecurityData*

Второе поколение:

Простая текстовая информация и MAC, передаваемые через DSRC из тахографа в устройство дистанционного опроса (RI); более подробно см. приложение 11, часть Б, глава 13.



```

DSRCSecurityData ::= SEQUENCE {
    tagLenthPlainText          OCTET STRING(SIZE(2)),
    currentDateTime            CurrentDateTime,
    counter                    INTEGER(0..224-1),
    vuSerialNumber             VuSerialNumber,
    dSRCKMVersionNumber       INTEGER(SIZE(1)),
    tagLengthMac               OCTET STRING(SIZE(2)),
    mac                        MAC
}

```

Б, 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 Б, глава 13).

**mac** —это значение MAC, вычисленное при помощи сообщения RTM (см. приложение 11, часть Б, глава 13).

## 2.64. *EGFCertificate*

Второе поколение:

Сертификат открытого ключа внешнего устройства ГНСС для взаимной проверки подлинности с БУ. Структура данного сертификата представлена в приложении 11.

EGFCertificate ::= Certificate

## 2.65. *EmbedderIcAssemblerId*

Информация об установщике ИС.

```

EmbedderIcAssemblerId ::= SEQUENCE{
    countryCode                IA5String(SIZE(2)),
    moduleEmbedder             BCDSString(SIZE(2)),
    manufacturerInformation    OCTET STRING(SIZE(1))
}

```

**countryCode** —двухбуквенный код страны установщика модуля в соответствии с ISO 3166.

**moduleEmbedder** —идентификатор установщика модуля.

**manufacturerInformation** —для внутреннего пользования производителя.

## 2.66. *EntryTypeDailyWorkPeriod*

Код, позволяющий провести различие между началом и концом ввода данных о месте дневного периода работы и условиями ввода.

Первое поколение

```
EntryTypeDailyWorkPeriod ::= INTEGER {
    Begin,    related time = card insertion time or time of entry      (0),
    End,      related time = card withdrawal time or time of entry    (1),
    Begin,    related time manually entered (start time)              (2),
    End,      related time manually entered (end of work period)      (3),
    Begin,    related time assumed by VU                              (4),
    End,      related time assumed by VU                              (5)
}
```

**Присвоение значения:** в соответствии с ISO/IEC8824-1.

Второе поколение

```
EntryTypeDailyWorkPeriod ::= INTEGER {
    Begin,    related time = card insertion time or time of entry      (0),
    End,      related time = card withdrawal time or time of entry    (1),
    Begin,    related time manually entered (start time)              (2),
    End,      related time manually entered (end of work period)      (3),
    Begin,    related time assumed by VU                              (4),
    End,      related time assumed by VU                              (5),
    Begin,    related time based on GNSS data                        (6),
    End,      related time based on GNSS data                        (7)
}
```

**Присвоение значения:** в соответствии с ISO/IEC8824-1.

## 2.67. *EquipmentType*

Код, позволяющий провести различие между различными типами оборудования в связи с использованием тахографа.

```
EquipmentType ::= INTEGER(0..255)
```

Первое поколение:

```
--Reserved                (0),
--Driver Card              (1),
--Workshop Card            (2),
--Control Card             (3),
--Company Card             (4),
--Manufacturing Card       (5),
--Vehicle Unit             (6),
--Motion Sensor            (7),
--RFU                      (8..255)
```

**Присвоение значения:** В соответствии со стандартом ISO/IEC8824-1.

Значение 0 зарезервировано для целей указания государства-члена или Европы в поле данных СНА сертификатов.

Второе поколение:

Используются такие же значения, как и для первого поколения, со следующими дополнениями:

--GNSS Facility	(8),
--Remote Communication Module	(9),
--ITS interface module	(10),
--Plaque	(11), -- may be used in SealRecord
--M1/N1 Adapter	(12), -- may be used in SealRecord
--European Root CA (ERCA)	(13),
--Member State CA (MSCA)	(14),
--External GNSS connection	(15), -- may be used in SealRecord
--Unused	(16), -- used in SealDataVu
--RFU	(17..255)

Примечание: Значения второго поколения в отношении таблички, адаптера и внешнего соединения ГНСС, а также значения первого поколения в отношении бортового устройства и датчика движения могут использоваться в SealRecord, т.е. если применимы.

## 2.68. *EuropeanPublicKey*

Первое поколение:

Европейский открытый ключ.

EuropeanPublicKey ::= PublicKey

## 2.69. *EventFaultRecordPurpose*

Код, указывающий на причину регистрации события или неисправности.

EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))

### Присвоение значения:

'00' H	одно из 10 недавних (последних) событий или неисправностей
'01' H	самое продолжительное событие за один из последних 10 дней данного случая
'02' H	одно из 5 самых продолжительных событий за последние 365 дней
'03' H	последнее событие за один из последних 10 дней данного случая
'04' H	самое серьезное событие за один из последних 10 дней данного случая
'05' H	одно из 5 самых серьезных событий за последние 365 дней
'06' H	первое событие или неисправность, наступившие после последней калибровки
'07' H	текущее/продолжающееся событие или неисправность
'08' H – '7F' H	RFU
'80' H – 'FF' H	относится конкретно к производителю

## 2.70. *EventFaultType*

Код, отображающий событие или неисправность.

EventFaultType ::= OCTET STRING (SIZE(1))

### Присвоение значения:

Первое поколение:

\0x' H	общие события,
\00' H	дополнительно не уточняется,
\01' H	ввод недействительной карточки,
\02' H	несовместимость карточек,
\03' H	совпадение 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	ошибочные данные о движении,
\0A' H	противоречивые данные о движении транспортного средства,
\0B' H – \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	несанкционированное изменение датчика движения,
\14' H	ошибка при проверке целостности введённых данных карточки
\15' H	ошибка при проверке целостности сохранённых пользовательских данных,
\16' H	ошибка при внутренней передаче данных,
\17' H	несанкционированное открытие корпуса,
\18' H	саботаж аппаратного обеспечения,
\19' H – \1F' H	RFU,
\2x' H	события, связанные с попыткой нарушения защиты датчика,
\20' H	дополнительно не уточняется,
\21' H	сбой в аутентификации,
\22' H	ошибка при проверке целостности сохранённых данных,
\23' H	ошибка при внутренней передаче данных,
\24' H	несанкционированное открытие корпуса,
\25' H	саботаж аппаратного обеспечения,
\26' H – \2F' H	RFU,
\3x' H	неисправность записывающего оборудования,
\30' H	дополнительно не уточняется,
\31' H	внутренние неполадки в БУ,
\32' H	неисправность принтера,
\33' H	неисправность дисплея,
\34' H	неисправность при загрузке,
\35' H	неисправность датчика,
\36' H – \3F' H	RFU,
\4x' H	неисправности карточки,
\40' H	дополнительно не уточняется,

\41' H - \4F' H	RFU,
\50' H - \7F' H	RFU,
\80' H - \FF' H	относится конкретно к производителю.

Второе поколение:

Используются такие же значения, как и для первого поколения, со следующими дополнениями:

\0B' H	нестыковка во времени (ГНСС и внутренние часы БУ),
\0C' - \0F' H	RFU,
\5x' H	неисправности, связанные с ГНСС,
\50' H	дополнительно не уточняется,
\51' H	внутренняя неисправность приёмника ГНСС,
\52' H	внешняя неисправность приёмника ГНСС,
\53' H	неисправность внешней связи ГНСС,
\54' H	отсутствие данных ГНСС о местоположении,
\55' H	обнаружение взлома ГНСС,
\56' H	истёкший срок действия сертификата внешнего устройства ГНСС,
\57' H - \5F' H	RFU,
\6x' H	неисправности, связанные с модулем удалённой связи,
\60' H	дополнительно не уточняется,
\61' H	неисправность модуля удалённой связи,
\62' H	неисправность связи модуля удалённой связи,
\63' H - \6F' H	RFU,
\7x' H	неисправности интерфейса ИТС,
\70' H	дополнительно не уточняется,
\71' H - \7F' H	RFU.

## 2.71. *ExtendedSealIdentifier*

Второе поколение:

Расширенный идентификатор пломбы для уникальной идентификации пломбы (приложение 1С, требование 401).

```
ExtendedSealIdentifier ::= SEQUENCE{
    manufacturerCode      OCTET STRING (SIZE(2)),
    sealIdentifier        OCTET STRING (SIZE(6))
}
```

**manufacturerCode** – код производителя пломбы.

**sealIdentifier** – идентификатор пломбы, уникальный для производителя.

## 2.72. *ExtendedSerialNumber*

Уникальная идентификация оборудования. Она может использоваться в качестве идентификатора открытого ключа оборудования.

Первое поколение:

```
ExtendedSerialNumber ::= SEQUENCE{
    serialNumber          INTEGER(0..232-1),
    monthYear            BCDSString(SIZE(2)),
    type                 OCTET STRING(SIZE(1)),
    manufacturerCode     ManufacturerCode
}
```

**serialNumber** – серийный номер оборудования, уникальный для данного производителя, 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:** связано с конкретным производителем, с зарезервированным значением ‘FFh’.

**manufacturerCode** – цифровой код идентификации производителя оборудования утверждённого типа.

Второе поколение:

```
ExtendedSerialNumber ::= SEQUENCE{
    serialNumber          INTEGER(0..232-1),
    monthYear            BCDSString(SIZE(2)),
    type                 EquipmentType,
    manufacturerCode     ManufacturerCode
}
```

**serialNumber** – см. первое поколение

**monthYear** – см. первое поколение

**type** указывает тип оборудования

**manufacturerCode** – см. первое поколение.

## 2.73. FullCardNumber

Код, полностью идентифицирующий карточку тахографа.

```
FullCardNumber ::= SEQUENCE {
    cardType                               EquipmentType,
    cardIssuingMemberState                 NationNumeric,
    cardNumber                             CardNumber
}
```

**cardType** – тип карточки тахографа.

**cardIssuingMemberState** – код государства-члена, выдавшего карточку.

**cardNumber** – номер карточки.

## 2.74. FullCardNumberAndGeneration

Второе поколение:

Код, полностью идентифицирующий карточку тахографа и её поколение.

```
FullCardNumberAndGeneration ::= SEQUENCE {
    fullCardNumber                         FullCardNumber,
    generation                             Generation
}
```

**fullcardNumber** идентифицирует карточку тахографа.

**generation** указывает на поколение используемой карточки тахографа.

## 2.75. Generation

Второе поколение:

Указывает на поколение используемого тахографа.

Generation ::= INTEGER(0..255)

**Присвоение значения:**

'00'H	RFU
'01'H	первое поколение
'02'H	второе поколение
'03'H .. 'FF'H	RFU

## 2.76. GeoCoordinates

Второе поколение:

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 и минуты  $MM.M$ .

```
GeoCoordinates ::= SEQUENCE {
    latitude          INTEGER(-90000..90001),
    longitude        INTEGER(-180000..180001)
}
```

**latitude** кодируется как показатель (коэффициент 10) выражения  $\pm DDMM.M$ .

**longitude** кодируется как показатель (коэффициент 10) выражения  $\pm DDDMM.M$ .

## 2.77. GNSSAccuracy

Второе поколение:

Точность данных ГНСС о местоположении (определение ее). Эта точность кодируется как целое число и является показателем (коэффициент 10) значения X.Y из строки GSA NMEA.

```
GNSSAccuracy ::= INTEGER(1..100)
```

## 2.78. GNSSContinuousDriving

Второе поколение:

Информация, записанная на карточке водителя или мастерской, которая относится к местоположению транспортного средства по ГНСС, если непрерывное время управления водителем достигает значения, кратного трём часам (приложение 1С, требования 306 и 354).

```
GNSSContinuousDriving ::= SEQUENCE {
    gnssCDPointerNewestRecord    INTEGER(0..NoOfGNSSCDRecords -1),
    gnssContinuousDrivingRecords SET SIZE(NoOfGNSSCDRecords) OF
                                GNSSContinuousDrivingRecord
}
```

**gnssCDPointerNewestRecord** – индекс последней обновлённой записи ГНСС, касающейся непрерывного управления.

**Присвоение значения:** Число, соответствующее числовому показателю записи данных ГНСС о непрерывном управлении, которое начинается с 0 в случае первой регистрации регистрации записей ГНСС, касающихся непрерывного управления, в структуре.

**gnssContinuousDrivingRecords** – массив записей, содержащих дату и время, когда непрерывное управление достигает значения, кратного трём часам, и информацию о местоположении транспортного средства.

## 2.79. GNSSContinuousDrivingRecord

Второе поколение:

Информация, записанная на карточке водителя или мастерской, которая относится к местоположению транспортного средства по ГНСС, если непрерывное время управления водителем достигает значения, кратного трём часам (приложение 1С, требования 305 и 353).



```
GNSSContinuousDrivingRecord ::= SEQUENCE {
    timeStamp                TimeReal,
    gnssPlaceRecord         GNSSPlaceRecord
}
```

**timeStamp** – дата и время, когда непрерывное время управления владельцем карточки достигает значения, кратного трём часам.

**gnssPlaceRecord** содержит информацию, связанную с местоположением транспортного средства.

## 2.80. *GNSSPlaceRecord*

Второе поколение:

Информация, которая имеет отношение к местоположению транспортного средства по ГНСС (приложение 1С, требования 108, 109, 110, 296, 305, 347 и 353).

```
GNSSPlaceRecord ::= SEQUENCE {
    timeStamp                TimeReal,
    gnssAccuracy            GNSSAccuracy,
    geoCoordinates          GeoCoordinates
}
```

**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*

Показания одометра транспортного средства. общее расстояние, пройденное транспортным средством за период его эксплуатации.

HighResOdometer ::= INTEGER(0..2<sup>32</sup>-1)

**Присвоение значения:** Двоичное значение без знака. Значение в 1/200 км в рабочем диапазоне от 0 до 21 055 406 км.

## 2.82. *HighResTripDistance*

Расстояние, пройденное за весь или часть рейса.

HighResTripDistance ::= INTEGER(0..2<sup>32</sup>-1)

**Присвоение значения:** Двоичное значение без знака. Значение в 1/200 км в рабочем диапазоне от 0 до 21 055 406 км.

## 2.83. *HolderName*

Фамилия и имя (имена) владельца карточки.

```
HolderName ::= SEQUENCE {
    holderSurname            Name,
    holderFirstNames        Name
}
```

**holderSurname** – фамилия владельца. Фамилия не включает в себя обращение.

**Присвоение значения:** если карточка не именная, позиция holderSurname содержит ту же информацию, что и companyName или workshopName, или controlBodyName.

**holderFirstNames** – имя (имена) и инициалы владельца.

## 2.84. *InternalGNSSReceiver*

Второе поколение:

Информация о том, является ли приёмник ГНСС внешним или внутренним устройством бортового устройства. True – приёмник ГНСС встроен в БУ. False – приёмник ГНСС является внешним устройством.

InternalGNSSReceiver ::= BOOLEAN

## 2.85. *K-ConstantOfRecordingEquipment*

Постоянная величина записывающего оборудования (определение m).

K-ConstantOfRecordingEquipment ::= INTEGER(0..2<sup>16</sup>-1)

**Присвоение значения:** импульсы на километр в рабочем диапазоне от 0 до 64 255 имп./км.

## 2.86. *KeyIdentifier*

Уникальный идентификатор открытого ключа, используемого для назначения и выбора ключа. Также идентифицирует владельца ключа.

```
KeyIdentifier ::= CHOICE {
    extendedSerialNumber          ExtendedSerialNumber,
    certificateRequestID          CertificateRequestID,
    certificationAuthorityKID     CertificationAuthorityKID
}
```

Первый вариант выбора позволяет назначить открытый ключ бортового устройства или карточки тахографа.

Второй вариант выбора позволяет назначить открытый ключ бортового устройства (если в момент создания сертификата серийный номер бортового устройства неизвестен).

Третий вариант выбора позволяет назначить открытый ключ государства-члена.

## 2.87. *kMWCKey*

Второе поколение:

Ключ AES и связанная с ним версия ключа используются для соединения БУ и датчика движения. Более подробно см. приложение 11.

```
kMWCKey ::= SEQUENCE {
    kMWCKey          AESKey,
    keyVersion       INTEGER (SIZE(1))
}
```

**kMWCKey** – длина ключа AES, соединённого с ключом, используемым для соединения БУ и датчика движения.

**keyVersion** обозначает основную версию ключа AES.

## 2.88. *Language*

Код, идентифицирующий язык.

Language ::= IA5String(SIZE(2))

**Присвоение значения:** код в виде двух строчных букв в соответствии со стандартом ISO 639.

## 2.89. *LastCardDownload*

Дата и время, записанные на карточке водителя, последней загрузки данных с карточки (для иных целей, кроме контроля) (приложение 1С, требования 257 и 282). Эта дата может обновляться БУ или любым считывающим устройством.

LastCardDownload ::= TimeReal

**Присвоение значения:** дополнительно не указывается.

## 2.90. *LinkCertificate*

Второе поколение:

Сертификат связи между парами ключей European Root CA.

LinkCertificate ::= Certificate

## 2.91. *L-TyreCircumference*

Фактическая окружность шин колёс (определение u).

L-TyreCircumference ::= INTEGER(0.. 2<sup>16</sup>-1)

**Присвоение значения:** двоичное значение без знака; значение в 1/8 мм в рабочем диапазоне от 0 до 8 031 мм.

## 2.92. *MAC*

Второе поколение:

криптографическая контрольная сумма длиной 8, 12 или 16 байтов, соответствующая наборам шифров, представленным в приложении 11.

```
MAC ::= CHOICE {
    mac8                OCTET STRING (SIZE(8)),
    mac12               OCTET STRING (SIZE(12)),
    mac16               OCTET STRING (SIZE(12))
}
```

## 2.93. *ManualInputFlag*

Код, позволяющий определить, ввёл ли владелец карточки данные о деятельности водителя вручную в момент ввода карточки или нет (приложение 1В, требование 081 и приложение 1С, требование 102).

```
ManualInputFlag ::= INTEGER {
    noEntry              (0)
    manualEntries       (1)
}
```

**Присвоение значения:** дополнительно не указывается.

## 2.94. *ManufacturerCode*

Код идентификации производителя оборудования утверждённого типа.

ManufacturerCode ::= INTEGER(0..255)

Лаборатория, уполномоченная проводить испытания эксплуатационной совместимости, составляет и публикует перечень кодов производителей на своём веб-сайте (приложение 1С, требование 454).

ManufacturerCodes временно присваиваются разработчикам оборудования тахографов при подаче заявки лаборатории, уполномоченной проводить испытания эксплуатационной совместимости.

## 2.95. *ManufacturerSpecificEventFaultData*

Второе поколение:

Коды ошибок, связанные с конкретными производителями, упрощают анализ ошибок и обслуживание бортовых устройств.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
    manufacturerCode           ManufacturerCode,
    manufacturerSpecificErrorCode OCTET STRING(SIZE(3))
}
```

**manufacturerCode** идентифицирует производителя бортового устройства.

**manufacturerSpecificErrorCode** – код ошибки, связанный с конкретным производителем.

## 2.96. *MemberStateCertificate*

Сертификат открытого ключа государства-члена, выданный европейским сертификационным органом.

MemberStateCertificate ::= Certificate

## 2.97. *MemberStateCertificateRecordArray*

Второе поколение:

Сертификат государства-члена и метаданные, используемые в протоколе загрузки.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
    recordType           RecordType,
    recordSize           INTEGER(1..65535),
    noOfRecords          INTEGER(0..65535),
    records              SET SIZE(noOfRecords) OF MemberStateCertificate
}
```

**recordType** указывает на тип записи (MemberStateCertificate). **Присвоение значения:** см. RecordType

**recordSize** – размер MemberStateCertificate в байтах.

**noOfRecords** – число записей в массиве. Значение устанавливается на 1, так как сертификаты могут быть разной длины.

**records** – набор сертификатов государств-членов.

## 2.98. *MemberStatePublicKey*

Первое поколение:

Открытый ключ государства-члена.

MemberStatePublicKey ::= PublicKey

## 2.99. *Name*

Название.

```
Name ::= SEQUENCE {
    codePage          INTEGER (0..255),
    name              OCTET STRING (SIZE(35))
}
```

**codePage** определяет набор символов, указанный в главе 4,

**name** – название, закодированное с помощью указанного набора символов.

## 2.100. *NationAlpha*

Буквенное обозначение страны соответствует отличительным знакам, используемым на транспортных средствах в международных перевозках (Венская конвенция ООН о дорожном движении 1968 г.).

NationAlpha ::= IA5String(SIZE(3))

NationAlpha и цифровые коды включаются в перечень, составляемый на веб-сайте лаборатории, назначенной для проведения испытаний эксплуатационной совместимости, как указано в требовании 440 приложения 1С.

## 2.101. *NationNumeric*

Цифровое обозначение страны.

NationNumeric ::= INTEGER(0 .. 255)

**Присвоение значения:** см. тип данных 2.100 (NationAlpha).

Любое изменение или обновление спецификации буквенного или цифрового обозначения страны, описанной в предыдущем пункте, осуществляется только после того, как назначенная лаборатория получит отзывы производителей бортовых устройств цифровых и «умных» тахографов утверждённого типа.

## 2.102. *NoOfCalibrationRecords*

Число записей калибровки, которое может храниться на карточке.

Первое поколение:

NoOfCalibrationRecords ::= INTEGER(0..255)

**Присвоение значения:** см. приложение 2.

Второе поколение:

NoOfCalibrationRecords ::= INTEGER(0..2<sup>16</sup>-1)

**Присвоение значения:** см. приложение 2.

### **2.103. NoOfCalibrationsSinceDownload**

Счётчик, указывающий на число калибровок, произведённых с карточкой мастерской после последней загрузки данных с этой карточки (приложение 1С, требования 317 и 340).

NoOfCalibrationsSinceDownload ::= INTEGER(0..2<sup>16</sup>-1)

**Присвоение значения:** дополнительно не указывается.

### **2.104. NoOfCardPlaceRecords**

Число записей о месте, которое может храниться на карточке водителя или мастерской.

Первое поколение:

NoOfCardPlaceRecords ::= INTEGER(0..255)

**Присвоение значения:** см. приложение 2.

Второе поколение:

NoOfCardPlaceRecords ::= INTEGER(0..2<sup>16</sup>-1)

**Присвоение значения:** см. приложение 2.

### **2.105. NoOfCardVehicleRecords**

Число записей об используемых транспортных средствах, которое может храниться на карточке водителя или мастерской.

NoOfCardVehicleRecords ::= INTEGER(0.. 2<sup>16</sup>-1)

**Присвоение значения:** см. приложение 2.

### **2.106. NoOfCardVehicleUnitRecords**

Второе поколение:

Число записей об используемых бортовых устройствах, которое может храниться на карточке водителя или мастерской.

NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2<sup>16</sup>-1)

**Присвоение значения:** см. приложение 2.

### **2.107. NoOfCompanyActivityRecords**

Число записей о действиях предприятия, которое может храниться на карточке предприятия.

NoOfCompanyActivityRecords ::= INTEGER(0.. 2<sup>16</sup>-1)

**Присвоение значения:** см. приложение 2.

### **2.108. NoOfControlActivityRecords**

Число записей о контрольных действиях, которое может храниться на контрольной карточке.

NoOfControlActivityRecords ::= INTEGER(0.. 2<sup>16</sup>-1)

**Присвоение значения:** см. приложение 2.

**2.109. NoOfEventsPerType**

Число событий по типу события, которое может быть записано на карточку.

NoOfEventsPerType ::= INTEGER(0..255)

**Присвоение значения:** см. приложение 2.

**2.110. NoOfFaultsPerType**

Число неисправностей по типу неисправности, которое может быть записано на карточку.

NoOfFaultsPerType ::= INTEGER(0..255)

**Присвоение значения:** см. приложение 2.

**2.111. NoOfGNSSCDRecords**

Второе поколение:

Число записей о непрерывном времени управления по ГНСС, которые могут храниться на карточке.

NoOfGNSSCDRecords ::= INTEGER(0..216-1)

**Присвоение значения:** см. приложение 2.

**2.112. NoOfSpecificConditionRecords**

Второе поколение:

Число записей об особых условиях, которые могут храниться на карточке.

NoOfSpecificConditionRecords ::= INTEGER(0..216-1)

**Присвоение значения:** см. приложение 2.

**2.113. OdometerShort**

Показания одометра транспортного средства в краткой форме.

OdometerShort ::= INTEGER(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 одометра транспортного средства в полночь на данный день (приложение 1B, требование 090 и приложение 1C, требование 113).

OdometerValueMidnight ::= OdometerShort

**Присвоение значения:** дополнительно не указывается.

**2.115. OdometerValueMidnightRecordArray**

Второе поколение:

OdometerValueMidnight и метаданные, используемые в протоколе загрузки.

OdometerValueMidnightRecordArray ::= SEQUENCE {

recordType      RecordType,

```

recordSize    INTEGER(1..65535),
noOfRecords   INTEGER(0..65535),
records       SET SIZE(noOfRecords) OF OdometerValueMidnight

```

```

}
```

**recordType** указывает на тип записи (OdometerValueMidnight). **Присвоение значения:** см. RecordType

**recordSize** – размер OdometerValueMidnight в байтах.

**noOfRecords** – число записей в массиве.

**records** – массив записей OdometerValueMidnight.

## 2.116. *OverspeedNumber*

Число случаев превышения скорости после последнего контроля за превышением скорости.

OverspeedNumber ::= INTEGER(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.

## 2.117. *PlaceRecord*

Информация, касающаяся места, в котором начинается или заканчивается дневной период работы (приложение 1С, требования 108, 271, 296, 324 и 347).

Первое поколение:

```

PlaceRecord ::= SEQUENCE {
    entryTime                TimeReal,
    entryTypeDailyWorkPeriod EntryTypeDailyWorkPeriod,
    dailyWorkPeriodCountry   NationNumeric,
    dailyWorkPeriodRegion    RegionNumeric,
    vehicleOdometerValue     OdometerShort
}

```

**entryTime** – дата и время, связанные с вводом данных.

**entryTypeDailyWorkPeriod** – тип ввода.

**dailyWorkPeriodCountry** – введённая страна.

**dailyWorkPeriodRegion** – введённый регион.

**vehicleOdometerValue** – показания одометра в момент ввода данных о месте.

Второе поколение:



```
PlaceRecord ::= SEQUENCE {
    entryTime                TimeReal,
    entryTypeDailyWorkPeriod EntryTypeDailyWorkPeriod,
    dailyWorkPeriodCountry   NationNumeric,
    dailyWorkPeriodRegion    RegionNumeric,
    vehicleOdometerValue     OdometerShort,
    entryGNSSPlaceRecord     GNSSPlaceRecord
}
```

В дополнение к первому поколению, используется следующий компонент:

**entryGNSSPlaceRecord** – зафиксированные место и время.

## 2.118. PreviousVehicleInfo

Информация, касающаяся транспортного средства, использованного водителем ранее, в момент ввода его карточки в бортовое устройство (приложение 1B, требование 081 и приложение 1C, требование 102).

Первое поколение:

```
PreviousVehicleInfo ::= SEQUENCE {
    vehicleRegistrationIdentification VehicleRegistrationIdentification,
    cardWithdrawalTime              TimeReal
}
```

**vehicleRegistrationIdentification** – VRN и государство-член регистрации транспортного средства.

**cardWithdrawalTime** – дата и время извлечения карточки.

Второе поколение:

```
PreviousVehicleInfo ::= SEQUENCE {
    vehicleRegistrationIdentification VehicleRegistrationIdentification,
    cardWithdrawalTime              TimeReal,
    vuGeneration                     Generation
}
```

В дополнение к первому поколению, используется следующий элемент данных:

**vuGeneration** идентифицирует поколение бортового устройства.

## 2.119. PublicKey

Первое поколение:

Открытый ключ RSA.

```
PublicKey ::= SEQUENCE {
    rsaKeyModulus             RSAKeyModulus,
    rsaKeyPublicExponent     RSAKeyPublicExponent
}
```

**rsaKeyModulus** – модуль пары ключей.

**rsaKeyPublicExponent** – открытый показатель пары ключей.

## 2.120. RecordType

Второе поколение:

Указание на тип записи. Такой тип данных используется в RecordArrays.

RecordType ::= OCTET STRING(SIZE(1))

### Присвоение значения:

'01' H	ActivityChangeInfo,
'02' H	CardSlotsStatus,
'03' H	CurrentDateTime,
'04' H	MemberStateCertificate,
'05' H	OdometerValueMidnight,
'06' H	DateOfDayDownloaded,
'07' H	SensorPaired,
'08' H	Signature,
'09' H	SpecificConditionRecord,
'0A' H	VehicleIdentificationNumber,
'0B' H	VehicleRegistrationNumber,
'0C' H	VuCalibrationRecord,
'0D' H	VuCardIWRecord,
'0E' H	VuCardRecord,
'0F' H	VuCertificate,
'10' H	VuCompanyLocksRecord,
'11' H	VuControlActivityRecord,
'12' H	VuDetailedSpeedBlock,
'13' H	VuDownloadablePeriod,
'14' H	VuDownloadActivityData,
'15' H	VuEventRecord,
'16' H	VuGNSSCDRecord,
'17' H	VuTSConsentRecord,
'18' H	VuFaultRecord,
'19' H	VuIdentification,
'1A' H	VuOverSpeedingControlData,
'1B' H	VuOverSpeedingEventRecord,
'1C' H	VuPlaceDailyWorkPeriodRecord,
'1D' H	VuTimeAdjustmentGNSSRecord,
'1E' H	VuTimeAdjustmentRecord,
'1F' H	VuPowerSupplyInterruptionRecord,
'20' H	SensorPairedRecord,
'21' H	SensorExternalGNSSCoupledRecord,
'22' H – '7F' H	RFU,
'80' H – 'FF' H	относится к конкретному производителю.

## 2.121. RegionAlpha

Буквенное обозначение региона в конкретной стране.

RegionAlpha ::= IA5STRING(SIZE(3))

Первое поколение:

### Присвоение значения:

` ' `	Нет информации,
Испания:	
`AN`	Andalucía,
`AR`	Aragón,
`AST`	Asturias,
`C`	Cantabria,
`CAT`	Cataluña,
`CL`	Castilla-León,
`CM`	Castilla-La-Mancha,
`CV`	Valencia,
`EXT`	Extremadura,
`G`	Galicia,
`IB`	Baleares,
`IC`	Canarias,
`LR`	La Rioja,
`M`	Madrid,
`MU`	Murcia,
`NA`	Navarra,
`PV`	País Vasco

Второе поколение:

Коды RegionAlpha включаются в перечень, составляемый на веб-сайте лаборатории, назначенной для проведения испытаний эксплуатационной совместимости.

## 2.122. *RegionNumeric*

Цифровое обозначение региона в конкретной стране.

RegionNumeric ::= OCTET STRING (SIZE(1))

Первое поколение:

### Присвоение значения:

`00`H	Нет информации,
Испания:	
`01`H	Andalucía,
`02`H	Aragón,
`03`H	Asturias,
`04`H	Cantabria,
`05`H	Cataluña,
`06`H	Castilla-León,
`07`H	Castilla-La-Mancha,
`08`H	Valencia,
`09`H	Extremadura,
`0A`H	Galicia,
`0B`H	Baleares,
`0C`H	Canarias,
`0D`H	La Rioja,
`0E`H	Madrid,
`0F`H	Murcia,
`10`H	Navarra,
`11`H	País Vasco

Второе поколение:

Коды RegionNumeric включаются в перечень, составляемый на веб-сайте лаборатории, назначенной для проведения испытаний эксплуатационной совместимости.

### **2.123. RemoteCommunicationModuleSerialNumber**

Второе поколение:

Серийный номер модуля удалённой связи.

RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber

### **2.124. RSAKeyModulus**

Первое поколение:

Модуль пары ключей RSA.

RSAKeyModulus ::= OCTET STRING (SIZE(128))

**Присвоение значения:** Не указано.

### **2.125. RSAKeyPrivateExponent**

Первое поколение:

Закрытый показатель пары ключей RSA.

RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))

**Присвоение значения:** Не указано.

### **2.126. RSAKeyPublicExponent**

Первое поколение:

Открытый показатель пары ключей RSA.

RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))

**Присвоение значения:** Не указано.

### **2.127. RtmData**

Второе поколение:

Определение данного типа данных см. в приложении 14.

### **2.128. SealDataCard**

Второе поколение:

Данный тип данных хранит информацию о пломбах, наложенных на различные компоненты транспортного средства, и предназначен для хранения на карточке. Данный тип данных связан с требованием 337 приложения 1С.

```
SealDataCard ::= SEQUENCE {
    noOfSealRecords          INTEGER(1..5),
    sealRecords              SET SIZE(noOfSealRecords) OF SealRecord
}
```

**noOfSealRecords** – число записей в sealRecords.

**sealRecords** – массив записей о пломбах.

## 2.129. SealDataVu

Второе поколение:

Данный тип данных хранит информацию о пломбах, наложенных на различные компоненты транспортного средства, и предназначен для хранения в бортовом устройстве.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
    sealRecords              SealRecord
}
```

**sealRecords** – массив записей о пломбах. Если число пломб менее 5, значение EquipmentType во всех неиспользуемых sealRecords устанавливается на 16, т.е. не используется.

## 2.130. SealRecord

Второе поколение:

Данный тип данных хранит информацию о пломбе, наложенной на компонент. Данный тип данных связан с требованием 337 приложения 1С.

```
SealRecord ::= SEQUENCE {
    equipmentType            EquipmentType,
    extendedSealIdentifier   ExtendedSealIdentifier
}
```

**equipmentType** идентифицирует тип оборудования, на которое наложена пломба.

**extendedSealIdentifier** – идентификатор пломбы, наложенной на оборудование.

## 2.131. SensorApprovalNumber

Номер официального утверждения типа датчика.

Первое поколение:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

**Присвоение значения:** Не указано.

Второе поколение:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

**Присвоение значения:**

Номер официального утверждения указывается в соответствии с публикацией на соответствующем веб-сайте Европейской комиссии, например, с дефисами, если они есть. Номер официального утверждения смещён влево.

## 2.132. *SensorExternalGNSSApprovalNumber*

Второе поколение:

Номер официального утверждения типа внешнего устройства ГНСС.

`SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))`

**Присвоение значения:**

Номер официального утверждения указывается в соответствии с публикацией на соответствующем веб-сайте Европейской комиссии, например, с дефисами, если они есть. Номер официального утверждения смещён влево.

## 2.133. *SensorExternalGNSSCoupledRecord*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к идентификации внешнего устройства ГНСС, соединённого с бортовым устройством (приложение 1С, требование 100).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {  
    sensorSerialNumber          SensorGNSSSerialNumber,  
    sensorApprovalNumber       SensorExternalGNSSApprovalNumber,  
    sensorCouplingDate         SensorGNSSCouplingDate  
}
```

**sensorSerialNumber** – серийный номер внешнего устройства ГНСС, соединённого с бортовым устройством.

**sensorApprovalNumber** – номер официального утверждения внешнего устройства ГНСС.

**sensorCouplingDate** – дата соединения внешнего устройства ГНСС с бортовым устройством.

## 2.134. *SensorExternalGNSSIdentification*

Второе поколение:

Информация, связанная с идентификацией внешнего устройства ГНСС (приложение 1С, требование 98).

```
SensorExternalGNSSIdentification ::= SEQUENCE {
    sensorSerialNumber          SensorGNSSSerialNumber,
    sensorApprovalNumber       SensorExternalGNSSApprovalNumber,
    sensorSCIdentifier          SensorExternalGNSSSCIdentifier,
    sensorOSIdentifier          SensorExternalGNSSOSIdentifier
}
```

**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*

Второе поколение:

Информация, хранящаяся на внешнем устройстве ГНСС, которая относится к установке внешнего датчика ГНСС (приложение 1С, требование 123).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
    sensorCouplingDateFirst    SensorGNSSCouplingDate,
    firstVuApprovalNumber      VuApprovalNumber,
    firstVuSerialNumber        VuSerialNumber,
    sensorCouplingDateCurrent  SensorGNSSCouplingDate,
    currentVuApprovalNumber    VuApprovalNumber,
    currentVUSerialNumber      VuSerialNumber
}
```

**sensorCouplingDateFirst** —дата первого соединения внешнего устройства ГНСС с бортовым устройством.

**firstVuApprovalNumber** —номер официального утверждения первого бортового устройства, соединённого с внешним устройством ГНСС.

**firstVuSerialNumber** —серийный номер первого бортового устройства, соединённого с внешним устройством ГНСС.

**sensorCouplingDateCurrent** —дата текущего соединения внешнего устройства ГНСС с бортовым устройством.

**currentVuApprovalNumber** —номер официального утверждения бортового устройства, в настоящее время соединённого с внешним устройством ГНСС.

**currentVUSerialNumber** —серийный номер бортового устройства, в настоящее время соединённого с внешним устройством ГНСС.

### **2.136. *SensorExternalGNSSOSIdentifier***

Второе поколение:

Идентификатор операционной системы внешнего устройства ГНСС.

SensorOSIdentifier ::= IA5String(SIZE(2))

**Присвоение значения:** связано с конкретным производителем.

### **2.137. *SensorExternalGNSSSCIdentifier***

Второе поколение:

Данный тип используется, например, для идентификации криптографического модуля внешнего устройства ГНСС.

Идентификатор компонента защиты внешнего устройства ГНСС.

SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))

**Присвоение значения:** связано с конкретным производителем компонента.

### **2.138. *SensorGNSSCouplingDate***

Второе поколение:

Дата соединения внешнего устройства ГНСС с бортовым устройством.

SensorGNSSCouplingDate ::= TimeReal

**Присвоение значения:** Не указано.

### **2.139. *SensorGNSSSerialNumber***

Второе поколение:

Данный тип используется для хранения серийного номера приёмника ГНСС, и когда он внутри БУ, и когда снаружи него.

Серийный номер приёмника ГНСС.

SensorGNSSSerialNumber ::= ExtendedSerialNumber

### **2.140. *SensorIdentification***

Информация, записанная в датчике движения, которая относится к идентификации датчика движения (приложение 1В, требование 077 и приложение 1С, требование 95).

```
SensorIdentification ::= SEQUENCE {  
    sensorSerialNumber          SensorSerialNumber,  
    sensorApprovalNumber       SensorApprovalNumber,  
    sensorSCIdentifier          SensorSCIdentifier,  
    sensorOSIdentifier         SensorOSIdentifier  
}
```

**sensorSerialNumber** – расширенный серийный номер датчика движения (включая номер детали и код производителя).

**sensorApprovalNumber** – номер официального утверждения датчика движения.

**sensorSCIdentifier** – идентификатор компоненты защиты датчика движения.

**sensorOSIdentifier** – идентификатор операционной системы датчика движения.



## 2.141. *SensorInstallation*

Информация, записанная в датчике движения, которая относится к установке датчика движения (приложение 1B, требование 099 и приложение 1C, требование 122).

```
SensorInstallation ::= SEQUENCE {
    sensorPairingDateFirst           SensorPairingDate,
    firstVuApprovalNumber           VuApprovalNumber,
    firstVuSerialNumber             VuSerialNumber,
    sensorPairingDateCurrent        SensorPairingDate,
    currentVuApprovalNumber         VuApprovalNumber,
    currentVUSerialNumber           VuSerialNumber
}
```

**sensorPairingDateFirst** – дата первого соединения датчика движения с бортовым устройством.

**firstVuApprovalNumber** – номер официального утверждения первого бортового устройства, соединённого с датчиком движения.

**firstVuSerialNumber** – серийный номер первого бортового устройства, соединённого с датчиком движения.

**sensorPairingDateCurrent** – дата текущего соединения датчика движения с бортовым устройством.

**currentVuApprovalNumber** – номер официального утверждения бортового устройства, в настоящее время соединённого с датчиком движения.

**currentVUSerialNumber** – серийный номер бортового устройства, в настоящее время соединённого с датчиком движения.

## 2.142. *SensorInstallationSecData*

Информация, записанная на карточке мастерской, которая имеет отношение к данным о защите, необходимым для подсоединения датчиков движения к бортовым устройствам (приложение 1C, требования 308 и 331).

Первое поколение:

```
SensorInstallationSecData ::= TDesSessionKey
```

**Присвоение значения:** в соответствии с ISO 16844-3.

Второе поколение:

Как описано в приложении 11, на карточке мастерской хранится до трёх ключей для соединения БУ и датчика движения. У этих ключей разные версии.

```
SensorInstallationSecData ::= SEQUENCE {
    kMWCKey1           KMWCKey,
    kMWCKey2           KMWCKey OPTIONAL,
    kMWCKey3           KMWCKey OPTIONAL
}
```

## 2.143. *SensorOSIdentifier*

Идентификатор операционной системы датчика движения.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

**Присвоение значения:** связано с конкретным производителем.

## 2.144. *SensorPaired*

Первое поколение:

Информация, записанная в бортовом устройстве, которая относится к идентификации датчика движения, соединённого с бортовым устройством (приложение 1В, требование 079).

```
SensorPaired ::= SEQUENCE {
    sensorSerialNumber          SensorSerialNumber,
    sensorApprovalNumber       SensorApprovalNumber,
    sensorPairingDateFirst     SensorPairingDate
}
```

**sensorSerialNumber** – серийный номер датчика движения, в настоящее время соединённого с бортовым устройством.

**sensorApprovalNumber** – номер официального утверждения датчика движения, в настоящее время соединённого с бортовым устройством.

**sensorPairingDateFirst** – дата первого соединения с бортовым устройством датчика движения, в настоящее время соединённого с бортовым устройством.

## 2.145. *SensorPairedRecord*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к идентификации датчика движения, соединённого с бортовым устройством (приложение 1С, требование 97).

```
SensorPairedRecord ::= SEQUENCE {
    sensorSerialNumber          SensorSerialNumber,
    sensorApprovalNumber       SensorApprovalNumber,
    sensorPairingDate          SensorPairingDate
}
```

**sensorSerialNumber** – серийный номер датчика движения, соединённого с бортовым устройством.

**sensorApprovalNumber** – номер официального утверждения датчика движения.

**sensorPairingDate** – дата соединения датчика движения с бортовым устройством.

## 2.146. *SensorPairingDate*

Дата соединения датчика движения с бортовым устройством.

SensorPairingDate ::= TimeReal

**Присвоение значения:** Не указано.

## 2.147. *SensorSCIdentifier*

Идентификатор компонента защиты датчика движения.

SensorSCIdentifier ::= IA5String(SIZE(8))

**Присвоение значения:** связано с конкретным производителем компонента.

## 2.148. *SensorSerialNumber*

Серийный номер датчика движения.

SensorSerialNumber ::= ExtendedSerialNumber

## 2.149. *Signature*

Цифровая подпись.

Первое поколение:

Signature ::= OCTET STRING (SIZE(128))

**Присвоение значения:** в соответствии с приложением 11 об общих механизмах защиты.

Второе поколение:

Signature ::= OCTET STRING (SIZE(64..132))

**Присвоение значения:** в соответствии с приложением 11 об общих механизмах защиты.

## 2.150. *SignatureRecordArray*

Второе поколение:

Набор подписей и метаданные, используемые в протоколе загрузки.

```
SignatureRecordArray ::= SEQUENCE {
    recordType           RecordType,
    recordSize          INTEGER(1..65535),
    noOfRecords         INTEGER(0..65535),
    records             SET SIZE(noOfRecords) OF Signature
}
```

**recordType** указывает на тип записи (Signature). **Присвоение значения:** см. RecordType

**recordSize** – размер Signature в байтах.

**noOfRecords** – число записей в массиве. Значение устанавливается на 1, так как подписи могут быть разной длины.

**records** – набор подписей.

## 2.151. *SimilarEventsNumber*

Число похожих событий в течение одного конкретного дня (приложение 1B, требование 094 и приложение 1C, требование 117).

SimilarEventsNumber ::= INTEGER(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*

Информация, записанная на карточке водителя или мастерской или в бортовом устройстве, которая имеет отношение к особому условию (приложение 1C, требования 130, 276, 301, 328 и 355).

```
SpecificConditionRecord ::= SEQUENCE {
    entryTime                TimeReal,
    specificConditionType    SpecificConditionType
}
```

**entryTime** – дата и время ввода.

**specificConditionType** – код, позволяющий идентифицировать особое условие.

## 2.153. *SpecificConditions*

Информация, записанная на карточке водителя или мастерской или в бортовом устройстве, которая имеет отношение к особому условию (приложение 1С, требования 131, 277, 302, 329 и 356).

Второе поколение:

```
SpecificConditions := SEQUENCE {
    conditionPointerNewestRecord    INTEGER(0..NoOfSpecificConditionRecords-1),
    specificConditionRecords        SET SIZE(NoOfSpecificConditionRecords) OF
                                     SpecificConditionRecord
}
```

**conditionPointerNewestRecord** – индекс последней обновлённой записи об особых условиях.

**Присвоение значения:** Число, соответствующее числовому показателю записи данных об особых условиях, которое начинается с 0 в случае первой регистрации регистрации записей, касающихся особых условий, в структуре.

**specificConditionRecords** – совокупность записей, содержащих информацию об зафиксированных особых условиях.

## 2.154. *SpecificConditionType*

Код, позволяющий идентифицировать особые условия (приложение 1В, требования 050b, 105a, 212a и 230a и приложение 1С, требование 62).

```
SpecificConditionType ::= INTEGER(0..255)
```

Первое поколение:

**Присвоение значения:**

'00'Н	RFU
'01'Н	Вне области применения –начало
'02'Н	Вне области применения –конец
'03'Н	Паром/ж/д переезд
'04'Н .. 'FF'Н	RFU

Второе поколение:

**Присвоение значения:**

'00'Н	RFU
'01'Н	Вне области применения –начало
'02'Н	Вне области применения –конец
'03'Н	Паром/ж/д переезд – начало
'04'Н	Паром/ж/д переезд – конец
'05'Н .. 'FF'Н	RFU

**2.155. Speed**

Скорость транспортного средства (км/ч).

Speed ::= INTEGER(0..255)

**Присвоение значения:** км в час в рабочем диапазоне от 0 до 220 км/ч.

**2.156. SpeedAuthorised**

Максимальная разрешённая скорость транспортного средства (определение hh).

SpeedAuthorised ::= Speed

**2.157. SpeedAverage**

Средняя скорость за предварительно определённый промежуток времени (км/ч).

SpeedAverage ::= Speed

**2.158. SpeedMax**

Максимальная скорость за предварительно определённый промежуток времени.

SpeedMax ::= Speed

**2.159. TachographPayload**

Второе поколение:

Определение данного типа данных см. в приложении 14.

**2.160. TachographPayloadEncrypted**

Второе поколение:

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 {
    tag                OCTET STRING(SIZE(1)),
    length             OCTET STRING(SIZE(1..2)),
    paddingContentIndicatorByte OCTET STRING(SIZE(1)),
    encryptedData      OCTET STRING(SIZE(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.

**paddingContentIndicatorByte** устанавливается на '00'.

**encryptedData** — это зашифрованная позиция tachographPayload, как указано в приложении 11, часть Б, глава 13. Октетная длина данного элемента данных всегда кратна 16.

## 2.161. TDesSessionKey

Первое поколение:

Тройной ключ сеанса в системе DES.

```
TDesSessionKey ::= SEQUENCE {
    tDesKeyA          OCTET STRING (SIZE(8)),
    tDesKeyB          OCTET STRING (SIZE(8))
}
```

**Присвоение значения:** дополнительно не указывается.

## 2.162. TimeReal

Код совмещённого поля данных даты и времени, в котором дата и время выражаются в секундах, начиная с 00 ч. 00 м. 00 с. 1 января 1970 г. (GMT).

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

**Присвоение значения – выровненный октет:** Число секунд с полуночи 1 января 1970 г. (GMT).

Максимально возможное отображение даты/времени – 2106 г.

## 2.163. TyreSize

Обозначение размера шин.

```
TyreSize ::= IA5String(SIZE(15))
```

**Присвоение значения:** в соответствии с Директивой 92/23 (ЕЭС), 31/03/1992, ОЖ L 129, стр. 95.

## 2.164. VehicleIdentificationNumber

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

Второе поколение:

Идентификационный номер транспортного средства и метаданные, используемые в протоколе загрузки.

```

VehicleIdentificationNumberRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize          INTEGER(1..65535),
    noOfRecords         INTEGER(0..65535),
    records              SET SIZE(noOfRecords) OF VehicleIdentificationNumber
}

```

**recordType** указывает на тип записи (VehicleIdentificationNumber). **Присвоение значения:** см. RecordType

**recordSize** – размер VehicleIdentificationNumber в байтах.

**noOfRecords** – число записей в массиве.

**records** – набор идентификационных номеров транспортных средств.

## 2.166. VehicleRegistrationIdentification

Идентификационные данные транспортного средства, уникальные для Европы (VRN и государство-член).

```

VehicleRegistrationIdentification ::= SEQUENCE {
    vehicleRegistrationNation  NationNumeric,
    vehicleRegistrationNumber  VehicleRegistrationNumber
}

```

**vehicleRegistrationNation** – страна, в которой зарегистрировано транспортное средство.

**vehicleRegistrationNumber** – регистрационный номер транспортного средства (VRN).

## 2.167. VehicleRegistrationNumber

Регистрационный номер транспортного средства (VRN). Номер регистрации присваивается компетентным органом, регистрирующим транспортное средство.

```

VehicleRegistrationNumber ::= SEQUENCE {
    codePage          ЦЕЛОЕ ЧИСЛО (0..255),
    vehicleRegNumber  OCTET STRING (SIZE (13))
}

```

**codePage** определяет набор символов, указанный в главе 4,

**vehicleRegNumber** – VRN, закодированный с помощью указанного набора символов.

**Присвоение значения:** связано с конкретной страной.

## 2.168. VehicleRegistrationNumberRecordArray

Второе поколение:

Регистрационный номер транспортного средства и метаданные, используемые в протоколе загрузки.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize          INTEGER(1..65535),
    noOfRecords         INTEGER(0..65535),
    records              SET SIZE(noOfRecords) OF VehicleRegistrationNumber
}
```

**recordType** указывает на тип записи (VehicleRegistrationNumber). **Присвоение значения:** см. RecordType

**recordSize** – размер VehicleRegistrationNumber в байтах.

**noOfRecords** – число записей в массиве.

**records** – набор регистрационных номеров транспортных средств.

## 2.169. VuAbility

Второе поколение:

Информация, хранящаяся в БУ о способности или неспособности БУ использовать карточки тахографов первого поколения (приложение 1С, требование 121).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

**Присвоение значения – выровненный октет:** ‘xxxxxxx’В (8 бит)

Относительно возможности поддерживать карточки первого поколения:

‘a’В           Способность поддерживать карточки тахографов первого поколения:  
‘0’В Первое поколение поддерживается,  
‘1’В Первое поколение не поддерживается,

‘xxxxxxx’В RFU

## 2.170. VuActivityDailyData

Первое поколение:

Информация, записанная в БУ, которая имеет отношение к изменению вида деятельности и/или изменению статуса управления и/или изменению состояния карточки за данный календарный день (приложение 1В, требование 084 и приложение 1С, требования 105, 106 и 107) и к состоянию считывающих устройств на 00:00 часов в указанный день.

```
VuActivityDailyData ::= SEQUENCE {
    noOfActivityChanges          INTEGER SIZE(0..1440),
    activityChangeInfos           SET SIZE(noOfActivityChanges) OF ActivityChangeInfo
}
```

**noOfActivityChanges** – число слов позиции ActivityChangeInfo в совокупности данных activityChangeInfos.

**activityChangeInfos** – совокупность слов позиции ActivityChangeInfo, записанных в БУ за данный день. Всегда включает в себя два слова ActivityChangeInfo, указывающих на состояние двух считывающих устройств в 00:00 часов в указанный день.

## 2.171. VuActivityDailyRecordArray

Второе поколение:

Информация, записанная в БУ, которая имеет отношение к изменению вида деятельности и/или изменению статуса управления и/или изменению состояния карточки за данный календарный день (приложение 1С, требования 105, 106 и 107) и к состоянию считывающих устройств на 00:00 часов в указанный день.



```
VuActivityDailyRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize          INTEGER(1..65535),
    noOfRecords        INTEGER(0..65535),
    records             SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

**recordType** указывает на тип записи (ActivityChangeInfo). **Присвоение значения:** см. RecordType

**recordSize** – размер ActivityChangeInfo в байтах.

**noOfRecords** – число записей в массиве.

**activityChangeInfos** – совокупность слов позиции ActivityChangeInfo, записанных в БУ за данный день. Всегда включает в себя два слова ActivityChangeInfo, указывающих на состояние двух считывающих устройств в 00:00 часов в указанный день.

## 2.172. VuApprovalNumber

Номер официального утверждения типа бортового устройства.

Первое поколение:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

**Присвоение значения:** Не указано.

Второе поколение:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

**Присвоение значения:**

Номер официального утверждения указывается в соответствии с публикацией на соответствующем веб-сайте Европейской комиссии, например, с дефисами, если они есть. Номер официального утверждения смещён влево.

## 2.173. VuCalibrationData

Первое поколение:

Информация, записанная в бортовом устройстве, которая относится к калибровке записывающего оборудования (приложение 1B, требование 098).

```
VuCalibrationData ::= SEQUENCE {
    noOfVuCalibrationRecords    INTEGER(0..255),
    vuCalibrationRecords        SET SIZE(noOfVuCalibrationRecords) OF VuCalibrationRecord
}
```

**noOfVuCalibrationRecords** – число записей, содержащихся в совокупности vuCalibrationRecords.

**vuCalibrationRecords** – массив записей калибровки.

## 2.174. VuCalibrationRecord

Информация, записанная в бортовом устройстве, которая относится калибровка записывающего оборудования (приложение 1B, требование 098 и приложение 1C, требования 119 и 120).

Первое поколение:

```
VuCalibrationRecord ::= SEQUENCE {
    calibrationPurpose           CalibrationPurpose,
    workshopName                 Name,
    workshopAddress              Address,
    workshopCardNumber           FullCardNumber,
    workshopCardExpiryDate      TimeReal,
    vehicleIdentificationNumber  VehicleIdentificationNumber,
    vehicleRegistrationIdentification VehicleRegistrationIdentification,
    wVehicleCharacteristicConstant W-VehicleCharacteristicConstant,
    kConstantOfRecordingEquipment K-ConstantOfRecordingEquipment,
    lTyreCircumference           L-TyreCircumference,
    tyreSize                     TyreSize,
    authorisedSpeed              SpeedAuthorised,
    oldOdometerValue             OdometerShort,
    newOdometerValue             OdometerShort,
    oldTimeValue                 TimeReal,
    newTimeValue                 TimeReal,
    nextCalibrationDate          TimeReal
}
```

**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** содержит VRN и государство-член регистрации.

**wVehicleCharacteristicConstant** – характеристический коэффициент транспортного средства.

**kConstantOfRecordingEquipment** – постоянная величина записывающего оборудования.

**lTyreCircumference** – фактическая окружность шин колёс.

**tyreSize** – обозначение габаритов шин транспортного средства.

**authorisedSpeed** – допустимая скорость транспортного средства.

**oldOdometerValue, newOdometerValue** – старые и новые показания одометра.

**oldTimeValue, newTimeValue** – старые и новые значения даты и времени.

**nextCalibrationDate** – дата следующей калибровки типа, указанного в CalibrationPurpose, которую должен провести компетентный инспекционный орган.

Второе поколение:

```

VuCalibrationRecord ::= SEQUENCE {
    calibrationPurpose           CalibrationPurpose,
    workshopName                 Name,
    workshopAddress              Address,
    workshopCardNumber          FullCardNumber,
    workshopCardExpiryDate      TimeReal,
    vehicleIdentificationNumber  VehicleIdentificationNumber,
    vehicleRegistrationIdentification
    VehicleRegistrationIdentification,
    wVehicleCharacteristicConstant
    W-VehicleCharacteristicConstant,
    kConstantOfRecordingEquipment
    K-ConstantOfRecordingEquipment,
    lTyreCircumference           L-TyreCircumference,
    tyreSize                     TyreSize,
    authorisedSpeed              SpeedAuthorised,
    oldOdometerValue             OdometerShort,
    newOdometerValue            OdometerShort,
    oldTimeValue                 TimeReal,
    newTimeValue                 TimeReal,
    nextCalibrationDate          TimeReal,
    sealDataVu                   SealDataVu
}

```

В дополнение к первому поколению, используется следующий элемент данных:

**sealDataVu** предоставляет информацию о пломбах, наложенных на различные компоненты транспортного средства.

## 2.175. VuCalibrationRecordArray

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к калибровке записывающего оборудования (приложение 1С, требования 119 и 120).

```

VuCalibrationRecordArray ::= SEQUENCE {
    recordType                   RecordType,
    recordSize                   INTEGER(1..65535),
    noOfRecords                  INTEGER(0..65535),
    records                      SET SIZE(noOfRecords) OF VuCalibrationRecord
}

```

**recordType** указывает на тип записи (VuCalibrationRecord). **Присвоение значения:** см. RecordType

**recordSize** – размер VuCalibrationRecord в байтах.

**noOfRecords** – число записей в массиве.

**records** – массив записей калибровки.

## 2.176. VuCardIWData

Первое поколение:

Информация, записанная в бортовом устройстве, которая имеет отношение к циклам ввода карточек водителя или карточек мастерской в бортовое устройство и их извлечения (приложение 1B, требование 081 и приложение 1C, требование 103).

```
VuCardIWData ::= SEQUENCE {
    noOfIWRecords          INTEGER(0..216-1),
    vuCardIWRecords       SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

**noOfIWRecords** – число записей в совокупности vuCardIWRecords.

**vuCardIWRecords** – совокупность записей, относящихся к циклам ввода и извлечения карточек.

## 2.177. VuCardIWRecord

Информация, записанная в бортовом устройстве, которая имеет отношение к циклу ввода карточки водителя или карточки мастерской в бортовое устройство и их извлечения (приложение 1B, требование 081 и приложение 1C, требование 102).

Первое поколение:

```
VuCardIWRecord ::= SEQUENCE {
    cardHolderName          HolderName,
    fullCardNumber          FullCardNumber,
    cardExpiryDate          TimeReal,
    cardInsertionTime       TimeReal,
    vehicleOdometerValueAtInsertion OdometerShort,
    cardSlotNumber          CardSlotNumber,
    cardWithdrawalTime      TimeReal,
    vehicleOdometerValueAtWithdrawal OdometerShort,
    previousVehicleInfo     PreviousVehicleInfo,
    manualInputFlag         ManualInputFlag
}
```

**cardHolderName** – фамилия и имя (имена) владельца карточки водителя или мастерской, записанные на карточке.

**fullCardNumber** – тип карточки, выдавшее её государство-член и номер карточки, записанные на карточке.

**cardExpiryDate** – дата истечения срока действия карточки, записанная на карточке.

**cardInsertionTime** – дата и время ввода.

**vehicleOdometerValueAtInsertion** – показание одометра транспортного средства в момент ввода карточки.

**cardSlotNumber** – считывающее устройство, в которое вставляется карточка.

**cardWithdrawalTime** – дата и время извлечения.

**vehicleOdometerValueAtWithdrawal** – показание одометра транспортного средства в момент извлечения карточки.

**previousVehicleInfo** – информация о предыдущем транспортном средстве, которым пользовался водитель, записанная на карточке.

**manualInputFlag** – метка, позволяющая определить, ввёл ли владелец карточки в момент её ввода данные о деятельности водителя вручную.

Второе поколение:

```
VuCardIWRecord ::= SEQUENCE {
    cardHolderName           HolderName,
    fullCardNumberAndGeneration FullCardNumberAndGeneration,
    cardExpiryDate           TimeReal,
    cardInsertionTime        TimeReal,
    vehicleOdometerValueAtInsertion OdometerShort,
    cardSlotNumber           CardSlotNumber,
    cardWithdrawalTime       TimeReal,
    vehicleOdometerValueAtWithdrawal OdometerShort,
    previousVehicleInfo       PreviousVehicleInfo,
    manualInputFlag          ManualInputFlag
}
```

Вместо fullCardNumber в структуре данных второго поколения используется следующий элемент данных.

**fullCardNumberAndGeneration** – тип карточки, выдавшее её государство-член и номер и поколение карточки, записанные на карточке.

## 2.178. VuCardIWRecordArray

Второе поколение:

Информация, записанная в бортовом устройстве, которая имеет отношение к циклам ввода карточек водителя или карточек мастерской в бортовое устройство и их извлечения (приложение 1С, требование 103).

```
VuCardIWRecordArray ::= SEQUENCE {
    recordType           RecordType,
    recordSize           INTEGER(1..65535),
    noOfRecords          INTEGER(0..65535),
    records              SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

**recordType** указывает на тип записи (VuCardIWRecord). **Присвоение значения:** см. RecordType

**recordSize** – размер VuCardIWRecord в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей, относящихся к циклам ввода и извлечения карточек.

## 2.179. VuCardRecord

Второе поколение:

Информация, записанная в бортовом устройстве, об используемой карточке тахографа (приложение 1С, требование 132).

```
VuCardRecord ::= SEQUENCE {  
    cardExtendedSerialNumber      ExtendedSerialNumber,  
    cardPersonaliserID            OCTET STRING(SIZE(1)),  
    typeOfTachographCardID       EquipmentType,  
    cardStructureVersion          CardStructureVersion,  
    cardNumber                    CardNumber  
}
```

**cardExtendedSerialNumber** считывается из файла EF\_ICC в MF карточки.

**cardPersonaliserID** считывается из файла EF\_ICC в MF карточки.

**typeOfTachographCardID** считывается из файла EF\_Application\_Identification в DF\_Tachograph\_G2

**cardStructureVersion** считывается из файла EF\_Application\_Identification в DF\_Tachograph\_G2.

**cardNumber** считывается из файла EF\_Identification в DF\_Tachograph\_G2.

## 2.180. VuCardRecordArray

Второе поколение:

Информация, записанная в бортовом устройстве, об карточках тахографа, используемых в данном бортовом устройстве. Данная информация включается в анализ БУ, касающийся проблем с карточками (приложение 1С, требование 132).

```
VuCardRecordArray ::= SEQUENCE {  
    recordType      RecordType,  
    recordSize      INTEGER(1..65535),  
    noOfRecords     INTEGER(0..65535),  
    records         SET SIZE(noOfRecords) OF VuCardRecord  
}
```

**recordType** указывает на тип записи (VuCardRecord). **Присвоение значения:** см. RecordType

**recordSize** – размер VuCardRecord в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей, относящихся к карточкам тахографа, используемым в БУ.

## 2.181. VuCertificate

Сертификат открытого ключа бортового устройства.

VuCertificate ::= Certificate

## 2.182. VuCertificateRecordArray

Второе поколение:

Сертификат БУ и метаданные, используемые в протоколе загрузки.

```
VuCertificateRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize          INTEGER(1..65535),
    noOfRecords         INTEGER(0..65535),
    records             SET SIZE(noOfRecords) OF VuCertificate
}
```

**recordType** указывает на тип записи (VuCertificate). **Присвоение значения:** см. RecordType

**recordSize** – размер VuCertificate в байтах.

**noOfRecords** – число записей в массиве. Значение устанавливается на 1, так как сертификаты могут быть разной длины.

**records** – набор сертификатов БУ.

### 2.183. VuCompanyLocksData

Первое поколение:

Информация, записанная в бортовом устройстве, которая относится к блокировке предприятием (приложение 1В, требование 104).

```
VuCompanyLocksData ::= SEQUENCE {
    noOfLocks           INTEGER(0..255),
    vuCompanyLocksRecords SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

**noOfLocks** – число блокировок, перечисленных в файле vuCompanyLocksRecords

**vuCompanyLocksRecords** – совокупность записей действий блокировки, произведённых предприятием.

### 2.184. VuCompanyLocksRecord

Информация, записанная в бортовом устройстве, которая относится к одной блокировке предприятием (приложение 1В, требование 104 и приложение 1С, требование 128).

Первое поколение:

```
VuCompanyLocksRecord ::= SEQUENCE {
    lockInTime          TimeReal,
    lockOutTime         TimeReal,
    companyName         Name,
    companyAddress      Address,
    companyCardNumber   FullCardNumber
}
```

**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.

Второе поколение:

```
VuCompanyLocksRecord ::= SEQUENCE {
    lockInTime           TimeReal,
    lockOutTime          TimeReal,
    companyName          Name,
    companyAddress       Address,
    companyCardNumberAndGeneration FullCardNumberAndGeneration
}
```

Вместо `companyCardNumber` в структуре данных второго поколения используется следующий элемент данных. **companyCardNumberAndGeneration** идентифицирует карточку, используемую при блокировке, и её поколение.

## 2.185. *VuCompanyLocksRecordArray*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к блокировке предприятием (приложение 1С, требование 128).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
    recordType           RecordType,
    recordSize           INTEGER(1..65535),
    noOfRecords          INTEGER(0..65535),
    records              SET SIZE(noOfRecords) OF VuCompanyLocksRecord
}
```

**recordType** указывает на тип записи (`VuCompanyLocksRecord`). **Присвоение значения:** см. `RecordType`

**recordSize** – размер `VuCompanyLocksRecord` в байтах.

**noOfRecords** – число записей в массиве. Значение 0..255.

**records** – совокупность записей действий блокировки, произведённых предприятием.

## 2.186. *VuControlActivityData*

Первое поколение:

Информация, записанная в бортовом устройстве, которая относится к контрольным действиям, проведённым с данным БУ (приложение 1В, требование 102).

```
VuControlActivityData ::= SEQUENCE {
    noOfControls          INTEGER(0..20),
    vuControlActivityRecords SET SIZE(noOfControls) OF VuControlActivityRecord
}
```

**noOfControls** – число контрольных действий, перечисленных в `vuControlActivityRecords`.

**vuControlActivityRecords** – совокупность записей контрольных действий.



## 2.187. *VuControlActivityRecord*

Информация, записанная в бортовом устройстве, которая относится к контрольному действию с данным БУ (приложение 1В, требование 102 и приложение 1С, требование 126).

Первое поколение:

```
VuControlActivityRecord ::= SEQUENCE {
    controlType           ControlType,
    controlTime           TimeReal,
    controlCardNumber    FullCardNumber,
    downloadPeriodBeginTime TimeReal,
    downloadPeriodEndTime TimeReal
}
```

**controlType** – тип контроля.

**controlTime** – дата и время ввода.

**controlCardNumber** – идентификатор карточки контролёра, использованной для контрольных действий.

**downloadPeriodBeginTime** – время начала периода, за который загружаются данные (в случае загрузки).

**downloadPeriodEndTime** – время окончания периода, за который загружаются данные (в случае загрузки).

Второе поколение:

```
VuControlActivityRecord ::= SEQUENCE {
    controlType           ControlType,
    controlTime           TimeReal,
    controlCardNumberAndGeneration FullCardNumberAndGeneration,
    downloadPeriodBeginTime TimeReal,
    downloadPeriodEndTime TimeReal
}
```

Вместо **controlCardNumber** в структуре данных второго поколения используется следующий элемент данных.

**controlCardNumberAndGeneration** – идентификатор контрольной карточки, использованной для контрольных действий.

## 2.188. *VuControlActivityRecordArray*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к контрольным действиям, проведённым с данным БУ (приложение 1С, требование 126).

```
VuControlActivityRecordArray ::= SEQUENCE {
    recordType           RecordType,
    recordSize           INTEGER(1..65535),
    noOfRecords          INTEGER(0..65535),
    records              SET SIZE(noOfRecords) OF VuControlActivityRecord
}
```

**recordType** указывает на тип записи (*VuControlActivityRecord*). **Присвоение значения:** см. *RecordType*

**recordSize** – размер *VuControlActivityRecord* в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей контрольных действий, связанных с БУ.

## 2.189. *VuDataBlockCounter*

Счётчик, записанный на карточке, который позволяет определять последовательную нумерацию циклов ввода и извлечения карточки в бортовых устройствах.

`VuDataBlockCounter ::= BCDString(SIZE(2))`

**Присвоение значения:** Порядковый номер с макс. значением 9 999, который снова начинается с 0.

## 2.190. *VuDetailedSpeedBlock*

Информация, записанная в бортовом устройстве, которая относится к подробным данным скорости транспортного средства за минуту, в течение которой транспортное средство находится в движении (приложение 1В, требование 093 и приложение 1С, требование 116).

```
VuDetailedSpeedBlock ::= SEQUENCE {
    speedBlockBeginDate          TimeReal,
    speedsPerSecond              SEQUENCE SIZE(60) OF Speed
}
```

**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 времени позиции `speedBlockBeginDate` (включительно).

## 2.191. *VuDetailedSpeedBlockRecordArray*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к подробным данным о скорости транспортного средства.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
    recordType                    RecordType,
    recordSize                    INTEGER(1..65535),
    noOfRecords                   INTEGER(0..65535),
    records                       SET SIZE(noOfRecords) OF VuDetailedSpeedBlock
}
```

**recordType** указывает на тип записи (`VuDetailedSpeedBlock`). **Присвоение значения:** см. `RecordType`

**recordSize** – размер `VuDetailedSpeedBlock` в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей о подробных блоках данных скорости.

## 2.192. *VuDetailedSpeedData*

Первое поколение:

Информация, записанная в бортовом устройстве, которая относится к подробным данным о скорости транспортного средства.

```
VuDetailedSpeedData ::= SEQUENCE {
    noOfSpeedBlocks               INTEGER(0..216-1),
    vuDetailedSpeedBlocks         SET SIZE(noOfSpeedBlocks) OF VuDetailedSpeedBlock
}
```

**noOfSpeedBlocks** – число блоков данных скорости в совокупности данных `vuDetailedSpeedBlocks`.

**vuDetailedSpeedBlocks** – совокупность записей о подробных блоках данных скорости.

## 2.193. *VuDownloadablePeriod*

Самая давняя и новейшая даты, на которые в бортовом устройстве хранятся данные, связанные с деятельностью водителя (приложение 1B, требования 081, 084 или 087 и приложение 1C, требования 102, 105, 108).

```
VuDownloadablePeriod ::= SEQUENCE {
    minDownloadableTime      TimeReal
    maxDownloadableTime      TimeReal
}
```

**minDownloadableTime** – самая давний ввод карточки или изменение вида деятельности, или дата и время прибытия на место, хранящиеся в БУ.

**maxDownloadableTime** – последнее извлечение карточки или изменение вида деятельности, или дата и время прибытия на место, хранящиеся в БУ.

## 2.194. *VuDownloadablePeriodRecordArray*

Второе поколение:

VUDownloadablePeriod и метаданные, используемые в протоколе загрузки.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
    recordType                RecordType,
    recordSize                INTEGER(1..65535),
    noOfRecords              INTEGER(0..65535),
    records                   SET SIZE(noOfRecords) OF VuDownloadablePeriod
}
```

**recordType** указывает на тип записи (VuDownloadablePeriod). **Присвоение значения:** см. RecordType

**recordSize** – размер VuDownloadablePeriod в байтах.

**noOfRecords** – число записей в массиве.

**records** – массив записей VuDownloadablePeriod.

## 2.195. *VuDownloadActivityData*

Информация, записанная в бортовом устройстве, которая относится к последней загрузке (приложение 1B, требование 105 и приложение 1C, требование 129).

Первое поколение:

```
VuDownloadActivityData ::= SEQUENCE {
    downloadingTime          TimeReal,
    fullCardNumber           FullCardNumber,
    companyOrWorkshopName    Name
}
```

**downloadingTime** – дата и время загрузки.

**fullCardNumber** – идентификатор использованной карточки, разрешающей загрузку.

**companyOrWorkshopName** – название предприятия или мастерской.

Второе поколение:

```
VuDownloadActivityData ::= SEQUENCE {  
    downloadingTime           TimeReal,  
    fullCardNumberAndGeneration FullCardNumberAndGeneration,  
    companyOrWorkshopName     Name  
}
```

Вместо fullCardNumber в структуре данных второго поколения используется следующий элемент данных.

**fullCardNumberAndGeneration** – идентификатор использованной карточки, разрешающей загрузку, и её поколения.

## 2.196. *VuDownloadActivityDataRecordArray*

Второе поколение:

Информация, связанная с последней загрузкой данных с БУ (приложение 1С, требование 129).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {  
    recordType           RecordType,  
    recordSize           INTEGER(1..65535),  
    noOfRecords          INTEGER(0..65535),  
    records              SET SIZE(noOfRecords) OF VuDownloadActivityData  
}
```

**recordType** указывает на тип записи (VuDownloadActivityData). **Присвоение значения:** см. RecordType

**recordSize** – размер VuDownloadActivityData в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей действий загрузки данных.

## 2.197. *VuEventData*

Первое поколение:

Информация, записанная в бортовом устройстве, связанная с событиями (приложение 1В, требование 094, кроме события превышения скорости).

```
VuEventData ::= SEQUENCE {  
    noOfVuEvents          INTEGER(0..255),  
    vuEventRecords       SET SIZE(noOfVuEvents) OF VuEventRecord  
}
```

**noOfVuEvents** – число событий, перечисленных в совокупности vuEventRecords.

**vuEventRecords** – массив записей о событиях.

## 2.198. VuEventRecord

Информация, записанная в бортовом устройстве, связанная с событием (приложение 1B, требование 094 и приложение 1C, требование 117, кроме события превышения скорости).

Первое поколение:

```
VuEventRecord ::= SEQUENCE {
    eventType                EventFaultType,
    eventRecordPurpose      EventFaultRecordPurpose,
    eventBeginTime          TimeReal,
    eventEndTime            TimeReal,
    cardNumberDriverSlotBegin FullCardNumber,
    cardNumberCodriverSlotBegin FullCardNumber,
    cardNumberDriverSlotEnd FullCardNumber,
    cardNumberCodriverSlotEnd FullCardNumber,
    similarEventsNumber     SimilarEventsNumber
}
```

**eventType** – тип события.

**eventRecordPurpose** – цель регистрации данного события.

**eventBeginTime** – дата и время начала события.

**eventEndTime** – дата и время завершения 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 аналогичных событий за указанный день.

Эта последовательность может быть использована для всех событий, помимо случаев превышения скорости.

Второе поколение:

```
VuEventRecord ::= SEQUENCE {
    eventType                EventFaultType,
    eventRecordPurpose      EventFaultRecordPurpose,
    eventBeginTime          TimeReal,
    eventEndTime            TimeReal,
    cardNumberAndGenDriverSlotBegin FullCardNumberAndGeneration,
    cardNumberAndGenCodriverSlotBegin FullCardNumberAndGeneration,
    cardNumberAndGenDriverSlotEnd FullCardNumberAndGeneration,
    cardNumberAndGenCodriverSlotEnd FullCardNumberAndGeneration,
    similarEventsNumber     SimilarEventsNumber,
    manufacturerSpecificEventFaultData ManufacturerSpecificEventFaultData
}
```

В дополнение к первому поколению, используются следующие элементы данных:

**manufacturerSpecificEventFaultData** содержит дополнительную информацию, связанную с конкретным производителем, о событии.

Вместо **cardNumberDriverSlotBegin**, **cardNumberCodriverSlotBegin**, **cardNumberDriverSlotEnd** и **cardNumberCodriverSlotEnd** в структуре данных второго поколения используются следующие элементы данных:

**cardNumberAndGenDriverSlotBegin** – идентификатор карточки, вставленной в считывающее устройство водителя в начале события, и её поколения.

**cardNumberAndGenCodriverSlotBegin** – идентификатор карточки, вставленной в считывающее устройство второго водителя в начале события, и её поколения.

**cardNumberAndGenDriverSlotEnd** – идентификатор карточки, вставленной в считывающее устройство водителя в конце события, и её поколения.

**cardNumberAndGenCodriverSlotEnd** – идентификатор карточки, вставленной в считывающее устройство второго водителя в конце события, и её поколения.

Если событие представляет собой нестыковку во времени, **eventBeginTime** и **eventEndTime** следует толковать следующим образом:

**eventBeginTime** – дата и время в записывающем оборудовании.

**eventEndTime** – дата и время по ГНСС.

## 2.199. *VuEventRecordArray*

Второе поколение:

Информация, записанная в бортовом устройстве, связанная с событиями (приложение 1С, требование 117, кроме события превышения скорости).

```
VuEventRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize          INTEGER(1..65535),
    noOfRecords         INTEGER(0..65535),
    records             SET SIZE(noOfRecords) OF VuEventRecord
}
```

**recordType** указывает на тип записи (*VuEventRecord*). **Присвоение значения:** см. *RecordType*

**recordSize** – размер *VuEventRecord* в байтах.

**noOfRecords** – число записей в массиве.

**records** – массив записей о событиях.

## 2.200. *VuFaultData*

Первое поколение:

Информация, записанная в бортовом устройстве, которая относится к неисправностям (приложение 1B, требование 096).

```
VuFaultData ::= SEQUENCE {
    noOfVuFaults          INTEGER(0..255),
    vuFaultRecords        SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

**noOfVuFaults** – число неисправностей, перечисленных в совокупности **vuFaultRecords**.

**vuFaultRecords** – массив записей о неисправностях.

## 2.201. *VuFaultRecord*

Информация, записанная в бортовом устройстве, которая относится к неисправности (приложение 1B, требование 096 и приложение 1C, требование 118).

Первое поколение:

```
VuFaultRecord ::= SEQUENCE {
    faultType              EventFaultType,
    faultRecordPurpose     EventFaultRecordPurpose,
    faultBeginTime         TimeReal,
    faultEndTime           TimeReal,
    cardNumberDriverSlotBegin FullCardNumber,
    cardNumberCodriverSlotBegin FullCardNumber,
    cardNumberDriverSlotEnd FullCardNumber,
    cardNumberCodriverSlotEnd FullCardNumber
}
```

**faultType** – тип неисправности записывающего оборудования.

**faultRecordPurpose** – цель регистрации данной неисправности.

**faultBeginTime** – дата и время начала неисправности.

**faultEndTime** – дата и время окончания неисправности.

**cardNumberDriverSlotBegin** – идентификатор карточки, вставленной в считывающее устройство водителя в начале неисправности.

**cardNumberCodriverSlotBegin** – идентификатор карточки, вставленной в считывающее устройство второго водителя в начале неисправности.

**cardNumberDriverSlotEnd** – идентификатор карточки, вставленной в считывающее устройство водителя в конце неисправности.

**cardNumberCodriverSlotEnd** – идентификатор карточки, вставленной в считывающее устройство второго водителя в конце неисправности.

Второе поколение:

```

VuFaultRecord ::= SEQUENCE {
    faultType                EventFaultType,
    faultRecordPurpose       EventFaultRecordPurpose,
    faultBeginTime           TimeReal,
    faultEndTime             TimeReal,
    cardNumberAndGenDriverSlotBegin FullCardNumberAndGeneration,
    cardNumberAndGenCodriverSlotBegin FullCardNumberAndGeneration,
    cardNumberAndGenDriverSlotEnd FullCardNumberAndGeneration,
    cardNumberAndGenCodriverSlotEnd FullCardNumberAndGeneration,
    manufacturerSpecificEventFaultData ManufacturerSpecificEventFaultData
}

```

В дополнение к первому поколению, используется следующий элемент данных:

**manufacturerSpecificEventFaultData** содержит дополнительную информацию, связанную с конкретным производителем, о неисправности.

Вместо **cardNumberDriverSlotBegin**, **cardNumberCodriverSlotBegin**, **cardNumberDriverSlotEnd** и **cardNumberCodriverSlotEnd** в структуре данных второго поколения используются следующие элементы данных:

**cardNumberAndGenDriverSlotBegin** – идентификатор карточки, вставленной в считывающее устройство водителя в начале неисправности, и её поколения.

**cardNumberAndGenCodriverSlotBegin** – идентификатор карточки, вставленной в считывающее устройство второго водителя в начале неисправности, и её поколения.

**cardNumberAndGenDriverSlotEnd** – идентификатор карточки, вставленной в считывающее устройство водителя в конце неисправности, и её поколения.

**cardNumberAndGenCodriverSlotEnd** – идентификатор карточки, вставленной в считывающее устройство второго водителя в конце неисправности, и её поколения.

## 2.202. VuFaultRecordArray

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к неисправностям (приложение 1С, требование 118).

```

VuFaultRecordArray ::= SEQUENCE {
    recordType                RecordType,
    recordSize                INTEGER(1..65535),
    noOfRecords               INTEGER(0..65535),
    records                   SET SIZE(noOfRecords) OF VuFaultRecord
}

```

**recordType** указывает на тип записи (VuFaultRecord). **Присвоение значения:** см. RecordType

**recordSize** – размер VuFaultRecord в байтах.

**noOfRecords** – число записей в массиве.

**records** – массив записей о неисправностях.

## 2.203. VuGNSSCDRecord

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к местоположению транспортного средства по ГНСС, если непрерывное время управления водителем достигает значения, кратного трём часам (приложение 1С, требования 108, 110).



```

VuGNSSCDRecord ::= SEQUENCE {
    timeStamp                TimeReal,
    cardNumberAndGenDriverSlot FullCardNumberAndGeneration,
    cardNumberAndGenCodriverSlot FullCardNumberAndGeneration,
    gnssPlaceRecord         GNSSPlaceRecord
}

```

**timeStamp** – дата и время, когда непрерывное время управления владельцем карточки достигает значения, кратного трём часам.

**cardNumberAndGenDriverSlot** – идентификатор карточки, вставленной в считывающее устройство водителя, и её поколения.

**cardNumberAndGenCodriverSlot** – идентификатор карточки, вставленной в считывающее устройство второго водителя, и её поколения.

**gnssPlaceRecord** содержит информацию, связанную с местоположением транспортного средства.

## 2.204. VuGNSSCDRecordArray

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к местоположению транспортного средства по ГНСС, если непрерывное время управления водителем достигает значения, кратного трём часам (приложение 1С, требования 108 и 110).

```

VuGNSSCDRecordArray ::= SEQUENCE {
    recordType                RecordType,
    recordSize                INTEGER(1..65535),
    noOfRecords              INTEGER(0..65535),
    records                   SET SIZE(noOfRecords) OF VuGNSSCDRecord
}

```

**recordType** указывает на тип записи (VuGNSSCDRecord). **Присвоение значения:** см. RecordType

**recordSize** – размер VuGNSSCDRecord в байтах.

**noOfRecords** – число записей в массиве.

**records** – массив записей о непрерывном управлении по ГНСС.

## 2.205. VuIdentification

Информация, записанная в бортовом устройстве, которая относится к идентификации бортового устройства (приложение 1В, требование 075 и приложение 1С, требования 93 и 121).

Первое поколение:

```

VuIdentification ::= SEQUENCE {
    vuManufacturerName       VuManufacturerName,
    vuManufacturerAddress    VuManufacturerAddress,
    vuPartNumber             VuPartNumber,
    vuSerialNumber           VuSerialNumber,
    vuSoftwareIdentification VuSoftwareIdentification,
    vuManufacturingDate      VuManufacturingDate,
    vuApprovalNumber         VuApprovalNumber
}

```

**vuManufacturerName** – название производителя бортового устройства.

**vuManufacturerAddress** – адрес производителя бортового устройства.

**vuPartNumber** – номер детали бортового устройства.

**vuSerialNumber** – серийный номер бортового устройства.

**vuSoftwareIdentification** позволяет идентифицировать программное обеспечение, установленное в бортовом устройстве.

**vuManufacturingDate** – дата изготовления бортового устройства.

**vuApprovalNumber** – номер официального утверждения типа бортового устройства.

Второе поколение:

```
VuIdentification ::= SEQUENCE {
    vuManufacturerName          VuManufacturerName,
    vuManufacturerAddress      VuManufacturerAddress,
    vuPartNumber               VuPartNumber,
    vuSerialNumber             VuSerialNumber,
    vuSoftwareIdentification   VuSoftwareIdentification,
    vuManufacturingDate       VuManufacturingDate,
    vuApprovalNumber          VuApprovalNumber,
    vuGeneration               Generation,
    vuAbility                   VuAbility
}
```

В дополнение к первому поколению, используются следующие элементы данных:

**vuGeneration** идентифицирует поколение бортового устройства.

**vuAbility** предоставляет информацию о том, поддерживает ли БУ карточки тахографов первого поколения или нет.

## 2.206. VuIdentificationRecordArray

Второе поколение:

VuIdentification и метаданные, используемые в протоколе загрузки.

```
VuIdentificationRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize         INTEGER(1..65535),
    noOfRecords        INTEGER(0..65535),
    records             SET SIZE(noOfRecords) OF VuIdentification
}
```

**recordType** указывает на тип записи (VuIdentification). **Присвоение значения:** см. RecordType

**recordSize** – размер VuIdentification в байтах.

**noOfRecords** – число записей в массиве.

**records** – массив записей VuIdentification.

## 2.207. VuITSConsentRecord

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к согласию водителя на пользование интеллектуальными транспортными системами.

```
VuITSConsentRecord ::= SEQUENCE {
    cardNumberAndGen          FullCardNumberAndGeneration,
    consent                    BOOLEAN
}
```

**cardNumberAndGen** позволяет идентифицировать карточку и её поколение. Это должна быть карточка водителя или карточка мастерской.

**consent** —это метка, указывающая на то, дал ли водитель своё согласие на пользование интеллектуальными транспортными системами на своём транспортном средстве/бортовом устройстве.

**Присвоение значения:**

TRUE означает согласие водителя на пользование интеллектуальными транспортными системами

FALSE означает несогласие водителя на пользование интеллектуальными транспортными системами

## 2.208. *VuITSConsentRecordArray*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к согласию на пользование интеллектуальными транспортными системами (приложение 1С, требование 200).

```
VuITSConsentRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize          INTEGER(1..65535),
    noOfRecords         INTEGER(0..65535),
    records              SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

**recordType** указывает на тип записи (VuITSConsentRecord). **Присвоение значения:** см. RecordType

**recordSize** – размер VuITSConsentRecord в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей о согласии на ИТС.

## 2.209. *VuManufacturerAddress*

Адрес производителя бортового устройства.

```
VuManufacturerAddress ::= Address
```

**Присвоение значения:** Не указано.

## 2.210. *VuManufacturerName*

Название производителя бортового устройства.

```
VuManufacturerName ::= Name
```

**Присвоение значения:** Не указано.

## 2.211. *VuManufacturingDate*

Дата изготовления бортового устройства.

```
VuManufacturingDate ::= TimeReal
```

**Присвоение значения:** Не указано.

## 2.212. *VuOverSpeedingControlData*

Информация, записанная в бортовом устройстве, которая относится к событиям превышения скорости с момента последнего контроля (приложение 1B, требование 095 и приложение 1C, требование 117).

```
VuOverSpeedingControlData ::= SEQUENCE {
    lastOverspeedControlTime      TimeReal,
    firstOverspeedSince           TimeReal,
    numberOfOverspeedSince        OverspeedNumber
}
```

**lastOverspeedControlTime** – дата и время последнего контроля за превышением скорости.

**firstOverspeedSince** – дата и время первого превышения скорости после данного контроля за превышением скорости.

**numberOfOverspeedSince** – число случаев превышения скорости после последнего контроля за превышением скорости.

## 2.213. *VuOverSpeedingControlDataRecordArray*

Второе поколение:

*VuOverSpeedingControlData* и метаданные, используемые в протоколе загрузки.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
    recordType                    RecordType,
    recordSize                    INTEGER(1..65535),
    noOfRecords                   INTEGER(0..65535),
    records                       SET SIZE(noOfRecords) OF VuOverSpeedingControlData
}
```

**recordType** указывает на тип записи (*VuOverSpeedingControlData*). **Присвоение значения:** см. *RecordType*

**recordSize** – размер *VuOverSpeedingControlData* в байтах.

**noOfRecords** – число записей в массиве.

**records** – массив записей данных контроля за превышением скорости.

## 2.214. *VuOverSpeedingEventData*

Первое поколение:

Информация, записанная в бортовом устройстве, которая относится к событиям превышения скорости (приложение 1B, требование 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
    noOfVuOverSpeedingEvents      INTEGER(0..255),
    vuOverSpeedingEventRecords    SET SIZE(noOfVuOverSpeedingEvents) OF
                                   VuOverSpeedingEventRecord
}
```

**noOfVuOverSpeedingEvents** – число событий, перечисленных в совокупности *vuOverSpeedingEventRecords*.

**vuOverSpeedingEventRecords** – совокупность записей о событиях превышения скорости.

## 2.215. *VuOverSpeedingEventRecord*

Первое поколение:

Информация, записанная в бортовом устройстве, которая относится к событиям превышения скорости (приложение 1B, требование 094 и приложение 1C, требование 117).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
    eventType                EventFaultType,
    eventRecordPurpose       EventFaultRecordPurpose,
    eventBeginTime           TimeReal,
    eventEndTime             TimeReal,
    maxSpeedValue            SpeedMax,
    averageSpeedValue        SpeedAverage,
    cardNumberDriverSlotBegin FullCardNumber,
    similarEventsNumber      SimilarEventsNumber
}
```

**eventType** – тип события.

**eventRecordPurpose** – цель регистрации данного события.

**eventBeginTime** – дата и время начала события.

**eventEndTime** – дата и время завершения события.

**maxSpeedValue** – максимальная скорость, измеренная во время события.

**averageSpeedValue** – средняя арифметическая скорость, измеренная во время события.

**cardNumberDriverSlotBegin** – идентификатор карточки, вставленной в считывающее устройство водителя в начале события.

**similarEventsNumber** – число аналогичных событий за указанный день.

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к событиям превышения скорости (приложение 1B, требование 094 и приложение 1C, требование 117).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
    eventType                EventFaultType,
    eventRecordPurpose       EventFaultRecordPurpose,
    eventBeginTime           TimeReal,
    eventEndTime             TimeReal,
    maxSpeedValue            SpeedMax,
    averageSpeedValue        SpeedAverage,
    cardNumberAndGenDriverSlotBegin FullCardNumberAndGeneration,
    similarEventsNumber      SimilarEventsNumber
}
```

Вместо **cardNumberDriverSlotBegin** в структуре данных второго поколения используется следующий элемент данных:

**cardNumberAndGenDriverSlotBegin** – идентификатор карточки, вставленной в считывающее устройство водителя в начале события, и её поколения.

## 2.216. *VuOverSpeedingEventRecordArray*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к событиям превышения скорости (приложение 1С, требование 117).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize          INTEGER(1..65535),
    noOfRecords         INTEGER(0..65535),
    records             SET SIZE(noOfRecords) OF VuOverSpeedingEventRecord
}
```

**recordType** указывает на тип записи (VuOverSpeedingEventRecord). **Присвоение значения:** см. RecordType

**recordSize** – размер VuOverSpeedingEventRecord в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей о событиях превышения скорости.

## 2.217. VuPartNumber

Номер детали бортового устройства.

```
VuPartNumber ::= IA5String(SIZE(16))
```

**Присвоение значения:** Относится конкретно к производителю БУ.

## 2.218. VuPlaceDailyWorkPeriodData

Первое поколение:

Информация, записанная в бортовом устройстве, которая относится к местам, где водители начинают или заканчивают дневной период работы (приложение 1В, требование 087 и приложение 1С, требования 108 и 110).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
    noOfPlaceRecords    INTEGER(0..255),
    vuPlaceDailyWorkPeriodRecords
                        SET SIZE(noOfPlaceRecords) OF
                        VuPlaceDailyWorkPeriodRecord
}
```

**noOfPlaceRecords** – число событий, перечисленных в совокупности vuPlaceDailyWorkPeriodRecords.

**vuPlaceDailyWorkPeriodRecords** – совокупность записей о местах.

## 2.219. VuPlaceDailyWorkPeriodRecord

Первое поколение:

Информация, записанная в бортовом устройстве, которая относится к месту, где водитель начинает или заканчивает дневной период работы (приложение 1В, требование 087 и приложение 1С, требования 108 и 110).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
    fullCardNumber      FullCardNumber,
    placeRecord         PlaceRecord
}
```

**fullCardNumber** – тип карточки водителя, государство-член, выдавшее карточку, и номер карточки.

**placeRecord** содержит информацию, связанную с местом ввода.

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к месту, где водитель начинает или заканчивает дневной период работы (приложение 1B, требование 087 и приложение 1C, требования 108 и 110).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
    fullCardNumberAndGeneration    FullCardNumberAndGeneration,
    placeRecord                    PlaceRecord
}
```

Вместо fullCardNumber в структуре данных второго поколения используется следующий элемент данных:

**fullCardNumberAndGeneration** – тип карточки, выдавшее её государство-член и номер и поколение карточки, записанные на карточке.

## 2.220. *VuPlaceDailyWorkPeriodRecordArray*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к местам, где водители начинают или заканчивают дневной период работы (приложение 1C, требования 108 и 110).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
    recordType                    RecordType,
    recordSize                    INTEGER(1..65535),
    noOfRecords                  INTEGER(0..65535),
    records                      SET SIZE(noOfRecords) OF VuPlaceDailyWorkPeriodRecord
}
```

**recordType** указывает на тип записи (VuPlaceDailyWorkPeriodRecord). **Присвоение значения:** см. RecordType

**recordSize** – размер VuPlaceDailyWorkPeriodRecord в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей о местах.

### **2.221. VuPrivateKey**

Первое поколение:

Закрытый ключ бортового устройства.

VuPrivateKey ::= RSAKeyPrivateExponent

### **2.222. VuPublicKey**

Первое поколение:

Открытый ключ бортового устройства.

VuPublicKey ::= PublicKey

### **2.223. VuSerialNumber**

Серийный номер бортового устройства (приложение 1B, требование 075 и приложение 1C, требование 93).

VuSerialNumber ::= ExtendedSerialNumber

### **2.224. VuSoftInstallationDate**

Дата установки программного обеспечения бортового устройства.

VuSoftInstallationDate ::= TimeReal

**Присвоение значения:** Не указано.

### **2.225. VuSoftwareIdentification**

Информация, записанная в бортовом устройстве, которая относится к установленному программному обеспечению.

```
VuSoftwareIdentification ::= SEQUENCE {  
    vuSoftwareVersion          VuSoftwareVersion,  
    vuSoftInstallationDate     VuSoftInstallationDate  
}
```

**vuSoftwareVersion** – номер версии программного обеспечения бортового устройства.

**vuSoftInstallationDate** – дата установки версии программного обеспечения.

### **2.226. VuSoftwareVersion**

Номер версии программного обеспечения бортового устройства.

VuSoftwareVersion ::= IA5String(SIZE(4))

**Присвоение значения:** Не указано.

### **2.227. VuSpecificConditionData**

Первое поколение:

Информация, записанная в бортовом устройстве, которая относится к особым условиям.

```
VuSpecificConditionData ::= SEQUENCE {  
    noOfSpecificConditionRecords    INTEGER(0..216-1)  
    specificConditionRecords        SET SIZE (noOfSpecificConditionRecords) OF  
                                     SpecificConditionRecord  
}
```



**noOfSpecificConditionRecords** – число записей, перечисленных в совокупности specificConditionRecords.

**specificConditionRecords** – совокупность записей об особых условиях.

## 2.228. *VuSpecificConditionRecordArray*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к особым условиям (приложение 1С, требование 130).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize          INTEGER(1..65535),
    noOfRecords         INTEGER(0..65535),
    records             SET SIZE(noOfRecords) OF SpecificConditionRecord
}
```

**recordType** указывает на тип записи (SpecificConditionRecord). **Присвоение значения:** см. RecordType

**recordSize** – размер SpecificConditionRecord в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей об особых условиях.

## 2.229. *VuTimeAdjustmentData*

Первое поколение:

Информация, записанная в бортовом устройстве, которая относится к корректировке времени, не связанной с регулярной калибровкой (приложение 1В, требование 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
    noOfVuTimeAdjRecords    INTEGER(0..6),
    vuTimeAdjustmentRecords SET SIZE(noOfVuTimeAdjRecords) OF
                            VuTimeAdjustmentRecord
}
```

**noOfVuTimeAdjRecords** – число записей в vuTimeAdjustmentRecords.

**vuTimeAdjustmentRecords** – совокупность записей о корректировках времени.

## 2.230. *VuTimeAdjustmentGNSSRecord*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к корректировке времени на основании данных времени по ГНСС (приложение 1С, требования 124 и 125).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {  
    oldTimeValue          TimeReal,  
    newTimeValue          TimeReal  
}
```

**oldTimeValue, newTimeValue** – старые и новые значения даты и времени.

## 2.231. *VuTimeAdjustmentGNSSRecordArray*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к корректировке времени на основании данных времени по ГНСС (приложение 1С, требования 124 и 125).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {  
    recordType            RecordType,  
    recordSize            INTEGER(1..65535),  
    noOfRecords           INTEGER(0..65535),  
    records                SET SIZE(noOfRecords) OF VuTimeAdjustmentGNSSRecord  
}
```

**recordType** указывает на тип записи (VuTimeAdjustmentGNSSRecord). **Присвоение значения:** см. RecordType

**recordSize** – размер VuTimeAdjustmentGNSSRecord в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей о корректировке времени по ГНСС.

## 2.232. *VuTimeAdjustmentRecord*

Информация, записанная в бортовом устройстве, которая относится к корректировке времени, не связанной с регулярной калибровкой (приложение 1В, требование 101 и приложение 1С, требования 124 и 125).

Первое поколение:

```
VuTimeAdjustmentRecord ::= SEQUENCE {  
    oldTimeValue          TimeReal,  
    newTimeValue          TimeReal,  
    workshopName          Name,  
    workshopAddress       Address,  
    workshopCardNumber    FullCardNumber  
}
```

**oldTimeValue, newTimeValue** – старые и новые значения даты и времени.

**workshopName, workshopAddress** – название и адрес мастерской.

**workshopCardNumber** – идентификатор карточки мастерской, используемой для корректировки времени.

Второе поколение:

```

VuTimeAdjustmentRecord ::= SEQUENCE {
    oldTimeValue           TimeReal,
    newTimeValue           TimeReal,
    workshopName           Name,
    workshopAddress        Address,
    workshopCardNumberAndGeneration FullCardNumberAndGeneration
}

```

Вместо `workshopCardNumber` в структуре данных второго поколения используется следующий элемент данных.

**workshopCardNumberAndGeneration** – идентификатор карточки мастерской, используемой для корректировки времени, и её поколения.

### 2.233. *VuTimeAdjustmentRecordArray*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к корректировке времени, не связанной с регулярной калибровкой (приложение 1С, требования 124 и 125).

```

VuTimeAdjustmentRecordArray ::= SEQUENCE {
    recordType             RecordType,
    recordSize             INTEGER(1..65535),
    noOfRecords           INTEGER(0..65535),
    records                SET SIZE(noOfRecords) OF VuTimeAdjustmentRecord
}

```

**recordType** указывает на тип записи (`VuTimeAdjustmentRecord`). **Присвоение значения:** см. `RecordType`

**recordSize** – размер `VuTimeAdjustmentRecord` в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей о корректировке времени.

## 2.234. *WorkshopCardApplicationIdentification*

Информация, записанная на карточке мастерской, которая относится к идентификации приложения карточки (приложение 1С, требования 307 и 330).

Первое поколение:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId      EquipmentType,
    cardStructureVersion         CardStructureVersion,
    noOfEventsPerType           NoOfEventsPerType,
    noOfFaultsPerType           NoOfFaultsPerType,
    activityStructureLength      CardActivityLengthRange,
    noOfCardVehicleRecords      NoOfCardVehicleRecords,
    noOfCardPlaceRecords        NoOfCardPlaceRecords,
    noOfCalibrationRecords      NoOfCalibrationRecords
}
```

**typeOfTachographCardId** уточняет реализованный 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 транспортном средстве, которые могут храниться на карточке.

**noOfCardPlaceRecords** – число записей о местах, которые могут храниться на карточке.

**noOfCalibrationRecords** – число записей о калибровке, которые могут храниться на карточке.

Второе поколение:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId      EquipmentType,
    cardStructureVersion         CardStructureVersion,
    noOfEventsPerType           NoOfEventsPerType,
    noOfFaultsPerType           NoOfFaultsPerType,
    activityStructureLength      CardActivityLengthRange,
    noOfCardVehicleRecords      NoOfCardVehicleRecords,
    noOfCardPlaceRecords        NoOfCardPlaceRecords,
    noOfCalibrationRecords      NoOfCalibrationRecords,
    noOfGNSSCDRecords          NoOfGNSSCDRecords,
    noOfSpecificConditionRecords NoOfSpecificConditionRecords
}
```

В дополнение к первому поколению, используются следующие элементы данных:

**noOfGNSSCDRecords** – число записей о непрерывном времени управления по ГНСС, которые могут храниться на карточке.

**noOfSpecificConditionRecords** – число записей об особых условиях, которые могут храниться на карточке.

## 2.235. *WorkshopCardCalibrationData*

Информация, записанная на карточке мастерской, которая относится к действиям мастерской, проводимым с карточкой (приложение 1С, требования 314, 316, 337 и 339).

```
WorkshopCardCalibrationData ::= SEQUENCE {
    calibrationTotalNumber      INTEGER(0 .. 216-1),
    calibrationPointerNewestRecord INTEGER(0 .. NoOfCalibrationRecords-1),
    calibrationRecords          SET SIZE(NoOfCalibrationRecords) OF
                                WorkshopCardCalibrationRecord
}
```

**calibrationTotalNumber** – общее число калибровок, произведённых с карточкой.

**calibrationPointerNewestRecord** – индекс последней обновлённой записи данных о калибровке.

**Присвоение значения:** Число, соответствующее числовому показателю записи данных о калибровке, которое начинается с 0 в случае первой регистрации записей, касающихся калибровки, в структуре.

**calibrationRecords** – массив данных с записями, содержащими данные о калибровке и/или корректировке времени.

## 2.236. *WorkshopCardCalibrationRecord*

Информация, записанная на карточке мастерской, которая относится к калибровке, проводимой с карточкой (приложение 1С, требования 314 и 337).

Первое поколение:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
    calibrationPurpose           CalibrationPurpose,
    vehicleIdentificationNumber  VehicleIdentificationNumber,
    vehicleRegistration          VehicleRegistrationIdentification,
    wVehicleCharacteristicConstant W-VehicleCharacteristicConstant,
    kConstantOfRecordingEquipment K-ConstantOfRecordingEquipment,
    lTyreCircumference          L-TyreCircumference,
    tyreSize                    TyreSize,
    authorisedSpeed              SpeedAuthorised,
    oldOdometerValue            OdometerShort,
    newOdometerValue            OdometerShort,
    oldTimeValue                TimeReal,
    newTimeValue                TimeReal,
    nextCalibrationDate         TimeReal,
    vuPartNumber                VuPartNumber,
    vuSerialNumber              VuSerialNumber,
    sensorSerialNumber          SensorSerialNumber
}
```

**calibrationPurpose** – цель калибровки.

**vehicleIdentificationNumber** – идентификационный номер транспортного средства (VIN).

**vehicleRegistration** содержит VRN и государство-член регистрации.

**wVehicleCharacteristicConstant** – характеристический коэффициент транспортного средства.

**kConstantOfRecordingEquipment** – постоянная величина записывающего оборудования.

**lTyreCircumference** – фактическая окружность шин колёс.

**tyreSize** – обозначение габаритов шин транспортного средства..

**authorisedSpeed** – максимальная допустимая скорость транспортного средства.

**oldOdometerValue, newOdometerValue** – старые и новые показания одометра.

**oldTimeValue, newTimeValue** – старые и новые значения даты и времени.

**nextCalibrationDate** – дата следующей калибровки типа, указанного в CalibrationPurpose, которую должен провести компетентный инспекционный орган.

**vuPartNumber, vuSerialNumber** и **sensorSerialNumber** – элементы данных для идентификации записывающего оборудования.

Второе поколение:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
    calibrationPurpose           CalibrationPurpose,
    vehicleIdentificationNumber  VehicleIdentificationNumber,
    vehicleRegistration          VehicleRegistrationIdentification,
    wVehicleCharacteristicConstant W-VehicleCharacteristicConstant,
    kConstantOfRecordingEquipment K-ConstantOfRecordingEquipment,
    lTyreCircumference          L-TyreCircumference,
    tyreSize                     TyreSize,
    authorisedSpeed              SpeedAuthorised,
    oldOdometerValue            OdometerShort,
    newOdometerValue            OdometerShort,
    oldTimeValue                 TimeReal,
    newTimeValue                 TimeReal,
    nextCalibrationDate          TimeReal,
    vuPartNumber                 VuPartNumber,
    vuSerialNumber               VuSerialNumber,
    sensorSerialNumber           SensorSerialNumber,
    sensorGNSSSerialNumber       SensorGNSSSerialNumber,
    rcmSerialNumber              RemoteCommunicationModuleSerialNumber,
    sealDataCard                 SealDataCard
}
```

В дополнение к первому поколению, используются следующие элементы данных:

**sensorGNSSSerialNumber** позволяет идентифицировать внешнее устройство ГНСС.

**rcmSerialNumber** позволяет идентифицировать модуль удалённой связи.

**sealDataCard** предоставляет информацию о пломбах, наложенных на различные компоненты транспортного средства.

## 2.237. *WorkshopCardHolderIdentification*

Информация, записанная на карточке мастерской, которая относится к идентификации владельца карточки (приложение 1С, требования 311 и 334).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
    workshopName           Name,
    workshopAddress        Address,
    cardHolderName         HolderName,
    cardHolderPreferredLanguage Language
}
```

**workshopName** – название мастерской владельца карточки.

**workshopAddress** – адрес мастерской владельца карточки.

**cardHolderName** – фамилия и имя (имена) владельца (например, фамилия и имя механика).

**cardHolderPreferredLanguage** – предпочитаемый язык владельца карточки.

## 2.238. *WorkshopCardPIN*

Персональный идентификационный номер карточки мастерской (приложение 1С, требования 309 и 332).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

**Присвоение значения:** Известный ПИН-код владельца карточки, за которым следует серия байтов ‘FF’ (до восьми байтов).

## 2.239. *W-VehicleCharacteristicConstant*

Характеристический коэффициент транспортного средства (определение k).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..216-1)
```

**Присвоение значения:** Импульсы на километр в рабочем диапазоне от 0 до 64 255 имп./км.

## 2.240. *VuPowerSupplyInterruptionRecord*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к событиям прекращения электропитания (приложение 1С, требование 117).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
    eventType                EventFaultType,
    eventRecordPurpose      EventFaultRecordPurpose,
    eventBeginTime          TimeReal,
    eventEndTime            TimeReal,
    cardNumberAndGenDriverSlotBegin FullCardNumberAndGeneration,
    cardNumberAndGenDriverSlotEnd   FullCardNumberAndGeneration,
    cardNumberAndGenCodriverSlotBegin FullCardNumberAndGeneration,
    cardNumberAndGenCodriverSlotEnd FullCardNumberAndGeneration,
    similarEventsNumber      SimilarEventsNumber
}
```

**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 её поколения.

**cardNumberAndGenDriverSlotEnd** – идентификатор карточки, вставленной в считывающее устройство водителя в конце события, и её поколения.

**cardNumberAndGenCodriverSlotBegin** – идентификатор карточки, вставленной в считывающее устройство второго водителя в начале события, и её поколения.

**cardNumberAndGenCodriverSlotEnd** – идентификатор карточки, вставленной в считывающее устройство второго водителя в конце события, и её поколения.

**similarEventsNumber** – число аналогичных событий за указанный день.

## 2.241. *VuPowerSupplyInterruptionRecordArray*

Второе поколение:

Информация, записанная в бортовом устройстве, которая относится к событиям прекращения электропитания (приложение 1С, требование 117).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
    recordType      RecordType,
    recordSize      INTEGER(1..65535),
    noOfRecords     INTEGER(0..65535),
    records         SET SIZE(noOfRecords) OF VuPowerSupplyInterruptionRecord
}
```

**recordType** указывает на тип записи (*VuPowerSupplyInterruptionRecord*). **Присвоение значения:** см. *RecordType*

**recordSize** – размер *VuPowerSupplyInterruptionRecord* в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей о событиях прекращения электропитания.



## 2.242. *VuSensorExternalGNSSCoupledRecordArray*

Второе поколение:

Совокупность *SensorExternalGNSSCoupledRecord* и метаданные, используемые в протоколе загрузки.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize          INTEGER(1..65535),
    noOfRecords         INTEGER(0..65535),
    records             SET SIZE(noOfRecords) OF SensorExternalGNSSCoupledRecord
}
```

**recordType** указывает на тип записи (*SensorExternalGNSSCoupledRecord*). **Присвоение значения:** см. *RecordType*

**recordSize** – размер *SensorExternalGNSSCoupledRecord* в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей *SensorExternalGNSSCoupledRecord*.

## 2.243. *VuSensorPairedRecordArray*

Второе поколение:

Совокупность *SensorPairedRecord* и метаданные, используемые в протоколе загрузки.

```
VuSensorPairedRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize          INTEGER(1..65535),
    noOfRecords         INTEGER(0..65535),
    records             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

**recordType** указывает на тип записи (*SensorPairedRecord*). **Присвоение значения:** см. *RecordType*

**recordSize** – размер *SensorPairedRecord* в байтах.

**noOfRecords** – число записей в массиве.

**records** – совокупность записей о соединениях датчика.

### 3. Определения диапазонов значений и размеров

Определение значений переменных, используемых для определений, содержащихся в пункте 2.

TimeRealRange ::= 2<sup>32</sup>-1

### 4. Наборы символов

В строках IA5 используются знаки ASCII, определённые 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 { | } ~ -

Другие строки символов (Address, Name, VehicleRegistrationNumber) дополнительно задействуют символы из спектра десятичных знаков 161 –255 следующих 8-битных стандартных наборов символов, указываемых по номеру кодовой страницы:	Кодовая страница (десятичная система)
Стандартный набор символов	
ISO/IEC 8859-1 латиница-1 Западная Европа	1
ISO/IEC 8859-2 латиница-2 Центральная Европа	2
ISO/IEC 8859-3 латиница-3 Южная Европа	3
ISO/IEC 8859-5 латиница/кириллица	5
ISO/IEC 8859-7 латиница/греческий алфавит	7
ISO/IEC 8859-9 латиница/турецкий алфавит	9
ISO/IEC 8859-13 латиница-7 Балтика	13
ISO/IEC 8859-15 латиница-9	15
ISO/IEC 8859-16 латиница-10 Восточная Европа	16
KOI8-R латиница/кириллица	80
KOI8-U латиница/кириллица	85

### 5. Кодировка

В случае кодирования по правилам кодирования ASN.1 все определённые типы данных кодируются в соответствии со стандартом ISO/IEC 8825-2 (согласованный вариант).

### 6. Идентификаторы объектов и приложений

#### 6.1. Идентификаторы объектов

Идентификаторы объектов (OID), указанные в настоящей главе, касаются только второго поколения. Эти OIDs представлены в TR-03110-3 и повторяются здесь для полноты. OID представлены в поддереве 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 проходить при помощи SHA-384, и в подобных случаях 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 – `0.4.0.127.0.7.2.2.2.2.4`.

	Точечная нотация	Байтовая нотация
<code>id-TA-ECDSA-SHA-256</code>	<code>0.4.0.127.0.7.2.2.2.2.3</code>	<code>'04 00 7F 00 07 02 02 02 03'</code>
<code>id-TA-ECDSA-SHA-384</code>	<code>0.4.0.127.0.7.2.2.2.2.4</code>	<code>'04 00 7F 00 07 02 02 02 04'</code>
<code>id-TA-ECDSA-SHA-512</code>	<code>0.4.0.127.0.7.2.2.2.2.5</code>	<code>'04 00 7F 00 07 02 02 02 05'</code>

#### Идентификаторы протокола аутентификации микросхемы

```
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 происходит при помощи алгоритма ECDH, и в результате получается ключ сеанса AES длиной 128 бит. Данный ключ сеанса впоследствии используется в рабочем режиме CBC для обеспечения конфиденциальности данных и с алгоритмом CMAC для обеспечения подлинности данных. Таким образом, идентификатор объекта, который следует применить, – (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
<code>id-CA-ECDH-AES-CBC-CMAC-128</code>	<code>0.4.0.127.0.7.2.2.3.2.2</code>	<code>'04 00 7F 00 07 02 02 03 02 02'</code>
<code>id-CA-ECDH-AES-CBC-CMAC-192</code>	<code>0.4.0.127.0.7.2.2.3.2.3</code>	<code>'04 00 7F 00 07 02 02 03 02 03'</code>
<code>id-CA-ECDH-AES-CBC-CMAC-256</code>	<code>0.4.0.127.0.7.2.2.3.2.4</code>	<code>'04 00 7F 00 07 02 02 03 02 04'</code>

## 6.2. Идентификаторы приложения

Второе поколение:

Идентификатор приложения (AID) для внешнего устройства ГНСС (второго поколения) происходит из `'FF 44 54 45 47 4D'`. Это собственный AID согласно ISO/IEC 7816-4.

Примечание: Последние 5 байтов кодируют DTEGM для внешнего устройства ГНСС «умных» тахографов.

Идентификатор приложения для приложения карточки тахографа второго поколения происходит из 'FF 53 4D 52 44 54'. Это собственный AID согласно ISO/IEC 7816-4.

**RU**

**Приложение 2. Спецификация карточек тахографов**

Дата: 02-02-2016

## СОДЕРЖАНИЕ

<b>1.</b>	<b>ВВЕДЕНИЕ .....</b>	<b>188</b>
<b>1.1.</b>	<b>Сокращения.....</b>	<b>188</b>
<b>1.2.</b>	<b>Ссылки .....</b>	<b>189</b>
<b>2.</b>	<b>ЭЛЕКТРИЧЕСКИЕ И ФИЗИЧЕСКИЕ ХАРАКТЕРИСТИКИ.....</b>	<b>189</b>
<b>2.1.</b>	<b>Напряжение питания и потребление тока.....</b>	<b>189</b>
<b>2.2.</b>	<b>Напряжение программирования <math>V_{pp}</math>.....</b>	<b>189</b>
<b>2.3.</b>	<b>Формирование и частота тактовых сигналов .....</b>	<b>189</b>
<b>2.4.</b>	<b>Контакт ввода/вывода.....</b>	<b>190</b>
<b>2.5.</b>	<b>Состояния карточки .....</b>	<b>190</b>
<b>3.</b>	<b>АППАРАТНОЕ ОБЕСПЕЧЕНИЕ И СВЯЗЬ .....</b>	<b>190</b>
<b>3.1.</b>	<b>Введение .....</b>	<b>190</b>
<b>3.2.</b>	<b>Протокол передачи данных.....</b>	<b>190</b>
3.2.1	Протоколы .....	190
3.2.2	ATR .....	191
3.2.3	PTS .....	192
<b>3.3.</b>	<b>Правила доступа.....</b>	<b>192</b>
<b>3.4.</b>	<b>Обзор команд и кодов ошибок.....</b>	<b>196</b>
<b>3.5.</b>	<b>Описания команд .....</b>	<b>198</b>
3.5.1	SELECT.....	199
3.5.1.1	Выбор по названию (AID).....	202
3.5.1.2	Выбор элементарного файла с использованием идентификатора файла.....	203
3.5.2	READ BINARY .....	201
3.5.2.1	Команда со смещением в P1-P2.....	204
3.5.2.1.1	Команда с защищённым обменом сообщениями (примеры) .....	204
3.5.2.2	Команда с коротким идентификатором EF (элементарного файла).....	207
3.5.2.3	Команда с нечётным командным байтом .....	208
3.5.2.3.1	Команда с защищённым обменом сообщениями (пример).....	209
3.5.3	UPDATE BINARY .....	208
3.5.3.1	Команда со смещением в P1-P2.....	211
3.5.3.1.1	Команда с защищённым обменом сообщениями (примеры) .....	211
3.5.3.2	Команда с коротким идентификатором EF .....	213
3.5.3.3	Команда с нечётным командным байтом .....	214
3.5.3.3.1	Команда с защищённым обменом сообщениями (пример).....	214
3.5.4	GET CHALLENGE.....	213
3.5.5	VERIFY.....	214
3.5.6	GET RESPONSE.....	216
3.5.7	PSO: VERIFY CERTIFICATE .....	217
3.5.7.1	Команда первого поколения – пара ответов.....	220
3.5.7.2	Команда второго поколения – пара ответов.....	220
3.5.8	INTERNAL AUTHENTICATE.....	219
3.5.9	EXTERNAL AUTHENTICATE.....	220
3.5.10	GENERAL AUTHENTICATE .....	221
3.5.11	MANAGE SECURITY ENVIRONMENT .....	222

3.5.11.1	Команда первого поколения – пара ответов .....	225
3.5.11.2	Команда второго поколения – пары ответов .....	225
3.5.11.2.1	MSE:SET AT для аутентификации микросхемы .....	225
3.5.11.2.2	MSE:SET AT для аутентификации БУ .....	226
3.5.11.2.3	MSE:SET DST .....	227
3.5.12	PSO: HASH .....	225
3.5.13	PERFORM HASH of FILE .....	225
3.5.14	PSO: COMPUTE DIGITAL SIGNATURE .....	227
3.5.15	PSO: VERIFY DIGITAL SIGNATURE .....	228
3.5.16	PROCESS DSRC MESSAGE .....	229
<b>4.</b>	<b>СТРУКТУРА КАРТОЧЕК ТАХОГРАФОВ.....</b>	<b>231</b>
<b>4.1.</b>	<b>Главный файл MF.....</b>	<b>231</b>
<b>4.2.</b>	<b>Приложения карточки водителя.....</b>	<b>233</b>
4.2.1	Приложение карточки водителя первого поколения .....	233
4.2.2	Приложение карточки водителя второго поколения .....	237
<b>4.3.</b>	<b>Приложения карточки мастерской.....</b>	<b>242</b>
4.3.1	Приложение карточки мастерской первого поколения .....	242
4.3.2	Приложение карточки мастерской второго поколения .....	247
<b>4.4.</b>	<b>Приложения контрольной карточки.....</b>	<b>253</b>
4.4.1	Приложение контрольной карточки первого поколения .....	253
4.4.2	Приложение контрольной карточки второго поколения.....	255
<b>4.5.</b>	<b>Приложения карточки предприятия.....</b>	<b>256</b>
4.5.1	Приложение карточки предприятия первого поколения.....	256
4.5.2	Приложение карточки предприятия второго поколения.....	258

## 1. Введение

### 1.1. Сокращения

В настоящем приложении употребляются следующие сокращения:

<b>AC</b>	Условия доступа
<b>AES</b>	Расширенный стандарт шифрования
<b>AID</b>	Идентификатор приложения
<b>ALW</b>	Всегда
<b>APDU</b>	Прикладной протокольный блок данных (структура команды)
<b>ATR</b>	Отклик на сигнал сброса
<b>AUT</b>	Аутентифицированный
<b>C6, C7</b>	Контакты № 6 и 7 карточки, как описано в ISO/IEC 7816-2
<b>cc (вц)</b>	временные циклы
<b>CHV</b>	Информация проверки данных владельца карточки
<b>CLA</b>	Классовый байт команды APDU
<b>DSRC</b>	Выделенная связь ближнего действия
<b>DF</b>	Выделенный файл. DF может содержать другие файлы (EF или DF)
<b>ECC</b>	Эллиптическая криптография
<b>EF</b>	Элементарный файл
<b>etu (эев)</b>	элементарная единица времени
<b>G1</b>	Первое поколение
<b>G2</b>	Второе поколение
<b>IC</b>	Интегральная схема
<b>ICC</b>	Карточка с интегральной схемой
<b>ID</b>	Идентификатор
<b>IFD</b>	Устройство интерфейса
<b>IFS</b>	Размер информационного поля
<b>IFSC</b>	Размер информационного поля для карточки
<b>IFSD</b>	Устройство размера информационного поля (для терминала)
<b>INS</b>	Командный байт команды APDU
<b>Lc</b>	Длина входных данных для команды APDU
<b>Le</b>	Длина ожидаемых данных (выходные данные для команды)
<b>MF</b>	главный файл (корневой DF)
<b>NAD</b>	Адрес узла, используемый в протоколе T=1
<b>NEV</b>	Никогда
<b>P1-P2</b>	Байты параметров
<b>PIN</b>	Персональный идентификационный номер
<b>PRO SM</b>	Криптозащищённое сообщение
<b>PTS</b>	Выбор передачи протокола
<b>RFU</b>	Зарезервировано для будущего пользования
<b>RST</b>	Перезагрузка (карточки)
<b>SFID</b>	Короткий идентификатор EF
<b>SM</b>	Безопасный обмен сообщениями
<b>SW1-SW2</b>	Статусные байты
<b>TS</b>	Исходный символ ATR
<b>VPP</b>	Напряжение программирования
<b>VU (БУ)</b>	Бортовое устройство
<b>XXh</b>	Значение XX в шестнадцатеричном исчислении
<b>'XXh'</b>	Значение XX в шестнадцатеричном исчислении
<b>  </b>	Символ конкатенации 03  04=0304



## 1.2. Ссылки

В настоящем приложении используются следующие источники:

ISO/IEC 7816-2	Идентификационные карточки – карточки с интегральными микросхемами. Часть 2: размеры и расположение контактов. ISO/IEC 7816-2:2007.
ISO/IEC 7816-3	Идентификационные карточки – карточки с интегральными микросхемами. Часть 3: электрический интерфейс и протоколы передачи. ISO/IEC 7816-3:2006.
ISO/IEC 7816-4	Идентификационные карточки – карточки с интегральными микросхемами. Часть 4: организация, безопасность и команды обмена. ISO/IEC 7816-4:2013 + Cor 1: 2014.
ISO/IEC 7816-6	Идентификационные карточки – карточки с интегральными микросхемами. Часть 6: межсекторные элементы данных для обмена. ISO/IEC 7816-6:2004 + Cor 1: 2006.
ISO/IEC 7816-8	Идентификационные карточки – карточки с интегральными микросхемами. Часть 8: команды операций по обеспечению безопасности. ISO/IEC 7816-8:2004.
ISO/IEC 9797-2	Информационные технологии. Техники обеспечения безопасности. Коды аутентификации сообщений (MAC). Часть 2: механизмы с использованием хэш-функции. ISO/IEC 9797-2:2011

## 2. Электрические и физические характеристики

- TCS\_01 Все электрические сигналы соответствуют стандарту ISO/IEC 7816-3, если не указано иначе.
- 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 рамках 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 соединён с  $V_{cc}$  карточки, но не заземлён. В любом случае это напряжение не должно интерпретироваться.

### 2.3. Формирование и частота тактовых сигналов

- TCS\_06 Карточка работает в диапазоне частот 1-5 МГц и может поддерживать более высокие частоты. В рамках 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:

Низкий	Высокий	
Бит 3	Бит 2	Бит 1

0	0	1	Остановка часов разрешена, предпочитаемый уровень отсутствует
0	1	1	Остановка часов разрешена, предпочитаемый уровень – высокий
1	0	1	Остановка часов разрешена, предпочитаемый уровень – низкий
0	0	0	Остановка часов не разрешена
0	1	0	Остановка часов разрешена только на высоком уровне
1	0	0	Остановка часов разрешена только на низком уровне

Биты 4-8 не используются.

## 2.4. Контакт ввода/вывода

TCS\_08 Контакт ввода/вывода C7 используется для получения данных из IFD и передачи данных в IFD. Во время работы в режиме передачи может находиться только карточка или только IFD. Если оба устройства работают в режиме передачи, никакого вреда карточке не наносится. Если передача данных не производится, карточка переключается в режим приёма.

## 2.5. Состояния 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,  
В нерабочем состоянии в остальное время; в этом состоянии все данные на карточке сохраняются.

## 3. Аппаратное обеспечение и связь

### 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 и протокол T=0, 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 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 вц.
- Интерфейс способен считывать символы, отделённые во времени на 12 эв.
- Интерфейс распознаёт ошибочные символы и их повторение, если они разделены во времени на 13 эв. В случае обнаружения ошибочного символа контакт ввода/вывода может отражать сигнал ошибки в интервале 1-2 эв. Устройство реагирует на задержку продолжительностью 1 эв.
- Интерфейс принимает ATR размером 33 байта (TS+ 32)
- Если в ATR есть TC1, для символов, передаваемых интерфейсом, должно быть предусмотрено дополнительное время хранения, хотя временной интервал между символами, посылаемыми карточкой, может и в этом случае составлять 12 эв. Это также применимо к символу AСК, посылаемому карточкой после передачи символа P3 интерфейсом.
- Интерфейс принимает символ NUL, передаваемый карточкой.
- Интерфейс принимает 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-block ABORT: не используется.
- S-block VPP state error: 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 передаёт запрос S-Block IFS после ATR, после чего карточка передаёт обратно данные S-Block 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.

Пример базового бипротоккола AID согласно ISO/IEC 7816-3

Символ	Значение	Примечания
TS	'3Bh'	Указывает на прямую связь.
T0	'85h'	TD1 присутствует; имеются 5 архивных байтов.
TD1	'80h'	TD2 присутствует; следует применять T=0
TD2	'11h'	TA3 присутствует; следует применять T=1
TA3	'XXh' (не менее 'F0h')	Размер информационного поля карточки (IFSC)
TH1-TH5	'XXh'	Архивные символы

TСК	'XXh'	Проверочный символ (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 устройство должно передать на карточку сигнал PTS (также обозначаемый сокращением 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 передаёт 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 символ
PPS0	'00h' или '01h'	PPS1-PPS3 не присутствуют; '00h' для выбора T0, '01h' для выбора T1.
PK	'XXh'	Проверочный символ: 'XXh' = 'FFh', если PPS0 = '00h', 'XXh' = 'FFh', 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 действительны следующие условия безопасности:

Сокращение	Значение
<b>ALW</b>	Действие возможно во всех случаях и может быть выполнено без ограничений. Команда и ответ APDU передаются простым текстом, т.е. без защищённого обмена сообщениями.
<b>NEV</b>	Действие невозможно ни в каких случаях.
<b>PLAIN-C</b>	Команда APDU передаётся простым текстом, т.е. без защищённого обмена сообщениями.
<b>PWD</b>	Действие может быть выполнено только в том случае, если ПИН-код карточки мастерской успешно прошёл проверку, т.е. если установлен внутренний статус безопасности карточки «PIN_Verified». Команда должна отправляться без защищённого обмена сообщениями.
<b>EXT-AUT-G1</b>	Действие может выполняться, только если успешно выполнена команда внешней аутентификации первого поколения (см. также приложение 11, часть А).
<b>SM-MAC-G1</b>	APDU (команда и ответ) должны применяться при защищённом обмене сообщениями первого поколения только в режиме аутентификации (см. приложение 11, часть А).

<b>SM-C-MAC-G1</b>	Команда APDU должна применяться при защищённом обмене сообщениями первого поколения только в режиме аутентификации (см. приложение 11, часть А).
<b>SM-R-ENC-G1</b>	Ответ APDU должен применяться при защищённом обмене сообщениями первого поколения в зашифрованном виде (см. приложение 11, часть А), т.е. код аутентификации сообщения не выдаётся.
<b>SM-R-ENC-MAC-G1</b>	Ответ APDU должен применяться при защищённом обмене сообщениями первого поколения в режиме шифрования с последующей аутентификацией (см. приложение 11, часть А).
<b>SM-MAC-G2</b>	APDU (команда и ответ) должны применяться при защищённом обмене сообщениями второго поколения только в режиме аутентификации (см. приложение 11, часть Б).
<b>SM-C-MAC-G2</b>	Команда APDU должна применяться при защищённом обмене сообщениями второго поколения только в режиме аутентификации (см. приложение 11, часть Б).
<b>SM-R-ENC-MAC-G2</b>	Ответ APDU должен применяться при защищённом обмене сообщениями второго поколения в режиме шифрования с последующей аутентификацией (см. приложение 11, часть Б).

TCS\_24 Данные условия обеспечения безопасности могут быть связаны следующими способами:

- **AND:** Должны быть выполнены все условия безопасности
- **OR:** 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.

TCS\_25 В приложении DF Tachograph G1 соблюдаются следующие правила доступа:

Команда	Карточка водителя	Карточка мастерской	Контрольная карточка	Карточка предприятия
External Authenticate				
• Аутентификация первого поколения	ALW	ALW	ALW	ALW
• Аутентификация второго поколения	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Неприменимо	Неприменимо	Неприменимо	Неприменимо
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Неприменимо	Неприменимо
PSO: Hash	Неприменимо	Неприменимо	ALW	Неприменимо
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Неприменимо	Неприменимо
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Неприменимо	Неприменимо	ALW	Неприменимо
Verify	Неприменимо	ALW	Неприменимо	Неприменимо

TCS\_26 В приложении DF Tachograph\_G2 соблюдаются следующие правила доступа:

Команда	Карточка водителя	Карточка мастерской	Контрольная карточка	Карточка предприятия
External Authenticate				
• Аутентификация первого поколения	Неприменимо	Неприменимо	Неприменимо	Неприменимо
• Аутентификация второго поколения	ALW	PWD	ALW	ALW
Internal Authenticate	Неприменимо	Неприменимо	Неприменимо	Неприменимо
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Неприменимо	ALW	ALW	Неприменимо
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Неприменимо	Неприменимо
PSO: Hash	Неприменимо	Неприменимо	ALW	Неприменимо
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Неприменимо	Неприменимо
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Неприменимо	Неприменимо	ALW	Неприменимо
Verify	Неприменимо	ALW	Неприменимо	Неприменимо

TCS\_27 В MF соблюдаются следующие правила доступа:

Команда	Карточка водителя	Карточка мастерской	Контрольная карточка	Карточка предприятия
External Authenticate				
• Аутентификация первого поколения	Неприменимо	Неприменимо	Неприменимо	Неприменимо
• Аутентификация второго поколения	ALW	PWD	ALW	ALW
Internal Authenticate	Неприменимо	Неприменимо	Неприменимо	Неприменимо
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Неприменимо	Неприменимо	Неприменимо	Неприменимо
PSO: Compute Digital Signature	Неприменимо	Неприменимо	Неприменимо	Неприменимо
PSO: Hash	Неприменимо	Неприменимо	Неприменимо	Неприменимо
PSO: Hash of File	Неприменимо	Неприменимо	Неприменимо	Неприменимо
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Неприменимо	ALW	Неприменимо	Неприменимо

TCS\_28 Карточка тахографа может принять или не принять команду с более высоким уровнем безопасности, нежели указано в условиях безопасности. Это значит, что если условие безопасности – ALW (или PLAIN-C), карточка может принять команду с защищённым обменом сообщениями (в режиме шифрования и/или аутентификации). Если по условию безопасности требуется защищённый обмен сообщениями в режиме аутентификации, карточка тахографа может принять команду с защищённым обменом 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 структура 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 1 и 2 поколений, представлены в соответствующих описаниях команд.

Команда	INS
SELECT	'A4h'
READ BINARY	'B0h', 'B1h'
UPDATE BINARY	'D6h', 'D7h'
GET CHALLENGE	'84h'
VERIFY	'20h'
GET RESPONSE	'C0h'
PERFORM SECURITY OPERATION	'2Ah'
<ul style="list-style-type: none"> <li>• VERIFY CERTIFICATE</li> <li>• COMPUTE DIGITAL SIGNATURE</li> <li>• VERIFY DIGITAL SIGNATURE</li> <li>• HASH</li> <li>• PERFORM HASH OF FILE</li> <li>• PROCESS DSRC MESSAGE</li> </ul>	
INTERNAL AUTHENTICATE	'88h'
EXTERNAL AUTHENTICATE	'82h'
MANAGE SECURITY ENVIRONMENT	'22h'
<ul style="list-style-type: none"> <li>• SET DIGITAL SIGNATURE TEMPLATE</li> <li>• SET AUTHENTICATION TEMPLATE</li> </ul>	
GENERAL AUTHENTICATE	'86h'

TCS\_29 Характеристики состояния SW1 SW2 включаются в любое ответное сообщение и означают состояние обработки команды.

SW1	SW2	Значение
90	00	Нормальная обработка
61	XX	Нормальная обработка. XX = число имеющихся байтов для ответа.
62	81	Обработка предупреждения. Часть передаваемых обратно данных может быть повреждена
63	00	Аутентификация неуспешна (предупреждение)
63	CX	Неправильный код CHV (PIN). Счётчик 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 безопасности: неверная криптографическая контрольная сумма (во время защищённого 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	Защищённый обмен сообщениями не поддерживается
68	83	Ожидается последняя команда цепочки
69	00	Запрещённая команда (отсутствие ответа в T=0)
69	82	Статус защиты неприемлем
69	83	Метод аутентификации заблокирован
69	85	Условия использования неприемлемы
69	86	Команда не разрешена (активный EF отсутствует)
69	87	Отсутствие предусмотренных криптозащищённых объектов данных
69	88	Неверные криптозащищённые объекты данных
6A	80	Неверные 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 точную длину. Поле данных не выдаётся
6D	00	Командный код не поддерживается или недействителен
6E	00	Класс не поддерживается
6F	00	Другие контрольные ошибки

TCS\_30 Если выполняется более чем одно условие ошибки в одной команде APDU, карточка может выдать любой из соответствующих статусов.

### 3.5. Описания команд

В настоящей главе описываются параметры обязательных команд для карточек тахографа.

Дополнительные соответствующие данные, относящиеся к криптографическим операциям, представлены в приложении 11 «Общие механизмы защиты» для тахографов первого и второго поколений.

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, относящаяся к ней длина, значение и описание не заполнены.

TCS\_31 Если запрашиваются оба байта длины (Lc и Le), описываемая команда разделяется на две части; если IFD использует протокол T=0: IFD передаёт 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 (защищённый обмен сообщениями):

- В случае использования протокола T=1 карточка выдает Le=0, передавая все имеющиеся выходные данные.
- В случае использования протокола T=0 IFD передает первую команду с P3=Lc + данные, карточка передаёт 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 RESPONSE с P3 = La для чтения данных.

TCS\_33 Карточка тахографа может поддерживать поля расширенной длины в соответствии с ISO/IEC 7816-4 как дополнительную функцию. Карточка тахографа, поддерживающая поля расширенной длины,

- Указывает на поддержку полей расширенной длины в ATR
- Обеспечивает поддерживаемые размеры буфера посредством информации о расширенной длине 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 защищённого обмена сообщениями, а уровень защищённого обмена сообщениями описан в приложении 11. По правилам доступа, касающимся команды, понятно, поддерживает ли команда защищённый обмен сообщениями или нет и поддерживает ли команда защищённый обмен сообщениями первого и/или второго поколений.

Некоторые варианты команды описываются и с точки зрения защищённого обмена сообщениями, чтобы проиллюстрировать применение защищённого обмена сообщениями.

TCS\_34 БУ полностью выполняет протокол взаимной аутентификации БУ и карточки второго поколения во время сеанса использования карточки, включая проверку сертификата (если требуется) в DF Tachograph, DF Tachograph\_G2 или MF.

### 3.5.1 SELECT

Данная команда соответствует стандарту ISO/IEC 7816-4, однако её использование ограничено по сравнению с командой, определённой в указанном стандарте.

Команда SELECT используется:

- для выбора приложения DF (должен использоваться выбор по названию);
- для выбора элементарного файла, соответствующего представленному файлу ID

#### 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 защищённого обмена сообщениями, ключи предыдущего сеанса защищённого 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'	Ответа не ожидается
Lc	1	'NNh'	Число байтов, переданных на карточку (длина AID): '06h' для приложения тахографа
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' для приложения тахографа первого поколения AID: 'FF 53 4D 52 44 54' для приложения тахографа второго поколения

Ответ на команду SELECT не требуется (в случае T=1 Lc отсутствует, а в случае T=0 запрос на ответ не передаётся).

TCS\_38 Ответное сообщение (запроса на ответ нет)

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- ◆ Если команда проходит успешно, карточка выдаёт '9000'.
- ◆ Если приложение, соответствующее AID, не найдено, статус обработки выдаётся в виде '6A82'.
- ◆ При T=1, если присутствует байт Lc, состояние выдаётся в виде '6700'.
- ◆ При T=0, если запрос на ответ поступает после команды SELECT, статус выдаётся в виде '6900'.
- ◆ Если выбранное приложение считается повреждённым (в атрибутах файла обнаружена ошибка целостности), статус обработки выдаётся в виде '6400' или '6581'.

### 3.5.1.2 Выбор элементарного файла с использованием идентификатора файла

TCS\_39 Командное сообщение

TCS\_40 Карточка тахографа поддерживает защищённый обмен сообщениями второго поколения, как указано в части Б приложения 11 для данного варианта команды.

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Выбор EF в текущем DF
P2	1	'0Ch'	Ответа не ожидается
Lc	1	'02h'	Число байтов, переданных на карточку
#6-#7	2	'XXXXh'	Идентификатор файла

Ответ на команду SELECT не требуется (в случае T=1 Lc отсутствует, а в случае T=0 запрос на ответ не передаётся).

TCS\_41 Ответное сообщение (запроса на ответ нет)

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт '9000'.
- Если приложение, соответствующее идентификатору файла, не найдено, статус обработки выдаётся в виде '6A82'.
- При T=1, если присутствует байт Lc, состояние выдаётся в виде '6700'.
- При T=0, если запрос на ответ поступает после команды SELECT, статус выдаётся в виде '6900'.
- Если выбранный файл считается повреждённым (в атрибутах файла обнаружена ошибка целостности), статус обработки выдаётся в виде '6400' или '6581'.

### 3.5.2 READ BINARY

Данная команда соответствует стандарту ISO/IEC 7816-4, однако её использование ограничено по сравнению с командой, определённой 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 защищённого 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 незащищённом виде.

Примечание: Данная команда без защищённого обмена сообщениями может использоваться только для чтения файла, который поддерживает условие безопасности ALW для режима доступа Read.

#### TCS\_42 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	Смещение в байтах от начала файла: Самый значимый байт
P2	1	'XXh'	Смещение в байтах от начала файла: Наименее значимый байт
Le	1	'XXh'	Ожидаемая длина данных. Число байтов, подлежащих извлечению.

Примечание: бит 8 байта P1 должен быть равен 0.

#### TCS\_43 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#X	X	'XX..XXh'	Прочитанные данные
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- ◆ Если команда проходит успешно, карточка выдаёт '9000'.
- ◆ Если EF не выбран, статус обработки выдаётся в виде '6986'.
- ◆ Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей '6982'.
- ◆ Если смещение не соответствует размеру EF (смещение > размер EF), статус обработки выдаётся в виде '6B00'.
- ◆ Если размер данных, подлежащих извлечению, не соответствует размеру EF (смещение + Le > размер EF), статус обработки выдаётся в виде '6700' или '6Cxx', где 'xx' указывает точную длину.
- ◆ Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл повреждён и не может быть восстановлен, и статус обработки выдаётся в виде '6400' или '6581'.
- ◆ Если в хранящихся данных обнаружена ошибка целостности, карточка выдаёт требуемые данные, и статус обработки выдаётся в виде '6281'.

#### 3.5.2.1.1 Команда с защищённым обменом сообщениями (примеры)

Данная команда позволяет IFD считывать данные из EF, выбранного для защищённого обмена сообщениями, чтобы проверить целостность получаемых данных и обеспечить их конфиденциальность, если применяется условие безопасности SM-R-ENC-MAC-G1 (первого поколения) или SM-R-ENC-MAC-G2 (второго поколения).

## TCS\_44 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'0Ch'	Требуется защищённый обмен сообщениями
INS	1	'B0h'	Read Binary
P1	1	'XXh'	P1 (смещение в байтах от начала файла): Самый значимый байт
P2	1	'XXh'	P2 (смещение в байтах от начала файла): Наименее значимый байт
Lc	1	'XXh'	Длина вводимых данных в защищённом виде
#6	1	'97h'	T <sub>LE</sub> : метка, указывающая на спецификацию ожидаемой длины
#7	1	'01h'	L <sub>LE</sub> : длина ожидаемой длины
#8	1	'NNh'	Спецификация ожидаемой длины (исходное значение Lc): Число байтов, подлежащих извлечению
#9	1	'8Eh'	T <sub>CC</sub> : метка, указывающая на криптографическую контрольную сумму
#10	1	'XXh'	L <sub>CC</sub> : Длина следующей криптографической контрольной суммы '04h' для защищённого обмена сообщениями первого поколения (см. часть А приложения 11) '08h', '0Ch' или '10h' в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#11-#(10+L)	L	'XX..XXh'	Криптографическая контрольная сумма
Le	1	'00h'	Как указано в стандарте ISO/IEC 7816-4

## TCS\_45 Ответное сообщение, если не требуется SM-R-ENC-MAC-G1 (первого поколения)/SM-R-ENC-MAC-G2 (второго поколения) и если формат ввода защищённого обмена сообщениями верен:

Байт	Длина	Значение	Описание
#1	1	'99h'	Метка статуса обработки (SW1-SW2) – факультативно для защищённого обмена сообщениями первого поколения
#2	1	'02h'	Длина статуса обработки
#3 - #4	2	'XX XXh'	Статус обработки для незащищённого ответа APDU
#5	1	'81h'	T <sub>PV</sub> : метка, указывающая на значение обычных данных
#6	L	'NNh' или '81 NNh'	L <sub>PV</sub> : длина переданных обратно данных (= исходное значение Lc) L равна 2 байтам, если L <sub>PV</sub> > 127 байтов.
#(6+L)-#(5+L+NN)	NN	'XX..XXh'	Значения обычных данных
#(6+L+NN)	1	'8Eh'	T <sub>CC</sub> : метка, указывающая на криптографическую контрольную сумму
#(7+L+NN)	1	'XXh'	L <sub>CC</sub> : Длина следующей криптографической контрольной суммы '04h' для защищённого обмена сообщениями первого поколения (см. часть А приложения 11) '08h', '0Ch' или '10h' в зависимости от длины ключа AES для защищённого обмена

			сообщениями (см. часть Б приложения 11)
#(8+L+NN)- #(7+M+L+NN)	M	'XX..XXh'	Криптографическая контрольная сумма
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

TCS\_46 **Ответное сообщение, если требуется SM-R-ENC-MAC-G1 (первого поколения)/SM-R-ENC-MAC-G2 (второго поколения) и если формат ввода защищённого обмена сообщениями верен:**

Байт	Длина	Значение	Описание
#1	1	'87h'	T <sub>PCG</sub> : Метка, указывающая на зашифрованные данные (криптограмма)
#2	L	'MMh' или '81 MMh'	L <sub>PCG</sub> : длина выданных зашифрованных данных (отличная от исходного значения L <sub>e</sub> команды, что обусловлено заполнением). L равна 2 байтам, если L <sub>PCG</sub> > 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 защищённого обмена сообщениями первого поколения
#(3+L+MM)	1	'02h'	Длина статуса обработки
#(4+L+MM) - #(5+L+MM)	2	'XX XXh'	Статус обработки для незащищённого ответа APDU
#(6+L+MM)	1	'8Eh'	T <sub>CC</sub> : метка, указывающая на криптографическую контрольную сумму
#(7+L+MM)	1	'XXh'	L <sub>CC</sub> : Длина следующей криптографической контрольной суммы '04h' для защищённого обмена сообщениями первого поколения (см. часть А приложения 11) '08h', '0Ch' или '10h' в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#(8+L+MM)- #(7+N+L+MM)	N	'XX..XXh'	Криптографическая контрольная сумма
SW	2	'XXXXh'	Характеристики статуса (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 защищённого обмена сообщениями.

Кроме того, могут иметь место некоторые ошибки, которые конкретно связаны с защищённым обменом сообщениями. В этом случае данные о состоянии обработки просто возвращаются, не задействуя использованную структуру защиты данных:

TCS\_47 **Ответное сообщение, если формат ввода защищённого обмена данными неправильный**

Байт	Длина	Значение	Описание
SW	2	'XXXXh' ,	Характеристики статуса (SW1,SW2)

- ♦ Если ключ текущего сеанса отсутствует, статус обработки выдается в виде '6A88'. Это происходит либо по той причине, что ключ сеанса ещё не создан, либо потому, что ключ сеанса больше

недействителен (в этом случае IFD должен повторить процесс взаимной аутентификации в целях генерации нового ключа сеанса).

- ◆ Если некоторые ожидаемые объекты данных (как указано выше) в формате защищённого обмена данными отсутствуют, статус обработки выдаётся в виде **'6987'**: эта ошибка имеет место в том случае, если ожидаемая метка отсутствует или если основная часть команды составлена неправильно.
- ◆ Если некоторые объекты данных неправильны, статус обработки выдаётся в виде **'6988'**: эта ошибка имеет место в том случае, если требуемые метки есть, но длина некоторых из них отличается от ожидаемой.
- ◆ Если проверка криптографической контрольной суммы показала неправильный результат, статус обработки выдаётся в виде **'6688'**.

### 3.5.2.2 Команда с коротким идентификатором EF (элементарного файла)

Данный вариант команды позволяет IFD выбрать 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 указанным коротким идентификатором EF. Такие короткие идентификаторы EF представлены в главе 4.

#### TCS\_49 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	Бит 8 устанавливается на 1 Биты 7 и 6 устанавливаются на 00 Бит 5 – 1 кодирует короткий идентификатор EF соответствующего EF
P2	1	'XXh'	Кодирует смещение от 0 до 255 байтов в EF с указанием P1
Le	1	'XXh'	Ожидаемая длина данных. Число байтов, подлежащих извлечению.

Примечание: Короткие идентификаторы EF, используемые в приложении тахографов второго поколения, представлены в главе 4.

Если P1 кодирует короткий идентификатор EF и команда проводится успешно, идентифицированный EF становится текущим выбранным EF (текущий EF).

#### TCS\_50 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#L	L	'XX..XXh'	Прочитанные данные
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- ◆ Если команда проходит успешно, карточка выдаёт **'9000'**.
- ◆ Если приложение, соответствующее короткому идентификатору EF, не найдено, статус обработки выдаётся в виде **'6A82'**.
- ◆ Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей **'6982'**.
- ◆ Если смещение не соответствует размеру EF (смещение > размер EF), статус обработки выдаётся в виде **'6B00'**.



- ◆ Если размер данных, подлежащих извлечению, не соответствует размеру EF (смещение + Le > размер EF), статус обработки выдаётся в виде '6700' или '6Схх', где 'хх' указывает точную длину.
- ◆ Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл повреждён и не может быть восстановлен, и статус обработки выдаётся в виде '6400' или '6581'.
- ◆ Если в хранящихся данных обнаружена ошибка целостности, карточка выдаёт требуемые данные, и статус обработки выдаётся в виде '6281'.

### 3.5.2.3 Команда с нечётным командным байтом

Данный вариант команды позволяет IFD считывать данные с EF с 32768 или более байтов.

TCS\_51 Карточка тахографа, поддерживающая EF с 32768 или более байтов, поддерживает данный вариант команды для данных 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'	Read Binary
P1	1	'00h'	Текущий EF
P2	1	'00h'	
Lc	1	'NNh'	Длина Lc смещённого объекта данных.
#6-#(5+NN)	NN	'XX..XXh'	Смещённый объект данных: Метка '54h' Длина '01h' или '02h' Значение смещение
Le	1	'XXh'	Число байтов, подлежащих извлечению.

IFD кодирует длину смещённого объекта данных 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 '65535' байтов.

TCS\_53 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#L	L	'XX..XXh'	Считываемые данные включаются в дискретный объект данных с меткой '53h'.
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- ◆ Если команда проходит успешно, карточка выдаёт '9000'.
- ◆ Если EF не выбран, статус обработки выдаётся в виде '6986'.
- ◆ Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей '6982'.
- ◆ Если смещение не соответствует размеру EF (смещение > размер EF), статус обработки выдаётся в виде '6B00'.
- ◆ Если размер данных, подлежащих извлечению, не соответствует размеру EF (смещение + Le > размер EF), статус обработки выдаётся в виде '6700' или '6Схх', где 'хх' указывает точную длину.
- ◆ Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл повреждён и не может быть восстановлен, и статус обработки выдаётся в виде '6400' или '6581'.
- ◆ Если в хранящихся данных обнаружена ошибка целостности, карточка выдаёт требуемые данные, и статус обработки выдаётся в виде '6281'.

### 3.5.2.3.1 Команда с защищённым обменом сообщениями (пример)

Следующий пример иллюстрирует применение защищённого обмена сообщениями, если применяется условие безопасности SM-MAC-G2.

TCS\_54 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'0Ch'	Требуется защищённый обмен сообщениями
INS	1	'B1h'	Read Binary
P1	1	'00h'	Текущий EF
P2	1	'00h'	
Lc	1	'XXh'	Длина поля защищённых данных
#6	1	'B3h'	Метка данных простого значения, кодируемых в BER-TLV
#7	1	'NNh'	L <sub>PV</sub> : длина переданных данных
#(8)-#(7+NN)	NN	'XX..XXh'	Простые данные, закодированные в BER-TLV, т.е. смещённый объект данных с меткой '54'
#(8+NN)	1	'97h'	T <sub>LE</sub> : метка, указывающая на спецификацию ожидаемой длины
#(9+NN)	1	'01h'	L <sub>LE</sub> : Длина ожидаемой длины
#(10+NN)	1	'XXh'	Спецификация ожидаемой длины (исходное значение Le): Число байтов, подлежащих извлечению
#(11+NN)	1	'8Eh'	T <sub>CC</sub> : Метка, указывающая на криптографическую контрольную сумму
#(12+NN)	1	'XXh'	L <sub>CC</sub> : Длина следующей криптографической контрольной суммы '08h', '0Ch' или '10h' в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#(13+NN)-#(12+M+NN)	M	'XX..XXh'	Криптографическая контрольная сумма
Le	1	'00h'	Как указано в стандарте ISO/IEC 7816-4

TCS\_55 Ответное сообщение, если команда выполнена успешно

Байт	Длина	Значение	Описание
#1	1	'B3h'	Простые данные, закодированные в BER-TLV
#2	L	'NNh' или '81 NNh'	L <sub>PV</sub> : длина переданных обратно данных (= исходное значение Le). L равна 2 байтам, если L <sub>PV</sub> > 127 байтов.
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Простые данные, закодированные с BER-TLV, т.е. прочитанные данные, включённые в дискретный объект данных с меткой '53h'.
#(2+L+NN)	1	'99h'	Статус обработки для незащищённого ответа APDU
#(3+L+NN)	1	'02h'	Длина статуса обработки
#(4+L+NN) - #(5+L+NN)	2	'XX XXh'	Статус обработки для незащищённого ответа APDU
#(6+L+NN)	1	'8Eh'	T <sub>CC</sub> : Метка, указывающая на криптографическую контрольную сумму
#(7+L+NN)	1	'XXh'	L <sub>CC</sub> : Длина следующей криптографической

			контрольной суммы '08h', '0Ch' или '10h' в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#(8+L+NN)- #(7+M+L+NN)	M	'XX..XXh'	Криптографическая контрольная сумма
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

### 3.5.3 UPDATE BINARY

Данная команда соответствует стандарту ISO/IEC 7816-4, однако её использование ограничено по сравнению с командой, определённой 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

Данная команда позволяет IFD записывать данные в выбранный в данный момент EF без проверки целостности полученных данных карточкой.

Примечание: Данная команда без защищённого обмена сообщениями может использоваться только для обновления файла, который поддерживает условие безопасности ALW для режима доступа Update.

#### TCS\_56 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'D6h'	Update Binary
P1	1	'XXh'	Смещение в байтах от начала файла: Самый значимый байт
P2	1	'XXh'	Смещение в байтах от начала файла: Наименее значимый байт
Lc	1	'NNh'	Длина Lc данных, подлежащих обновлению. Число байтов, подлежащих записи.
#6-#(5+NN)	NN	'XX..XXh'	Данные, подлежащие записи

Примечание: бит 8 байта P1 должен быть равен 0.

#### TCS\_57 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- ◆ Если команда проходит успешно, карточка выдаёт '9000'.
- ◆ Если EF не выбран, статус обработки выдаётся в виде '6986'.
- ◆ Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей '6982'.
- ◆ Если смещение не соответствует размеру EF (смещение > размер EF), статус обработки выдаётся в виде '6B00'.
- ◆ Если размер данных, подлежащих записи, не соответствует размеру EF (смещение + Lc > размер EF), статус обработки выдаётся в виде '6700'.
- ◆ Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл повреждён и не может быть восстановлен, и статус обработки выдаётся в виде '6400' или '6500'.
- ◆ Если запись неуспешна, статус обработки выдаётся в виде '6581'.

#### 3.5.3.1.1 Команда с защищённым обменом сообщениями (примеры)

Данная команда позволяет IFD записывать данные в выбранный в данный момент EF с проверкой целостности полученных данных карточкой. Поскольку требование конфиденциальности отсутствует, данные не шифруются.

#### TCS\_58 Командное сообщение

Байт	Длина	Значение	Описание
------	-------	----------	----------

CLA	1	'0Ch'	Требуется защищённый обмен сообщениями
INS	1	'D6h'	Update Binary
P1	1	'XXh'	Смещение в байтах от начала файла: Самый значимый байт
P2	1	'XXh'	Смещение в байтах от начала файла: Наименее значимый байт
Lc	1	'XXh'	Длина поля защищённых данных
#6	1	'81h'	Т <sub>Рv</sub> : Метка, указывающая на значение обычных данных
#7	L	'NNh' или '81 NNh'	L <sub>Рv</sub> : длина переданных данных. L равна 2 байтам, если L <sub>Рv</sub> > 127 байтов.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Значение простых данных (данные, подлежащие записи)
#(7+L+NN)	1	'8Eh'	Т <sub>СС</sub> : Метка, указывающая на криптографическую контрольную сумму
#(8+L+NN)	1	'XXh'	L <sub>СС</sub> : Длина следующей криптографической контрольной суммы '04h' для защищённого обмена сообщениями первого поколения (см. часть А приложения 11) '08h', '0Ch' или '10h' в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#(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 защищённого обмена данными правильный

Байт	Длина	Значение	Описание
#1	1	'99h'	T <sub>SW</sub> : Метка, указывающая на характеристики статуса (должна быть защищена с помощью криптографической суммы)
#2	1	'02h'	L <sub>SW</sub> : длина переданных обратно характеристик статуса
#3-#4	2	'XXXXh'	Статус обработки для незащищённого ответа APDU
#5	1	'8Eh'	T <sub>СС</sub> : Метка, указывающая на криптографическую контрольную сумму
#6	1	'XXh'	L <sub>СС</sub> : Длина следующей криптографической контрольной суммы '04h' для защищённого обмена сообщениями первого поколения (см. часть А приложения 11) '08h', '0Ch' или '10h' в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#7-#(6+L)	L	'XX..XXh'	Криптографическая контрольная сумма
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

Данные о статусах «нормальной» обработки, описанные для команды UPDATE BINARY, передаваемой в незащищённом виде (см. пункт 3.5.3.1), могут возвращаться с использованием структур ответного сообщения, описанных выше.

Кроме того, могут иметь место некоторые ошибки, которые конкретно связаны с защищённым обменом сообщениями. В этом случае данные о состоянии обработки просто возвращаются, не задействуя использованную структуру защиты данных:

## TCS\_60 Ответное сообщение в случае ошибки в защищённом обмене сообщениями

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- ◆ Если ключ текущего сеанса отсутствует, статус обработки выдается в виде '6A88'.
- ◆ Если некоторые ожидаемые объекты данных (как указано выше) в формате защищённого обмена данными отсутствуют, статус обработки выдаётся в виде '6987': эта ошибка имеет место в том случае, если ожидаемая метка отсутствует или если основная часть команды составлена неправильно.
- ◆ Если некоторые объекты данных неправильны, статус обработки выдается в виде '6988': эта ошибка имеет место в том случае, если требуемые метки есть, но длина некоторых из них отличается от ожидаемой.
- ◆ Если проверка криптографической контрольной суммы показала неправильный результат, статус обработки выдаётся 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 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'	Update Binary
P1	1	'XXh'	Бит 8 устанавливается на 1 Биты 7 и 6 устанавливаются на 00 Бит 5 – 1 кодирует короткий идентификатор EF соответствующего EF
P2	1	'XXh'	Кодирует смещение от 0 до 255 байтов в EF с указанием P1
Lc	1	'NNh'	Длина Lc данных, подлежащих обновлению. 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 статуса (SW1,SW2)

Примечание: Короткие идентификаторы EF, используемые в приложении тахографов второго поколения, представлены в главе 4.

Если P1 кодирует короткий идентификатор EF и команда проводится успешно, идентифицированный EF становится текущим выбранным EF (текущий EF).

- ◆ Если команда проходит успешно, карточка выдаёт '9000'.
- ◆ Если приложение, соответствующее короткому идентификатору EF, не найдено, статус обработки выдаётся в виде '6A82'.
- ◆ Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей '6982'.

- ◆ Если смещение не соответствует размеру EF (смещение > размер EF), статус обработки выдаётся в виде **'6B00'**.
- ◆ Если размер данных, подлежащих записи, не соответствует размеру EF (смещение + Lc > размер EF), статус обработки выдаётся в виде **'6700'**.
- ◆ Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл повреждён и не может быть восстановлен, и статус обработки выдаётся в виде **'6400'** или **'6581'**.
- ◆ Если запись неуспешна, статус обработки выдаётся в виде **'6581'**.

### 3.5.3.3 Команда с нечётным командным байтом

Данный вариант команды позволяет IFD записывать данные в EF с 32768 или более байтов.

TCS\_64 Карточка тахографа, поддерживающая EF с 32768 или более байтов, поддерживает данный вариант команды для данных EF. Карточка тахографа может поддерживать или не поддерживать данный вариант команды для других EF.

TCS\_65 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'D7h'	Update Binary
P1	1	'00h'	Текущий EF
P2	1	'00h'	
Lc	1	'NNh'	Lc Длина данных в поле командных данных
#6-#(5+NN)	NN	'XX..XXh'	Смещённый объект данных с меткой '54h'    Дискретный объект данных с меткой '53h', включающий в себя данные, подлежащие записи

IFD кодирует длину смещённого объекта данных и 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 '65535' байтов.

TCS\_66 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- ◆ Если команда проходит успешно, карточка выдаёт **'9000'**.
- ◆ Если EF не выбран, статус обработки выдаётся в виде **'6986'**.
- ◆ Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей **'6982'**.
- ◆ Если смещение не соответствует размеру EF (смещение > размер EF), статус обработки выдаётся в виде **'6B00'**.
- ◆ Если размер данных, подлежащих записи, не соответствует размеру EF (смещение + Lc > размер EF), статус обработки выдаётся в виде **'6700'**.
- ◆ Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл повреждён и не может быть восстановлен, и статус обработки выдаётся в виде **'6400'** или **'6500'**.
- ◆ Если запись неуспешна, статус обработки выдаётся в виде **'6581'**.

#### 3.5.3.3.1 Команда с защищённым обменом сообщениями (пример)

Следующий пример иллюстрирует применение защищённого обмена сообщениями, если применяется условие безопасности SM-MAC-G2.

TCS\_67 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'0Ch'	Требуется защищённый обмен сообщениями
INS	1	'D7h'	Update Binary
P1	1	'00h'	Текущий EF
P2	1	'00h'	
Lc	1	'XXh'	Длина поля защищённых данных
#6	1	'B3h'	Метка данных простого значения, кодируемых в BER-TLV
#7	L	'NNh' или '81 NNh'	L <sub>PV</sub> : длина переданных данных. L равна 2 байтам, если L <sub>PV</sub> > 127 байтов.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Простые данные, закодированные в BER-TLV, т.е. смещённый объект данных с меткой '54h'    Дискретный объект данных с меткой '53h', включающий в себя данные, подлежащие записи
#(7+L+NN)	1	'8Eh'	T <sub>CC</sub> : Метка, указывающая на криптографическую контрольную сумму
#(8+L+NN)	1	'XXh'	L <sub>CC</sub> : Длина следующей криптографической контрольной суммы '08h', '0Ch' или '10h' в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#(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 выполнена успешно

Байт	Длина	Значение	Описание
#1	1	'99h'	T <sub>sw</sub> : Метка, указывающая на характеристики статуса (должна быть защищена с помощью криптографической суммы)
#2	1	'02h'	L <sub>sw</sub> : длина переданных обратно характеристик статуса
#3-#4	2	'XXXXh'	Статус обработки для незащищённого ответа APDU
#5	1	'8Eh'	T <sub>CC</sub> : Метка, указывающая на криптографическую контрольную сумму
#6	1	'XXh'	L <sub>CC</sub> : Длина следующей криптографической контрольной суммы '08h', '0Ch' или '10h' в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#7-#(6+L)	L	'XX..XXh'	Криптографическая контрольная сумма
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)



### 3.5.4 GET CHALLENGE

Данная команда соответствует стандарту ISO/IEC 7816-4, однако её использование ограничено по сравнению с командой, определённой в указанном стандарте.

Команда GET CHALLENGE предлагает карточке выдать запрос для его использования в процедуре, связанной с защитой, которая предусматривает передачу карточке криптограммы или некоторых зашифрованных данных.

TCS\_69 Challenge, 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 (ожидаемая длина Challenge).

TCS\_71 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#8	8	'XX..XXh'	Запрос
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- ◆ Если команда проходит успешно, карточка выдаёт '9000'.
- ◆ Если Le отличается от '08h', статус обработки выдаётся в виде '6700'.
- ◆ Если параметры P1-P2 неправильны, статус обработки выдаётся в виде '6A86'.

### 3.5.5 VERIFY

Данная команда соответствует стандарту ISO/IEC 7816-4, однако её использование ограничено по сравнению с командой, определённой 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. Таким образом, такие карточки не могут успешно выполнять данную команду. В случае других типов карточек тахографов, кроме карточек мастерской, поведение, т.е. передаваемый обратно код ошибки, не попадает в область применения данной спецификации, если команда отправлена.

Команда Verify инициирует сравнение на уровне карточки между переданными данными CHV (PIN) и исходными данными CHV, записанными на карточке.

TCS\_72 ПИН-код, введённый пользователем, должен быть закодирован в ASCII и заполнен IFD с правой стороны байтами 'FFh' до достижения длины 8 байтов; см. также тип данных WorkshopCardPIN в приложении 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 счётчика 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, счётчик оставшихся попыток CHV выставляется на исходное значение. Исходное значение счётчика оставшихся попыток CHV составляет 5. Если команда проходит, карточка передаёт внутренний статус безопасности PIN\_Verified. Карточка сбрасывает этот статус безопасности, если её 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 не позволяют работнику мастерской снова ввести ПИН-код после выбора другого приложения тахографа DF.

TCS\_76 Сравнение, которое дало неправильные результаты, регистрируется на карточке, т.е. значение счётчика 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 переданного кода CHV
#6-#13	8	'XX..XXh'	CHV

TCS\_78 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт '9000'.
- Если исходное значение CHV не найдено, статус обработки выдаётся в виде '6A88'.

- Если данные CHV заблокированы (счётчик оставшихся попыток CHV показывает ноль), статус обработки выдаётся в виде **'6983'**. В этом состоянии данные CHV больше никогда не принимаются.
- Если сравнение дало неправильные результаты, показание счётчика оставшихся попыток уменьшается и статус обработки выдаётся в виде **'63CX'** ( $X > 0$  и X равен показанию счётчика оставшихся попыток CHV).
- Если исходное значение CHV считается повреждённым, статус обработки выдаётся в виде **'6400'** или **'6581'**.
- Если Lc отличается от '08h', статус обработки выдаётся в виде **'6700'**.

### 3.5.6 GET RESPONSE

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 статуса (SW1,SW2)

- ◆ Если команда проходит успешно, карточка выдаёт '9000'.
- ◆ Если данные карточкой подготовлены не были, статус обработки выдаётся в виде '6900' или '6F00'.
- ◆ Если Le превышает число имеющихся байтов или если Le равна нулю, статус обработки выдаётся в виде '6Cxx', где xx указывает на точное число имеющихся байтов. В этом случае подготовленные данные всё ещё доступны для следующей команды GET RESPONSE.
- ◆ Если Le не равна нулю и меньше, чем число имеющихся байтов, требуемые данные нормально передаются карточкой, а статус обработки выдаётся в виде '61xx', где 'xx' указывает число дополнительных байтов, всё ещё имеющихся для выполнения следующей команды GET RESPONSE.
- ◆ Если команда не поддерживается (протокол T=1), карточка выдает '6D00'.

### 3.5.7 PSO: VERIFY CERTIFICATE

Данная команда соответствует стандарту ISO/IEC 7816-8, однако её использование ограничено по сравнению с командой, определённой в указанном стандарте.

Команда VERIFY CERTIFICATE используется карточкой для получения открытого ключа извне и проверки его действительности.

#### 3.5.7.1 Команда первого поколения – пара ответов

- 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 прямо конфигурируется для использования команд, связанных с защитой (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE или VERIFY CERTIFICATE) с помощью команды MSE (см. пункт 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 Европы.
- TCS\_84 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'2Ah'	Выполнение операции обеспечения безопасности
P1	1	'00h'	P1
P2	1	'AEh'	P2: закодированные данные к классу BER-TLV не относятся (конкатенация элементов данных)
Lc	1	'C2h'	Lc : Длина сертификата, 194 байта
#6- #199	194	'XX..XXh'	Сертификат: конкатенация элементов данных (как указано в приложении 11)

- TCS\_85 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- ◆ Если команда проходит успешно, карточка выдаёт '9000'.
- ◆ Если проверка сертификата не удалась, статус обработки выдаётся в виде '6688'. Процесс проверки и расшифровки сертификата для первого и второго поколений описан в приложении 11.
- ◆ Если открытый ключ среды защиты отсутствует, выдается '6A88'.
- ◆ Если выбранный открытый ключ (используемый для расшифровки сертификата) считается повреждённым, статус обработки выдаётся в виде '6400' или '6581'.
- ◆ Только для первого поколения: Если параметр выбранного открытого ключа (используемого для расшифровки сертификата) CHA.LSB (CertificateHolderAuthorisation.equipmentType) отличается от '00' (т.е. не является ключом государства-члена или Европы), статус обработки выдаётся в виде '6985'.

#### 3.5.7.2 Команда второго поколения – пара ответов

В зависимости от размера кривой сертификаты ECC могут быть такими длинными, что их невозможно будет передать в одном APDU. В подобном случае должно применяться формирование цепочки команд в соответствии с ISO/IEC 7816-4, и сертификат передаётся двумя последовательными APDU PSO: Verify Certificate.

Структура сертификата и параметры области представлены в приложении 11.

- TCS\_86 Команда может выполняться в MF, DF Tachograph и DF Tachograph\_G2; также см. TCS\_33.

## TCS\_87 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'X0h'	Байт CLA, указывающий на формирование цепочки команд: '00h' единственная или последняя команда цепочки '10h' не последняя команда цепочки
INS	1	'2Ah'	Выполнение операции обеспечения безопасности
P1	1	'00h'	
P2	1	'BEh'	Проверка самодокументированного сертификата
Lc	1	'XXh'	Длина поля командных данных; см. TCS_88 и TCS_89.
#6- #5+L	L	'XX..XXh'	Данные, закодированные в DER-TLV: Объект данных сертифицирующего органа ЕСС как первый объект данных, конкатенированный с объектом данных подписи сертификата ЕСС как вторым объектом данных, или частью этой конкатенации. Метка '7F21' и соответствующая длина не передаются. Последовательность этих объектов данных фиксирована.

TCS\_88 В отношении коротких APDU применяются следующие положения: IFD использует минимальное число APDU, требуемое для передачи команды, и передаёт максимальное число байтов в первой команде APDU в соответствии со значением байтов карточки размера информационного поля; см. TCS\_14. Если IFD ведёт себя по-другому, поведение карточки в область применения не попадает.

TCS\_89 В отношении APDU расширенной длины применяются следующие положения: Если сертификат не помещается в один APDU, карточка поддерживает формирование цепочек команд. IFD использует минимальное число APDU, требуемое для передачи команды, и передаёт максимальное число байтов в первой команде APDU. Если IFD ведёт себя по-другому, поведение карточки в область применения не попадает.

Примечание: В соответствии с приложением 11 карточка сохраняет сертификат или соответствующее содержание сертификата и обновляет его currentAuthenticatedTime.

Структура ответного сообщения и характеристики статуса представлены в TCS\_85.

TCS\_90 Помимо кодов ошибок, перечисленных в TCS\_85, карточка может выдавать следующие коды ошибок:

- ◆ Если параметр выбранного открытого ключа (используемого для расшифровки сертификата) CHA.LSB (CertificateHolderAuthorisation.equipmentType), который не подходит для проверки сертификата соответствии с приложением 11, статус обработки выдаётся в виде '6985'.
- ◆ Если значение currentAuthenticatedTime карточки позднее, чем дата истечения срока действия сертификата, статус обработки выдаётся в виде '6985'.
- ◆ Если ожидается последняя команда цепочки, карточка выдаёт '6883'.
- ◆ Если в поле командных данных передаются неверные параметры, карточка выдаёт '6A80' (как и в случае, когда объекты данных не передаются в определённом порядке).

### 3.5.8 INTERNAL AUTHENTICATE

Данная команда соответствует стандарту ISO/IEC 7816-4.

- TCS\_91 Данную команду поддерживают все карточки тахографов в DF Tachograph первого поколения. Команда может быть доступной или недоступной в MF и/или DF Tachograph\_G2. Если она доступна, она прерывается при помощи подходящего кода ошибки, так как закрытый ключ карточки (Card.SK) для протокола аутентификации первого поколения доступен только в DF\_Tachograph первого поколения.

Используя команду INTERNAL AUTHENTICATE, IFD может произвести аутентификацию карточки. Процесс аутентификации описывается в приложении 11. Он включает в себя следующие сообщения:

- TCS\_92 Команда INTERNAL AUTHENTICATE использует закрытый ключ карточки (выбранный по косвенным признакам) для подтверждения данных аутентификации, включая K1 (первый элемент, указывающий на соответствие ключа сеанса) и RND1, и использует открытый ключ, выбранный в данный момент (на основании последней команды MSE) для шифрования подписи и создания маркера аутентификации (более подробно см. в приложении 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, переданных на карточку
#6 - #13	8	'XX..XXh'	Запрос, использованный для аутентификации карточки
#14 - #21	8	'XX..XXh'	VU.CHR (см. приложение 11)
Le	1	'80h'	Длина данных, ожидаемых с карточки

- TCS\_94 **Ответное сообщение**

Байт	Длина	Значение	Описание
#1-#128	128	'XX..XXh'	Маркер аутентификации карточки (см. приложение 11)
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- ◆ Если команда проходит успешно, карточка выдаёт '9000'.
- ◆ Если открытый ключ среды защиты отсутствует, статус обработки выдаётся в виде '6A88'.
- ◆ Если закрытый ключ среды защиты отсутствует, статус обработки выдаётся в виде '6A88'.
- ◆ Если VU.CHR не соответствует данному идентификатору открытого ключа, статус обработки выдаётся в виде '6A88'.
- ◆ Если выбранный закрытый ключ считается повреждённым, статус обработки выдаётся в виде '6400' или '6581'.

- TCS\_95 Если команда INTERNAL AUTHENTICATE проходит, ключ текущего сеанса, если он существует, стирается и более не доступен. Для создания нового ключа сеанса должна быть успешно выполнена команда EXTERNAL AUTHENTICATE для механизма аутентификации первого поколения.

### 3.5.9 EXTERNAL AUTHENTICATE

Данная команда соответствует стандарту ISO/IEC 7816-4.

Используя команду EXTERNAL AUTHENTICATE, карточка может произвести аутентификацию IFD. Процесс аутентификации описывается в приложении 11 для тахографов первого и второго поколений (аутентификация БУ).

TCS\_96 Вариант команды для механизма взаимной аутентификации первого поколения поддерживается только приложением тахографа первого поколения.

TCS\_97 Вариант команды для взаимной аутентификации БУ и карточки второго поколения может выполняться в MF, DF Tachograph и DF Tachograph\_G2; также см. TCS\_34.

TCS\_98 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Косвенно известные ключи и алгоритмы
P2	1	'00h'	
Lc	1	'XXh'	Lc (Длина данных, переданных на карточку)
#6-#(5+L)	L	'XX..XXh'	Аутентификация для первого поколения: Криптограмма (см. часть А приложения 11) Аутентификация для второго поколения: Подпись, которую генерирует IFD (см. часть Б приложения 11)

TCS\_99 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт '9000'.
- Если CHA выбранного открытого ключа не соответствует конкатенации AID приложения тахографа и типа БУ, статус обработки выдаётся в виде '6F00'.
- Если этой команде не предшествует непосредственно команда GET CHALLENGE, статус обработки выдаётся в виде '6985'.

Приложение тахографа первого поколения может выдавать следующие дополнительные коды ошибок:

- Если открытый ключ среды защиты отсутствует, выдаётся '6A88'.
- Если закрытый ключ среды защиты отсутствует, статус обработки выдаётся в виде '6A88'.
- Если проверка криптограммы показала неправильный результат, статус обработки выдаётся в виде '6688'.
- Если выбранный закрытый ключ считается повреждённым, статус обработки выдаётся в виде '6400' или '6581'.

Вариант команды для аутентификации для второго поколения может выдать следующий дополнительный код ошибки:

- Если проверка подписи не удалась, карточка выдаёт '6300'.



### 3.5.10 GENERAL AUTHENTICATE

Данная команда используется для протокола аутентификации микросхемы второго поколения, как указано в части Б приложения 11, и соответствует ISO/IEC 7816-4.

TCS\_100 Команда может выполняться в MF, DF Tachograph и DF Tachograph\_G2; также см. TCS\_34.

#### TCS\_101 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Косвенно известные ключи и протокол
P2	1	'00h'	
Lc	1	'NNh'	Lc: длина последующего поля данных
#6-#(5+L)	L	'7Ch' + L <sub>7C</sub> + '80h' + L <sub>80</sub> + 'XX..XXh'	Динамическое значение открытого ключа, закодированного в DER-TLV (см. приложение 11) БУ передаёт объекты данных в этом порядке.

#### TCS\_102 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#L	L	'7Ch' + L <sub>7C</sub> + '81h' + '08h' + 'XX..XXh' + '82h' + L <sub>82</sub> + 'XX..XXh'	Данные динамической аутентификации, закодированные в DER-TLV: временное значение и маркер аутентификации (см. приложение 11)
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- ◆ Если команда проходит успешно, карточка выдаёт '9000'.
- ◆ Карточка выдаёт '6A80', чтобы указать на неверные параметры в поле данных.
- ◆ Карточка выдаёт '6982', если команду External Authenticate не удалось выполнить успешно.

Ответ объекта данных динамической аутентификации '7Ch'

- должен выдаваться, если операция выполнена успешно, т.е. характеристика статуса – '9000',
- должен отсутствовать в случае ошибки выполнения или проверки, т.е. характеристики статуса находятся в интервале '6400' – '6FFF', и
- может отсутствовать в случае предупреждения, т.е. характеристики статуса находятся в интервале '6200' – '63FF'.

### 3.5.11 MANAGE SECURITY ENVIRONMENT

Данная команда используется для определения открытого ключа в целях аутентификации.

#### 3.5.11.1 Команда первого поколения – пара ответов

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 первого поколения.

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) отсутствует на карточке, среда защиты остаётся без изменений.

TCS\_106 **Командное сообщение**

Байт	Длина	Значение	Описание
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, касающиеся цифровой подписи)
Lc	1	'0Ah'	Lc: длина последующего поля 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, указанный в приложении 11

TCS\_107 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт '**9000**'.
- Если указанный ключ на карточке отсутствует, статус обработки выдаётся в виде '**6A88**'.
- Если некоторые ожидаемые объекты данных в формате защищённого обмена сообщениями отсутствуют, статус обработки выдаётся в виде '**6987**'. Это может произойти, если отсутствует метка '83h'.
- Если некоторые объекты данных неверны, статус обработки выдаётся в виде '**6988**'. Это может произойти в том случае, если длина идентификатора ключа не соответствует '08h'.
- Если выбранный ключ считается повреждённым, статус обработки выдаётся в виде '**6400**' или '**6581**'.

#### 3.5.11.2 Команда второго поколения – пары ответов

Для аутентификация для второго поколения карточки тахографа поддерживает следующую команду MSE: Установленные версии команды, соответствующие стандарту ISO/IEC 7816-4. Данные версии команды не поддерживаются для аутентификации для первого поколения.

##### 3.5.11.2.1 MSE:SET AT для аутентификации микросхемы

Следующая команда MSE:SET AT используется для выбора параметров аутентификации микросхемы, проводимой при помощи следующей команды General Authenticate.

TCS\_108 Команда может выполняться в MF, DF Tachograph и DF Tachograph\_G2; также см. 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'	Установлено для внутренней аутентификации
P2	1	'A4h'	Аутентификация
Lc	1	'NNh'	Lc: длина последующего поля данных
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Указанный криптографический механизм, закодированный в DER-TLV: Идентификатор объекта аутентификации микросхемы (только значение, метка '06h' опускается). Значения идентификаторов объектов см. в приложении 1; применяется нотация байтов. По вопросу, как выбирать один из этих идентификаторов объектов, см. приложение 11.

**3.5.11.2.2 MSE:SET AT для аутентификации БУ**

Следующая команда MSE:SET AT используется для выбора параметров и ключей аутентификации БУ, проводимой при помощи следующей команды External Authenticate.

TCS\_110 Команда может выполняться в MF, DF Tachograph и DF Tachograph\_G2; также см. 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'	Установлено для внешней аутентификации
P2	1	'A4h'	Аутентификация
Lc	1	'NNh'	Lc: длина последующего поля данных
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Указанный криптографический механизм, закодированный в DER-TLV: Идентификатор объекта аутентификации БУ (только значение, метка '06h' опускается). Значения идентификаторов объектов см. в приложении 1; применяется нотация байтов. По вопросу, как выбирать один из этих идентификаторов объектов, см. приложение 11.
		'83h' + '08h' + 'XX..XXh'	Указание на открытый ключ БУ, закодированное в DER-TLV, в рамках указания держателя сертификата, упомянутого в сертификате.
		'91h' + L <sub>91</sub> + 'XX..XXh'	Компактное выражение динамического открытого ключа БУ, закодированное в DER-TLV, которое будет использоваться для аутентификации микросхемы (см. приложение 11)

**3.5.11.2.3 MSE:SET DST**

Следующая команда MSE:SET DST используется для установления открытого ключа

- ◆ для проверки подписи при помощи последующей команды PSO: Verify Digital Signature или
- ◆ для проверки подписи сертификата при помощи последующей команды PSO: Verify Certificate

TCS\_112 Команда может выполняться в MF, DF Tachograph и DF Tachograph\_G2; также см. TCS\_33.

TCS\_113 **Командное сообщение MSE:SET DST**

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Установлено для проверки
P2	1	'B6h'	Цифровая подпись
Lc	1	'NNh'	Lc: длина последующего поля данных
#6-#(5+L)	L	'83h' + '08h' + 'XX...XXh'	Указание на открытый ключ, закодированное в DER-TLV, т.е. указание держателя сертификата в сертификате открытого ключа (см. приложение 11)

Для всех версий команды структура ответного сообщения и характеристики статуса задаются следующим образом:

TCS\_114 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- ◆ Если команда проходит успешно, карточка выдаёт '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.

### 3.5.12 PSO: HASH

Данная команда используется для передачи карточке результата расчёта хеширования некоторых данных. Она используется для проверки цифровых подписей. Значение хэша 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 контрольная карточка.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду. Команда может быть доступной или недоступной в MF.

Приложение контрольной карточки первого поколения поддерживает только SHA-1.

TCS\_115 Временно хранящееся значение хеширования удаляется, если при помощи команды PSO: HASH вычисляется новое значение хеширования, если выбран DF и если произведена перезагрузка карточки тахографа.

#### TCS\_116 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Выполнение операции обеспечения безопасности
P1	1	'90h'	Возврат хеш-кода
P2	1	'A0h'	Метка: поле данных содержит объекты данных, относящиеся к хешированию
Lc	1	'XXh'	Длина Lc последующего поля данных
#6	1	'90h'	Метка для хеш-кода
#7	1	'XXh'	Длина L хеш-кода: '14h' для приложения первого поколения (см. часть А приложения 11) '20h', '30h' или '40h' для приложения второго поколения (см. часть Б приложения 11)
#8-#(7+L)	L	'XX..XXh'	Хеш-код

#### TCS\_117 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт '9000'.
- Если некоторые ожидаемые объекты данных (как указано выше) отсутствуют, статус обработки выдаётся в виде '6987'. Это может произойти, если отсутствует одна из меток '90h'.
- Если некоторые объекты данных неверны, статус обработки выдаётся в виде '6988'. Данная ошибка возникает, если требуемая метка присутствует, но её 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 второго поколения).

### 3.5.13 PERFORM HASH of FILE

Данная команда не 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 контрольная карточка выполняют данную команду, она выполняется, как указано в настоящей главе.

Команда может быть доступной или недоступной в MF. Если она доступна, команда выполняется так, как указано в настоящей главе, т.е. не позволяет вычислять значение хеширования и прерывается на основании подходящего 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 для EF, перечисленных в главе 4 в DF\_Tachograph и DF\_Tachograph\_G2 с учётом следующего исключения. Карточка тахографа не поддерживает команду для EF Sensor\_Installation\_Data в DF Tachograph\_G2..

TCS\_120 Результат операции хеширования временно хранится на карточке. Он может затем использоваться для получения цифровой подписи файла с использованием команды PSO: COMPUTE DIGITAL SIGNATURE.

TCS\_121 Временно хранящееся значение хеширования удаляется, если при помощи команды PSO: HASH FILE вычисляется новое значение хеширования, если выбран DF и если произведена перезагрузка карточки тахографа.

TCS\_122 Приложение тахографа первого поколения поддерживает SHA-1.

TCS\_123 Приложение тахографа второго поколения поддерживает SHA-1 и SHA-2 (256, 384 и 512 бит).

TCS\_124 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'80h'	CLA
INS	1	'2Ah'	Выполнение операции обеспечения безопасности
P1	1	'90h'	Метка: Хеш
P2	1	'XXh'	P2: Указывает на алгоритм, используемый для хеширования данных выбранного в данный момент транспарентного файла: '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 статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт '9000'.
- Если текущий EF не позволяет выполнять такую команду (EF Sensor\_Installation\_Data в DF Tachograph\_G2), статус обработки выдаётся в виде '6985'.
- Если выбранный EF считается повреждённым (в атрибутах файла или хранящихся данных обнаружены ошибки целостности), статус обработки выдаётся в виде '6400' или '6581'.
- Если выбранный файл не является транспарентным файлом или нет текущего EF, статус обработки выдаётся в виде '6986'.

### 3.5.14 PSO: COMPUTE DIGITAL SIGNATURE

Данная команда используется для расчёта цифровой подписи ранее рассчитанного хеш-кода (см. PERFORM HASH of FILE, пункт 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, но для них нет ключа подписи. Таким образом, такие карточки не могут успешно выполнять эту команду и прерывают её на основании подходящего кода ошибки.

Команда может быть доступной или недоступной в MF. Если она доступна, она прерывается при помощи подходящего кода ошибки.

Данная команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению 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 расчёта цифровой подписи и известен карточке по косвенным признакам.

TCS\_128 Приложение тахографа первого поколения производит цифровую подпись с использованием метода заполнения, соответствующего PKCS1 (более подробно см. приложение 11).

TCS\_129 Приложение тахографа второго поколения рассчитывает цифровую подпись на основе эллиптической кривой (более подробно см. приложение 11).

#### TCS\_130 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Выполнение операции обеспечения безопасности
P1	1	'9Eh'	Цифровая подпись, подлежащая возврату
P2	1	'9Ah'	Метка: поле данных содержит данные, требующие подписи. Если 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 рассчитанного хеширования
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт '9000'.
- Если косвенно выбранный закрытый ключ считается повреждённым, статус обработки выдаётся в виде '6400' или '6581'.
- Если хеш, рассчитанный в рамках предыдущей команды Perform Hash of File, статус обработки выдаётся в виде '6985'.

### 3.5.15 PSO: VERIFY DIGITAL SIGNATURE

Данная команда используется для проверки цифровой подписи, представленной в качестве входных данных, хеш-код которых 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 контрольная карточка.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду. Команда может быть доступной или недоступной в MF.

TCS\_132 Команда VERIFY DIGITAL SIGNATURE всегда использует открытый ключ, выбранный на основании предыдущей команды Manage Security Environment MSE: 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 обеспечения безопасности
P1	1	'00h'	
P2	1	'A8h'	Метка: поле данных содержит объекты данных, относящиеся к проверке
Lc	1	'83h'	Длина Lc последующего поля данных
6	1	'9Eh'	Метка, указывающая на цифровую подпись
#7-#8	2	'81 XXh'	Длина цифровой подписи: 128 байтов, закодированные в соответствии с частью А приложения 11 для приложения тахографа первого поколения В зависимости от выбранной кривой для приложения тахографа второго поколения (см. часть Б приложения 11)
#9-#(8+L)	L	'XX..XXh'	Содержание цифровой подписи

#### TCS\_134 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- ◆ Если команда проходит успешно, карточка выдаёт '**9000**'.
- ◆ Если проверка подписи показала неправильный результат, статус обработки выдаётся в виде '**6688**'. Процесс проверки описывается в приложении 11.
- ◆ Если открытый ключ не выбран, статус обработки выдаётся в виде '**6A88**'.
- ◆ Если некоторые ожидаемые объекты данных (как указано выше) отсутствуют, статус обработки выдаётся в виде '**6987**'. Это может произойти, если отсутствует одна из требуемых меток.
- ◆ Если хеш-кода для обработки команды нет (в результате предыдущей команды PSO: Hash), статус обработки выдаётся в виде '**6985**'.
- ◆ Если некоторые объекты данных неверны, статус обработки выдаётся в виде '**6988**'. Это может произойти, если длина одного из требуемых объектов данных неверна.
- ◆ Если выбранный открытый ключ считается повреждённым, статус обработки выдаётся в виде '**6400**' или '**6581**'.



### 3.5.16 PROCESS DSRC MESSAGE

Данная команда используется для проверки целостности и подлинности 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, часть Б, глава 13.

Для поддержки данной команды в DF Tachograph\_G2 требуется только контрольная карточка и карточка мастерской.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду, но для них нет главного ключа DSRC. Таким образом, такие карточки не могут успешно выполнять эту команду и прерывают её на основании подходящего кода ошибки.

Команда может быть доступной или недоступной в MF и/или DF Tachograph. Если она доступна, она прерывается при помощи подходящего кода 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**

Байт	Длина	Значение	Описание
CLA	1	'80h'	Собственный CLA
INS	1	'2Ah'	Выполнение операции обеспечения безопасности
P1	1	'80h'	Ответные данные: простое значение
P2	1	'B0h'	Командные данные: простое значение, закодированное в BER-TLV и включающее в себя объекты данных SM
Lc	1	'NNh'	Длина Lc последующего поля данных
#6-#(5+L)	L	'87h' + L <sub>87</sub> + 'XX..XXh'	Байт показателя заполненного содержания, закодированный в DER-TLV, с последующими зашифрованными данными тахографа. Для байта показателя заполненного содержания используется значение '00h' (в соответствии с таблицей 52 стандарта ISO/IEC 7816-4:2013 «дополнительно не указывается»). По вопросу механизма шифрования см. приложение 11, часть Б, глава 13. Допустимые значения длины L <sub>87</sub> являются кратными длине блока AES плюс 1 с учётом байта показателя заполненного содержания, т.е. с 17 байтов и выше и включая 193 байтов.  Примечание: См. таблицу 49 стандарта ISO/IEC 7816-4:2013 по поводу объекта данных SM с меткой '87h'.

		‘81h’ + ‘10h’	<p>Шаблон управляющих ссылок конфиденциальности, закодированный в DER-TLV, в котором хранится конкатенация следующих элементов данных (см. приложение 1, DSRCSecurityData и приложение 11, часть Б, глава 13):</p> <ul style="list-style-type: none"> <li>• отметка времени 4 байта</li> <li>• счётчик 3 байта</li> <li>• серийный номер БУ 8 байтов</li> <li>• версия главного ключа DSRC 1 байт</li> </ul> <p>Примечание: См. таблицу 49 стандарта ISO/IEC 7816-4:2013 по поводу объекта данных SM с меткой ‘81h’.</p>
		‘8Eh’ + L <sub>8E</sub> + ‘XX..XXh’	<p>MAC, закодированный в DER-TLV, в рамках сообщения DSRC. По вопросу алгоритма и расчёта MAC см. приложение 11, часть Б, глава 13.</p> <p>Примечание: См. таблицу 49 стандарта ISO/IEC 7816-4:2013 по поводу объекта данных SM с меткой ‘8Eh’.</p>

## TCS\_139 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#L	L	‘XX..XXh’	Данные отсутствуют (в случае ошибки) или расшифрованы (без заполнения)
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘9000’.
- ‘6A80’ указывает на то, что в поле данных команды содержатся неверные параметры (как и в случае, когда объекты данных не передаются в определённом порядке).
- ‘6A88’ указывает на то, что указанные данные отсутствуют, т.е. указанный главный ключ DSRC не доступен.
- ‘6900’ указывает на то, что проверка криптографической контрольной суммы или расшифровка данных дали неверный результат.

#### 4. Структура карточек тахографов

В настоящем пункте уточняются структуры файлов карточек тахографа для хранения доступных данных.

В нём не указываются внутренние структуры, определяемые по усмотрению производителя, 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 первого и второго поколений одного и того же типа (например, приложения карточки водителя).

TCS\_141 Карточка тахографа поддерживает хотя бы минимальное число записей, указанное для соответствующих приложений, и не поддерживает число записей, превышающее максимальное число записей, указанное для соответствующих приложений.

Максимальное и минимальное числа записей в настоящей главе указываются для различных приложений.

Относительно условий безопасности, применяемых в правилах доступа во всей настоящей главе, см. главу 3.3. В целом, режим доступа Read обозначает команду READ BINARY с чётным и, если поддерживается, нечётным байтом INS, за исключением EF Sensor\_Installation\_Data на карточке мастерской; см. TCS\_156 и TCS\_160. Режим доступа Update обозначает команду Update Binary с чётным и, если поддерживается, нечётным байтом INS, а режим доступа Select – команду SELECT.

#### 4.1. Главный файл MF

TCS\_142 После персонализации главный файл MF имеет следующую постоянную структуру файла и правила доступа к файлам:

Примечание: Короткий идентификатор SFID файла EF присваивается как десятичное число, например, значение 30 в двоичной системе соответствует величине 11110.

Файл	ИД файла	SFID	Правила доступа	
			Read / Select	Update
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 (условно)	'0006h'	28	ALW	NEV
— DF Tachograph	'0500h'		SC1	
— DF Tachograph G2			SC1	

В настоящей таблице для условия безопасности используется следующее сокращение:

SC1 ALW 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	6		184	

EF	ICC	25	25	
	└ CardIccIdentification	25	25	
	└ clockStop	1	1	{00}
	└ cardExtendedSerialNumber	8	8	{00..00}
	└ cardApprovalNumber	8	8	{20..20}
	└ cardPersonaliserID	1	1	{00}
	└ embedderIcAssemblerId	5	5	{00..00}
	└ icIdentifier	2	2	{00 00}
EF	IC	8	8	
	└ CardChipIdentification	8	8	
	└ icSerialNumber	4	4	{00..00}
	└ icManufacturingReferences	4	4	{00..00}
EF	DIR	20	20	
	└ Cm. TCS_145	20	20	{00..00}
EF	ATR/INFO	7	128	
	└ Cm. TCS_146	7	128	{00..00}
EF	EXTENDED_LENGTH	3	3	
	└ Cm. TCS_147	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 ATR/INFO присутствует, если карточка тахографа в своей ATR указывает, что поддерживает поля расширенной длины. В данном случае EF ATR/INFO содержит объект данных информации расширенной длины (DO'7F66'), как указано в стандарте ISO/IEC 7816-4:2013, положение 12.7.1.

TCS\_147 Элементарный файл EF Extended\_Length присутствует, если карточка тахографа в своей ATR указывает, что поддерживает поля расширенной длины. В данном случае EF содержит следующий объект данных: '02 01 xx', где значение 'xx' показывает, поддерживаются ли поля расширенной длины для протокола T = 1 и/или T = 0. Значение '01' указывает, что поле расширенной длины поддерживается для протокола T = 1. Значение '10' указывает, что поле расширенной длины поддерживается для протокола T = 0. Значение '11' указывает, что поле расширенной длины поддерживается для протоколов T = 1 и T = 0.

## 4.2. Приложения карточки водителя

### 4.2.1 Приложение карточки водителя первого поколения

TCS\_148 После персонализации приложение карточки водителя первого поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

Файл	ИД файла	Правила доступа		
		Read	Select	Update
└ 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 OR SM-MAC-G2

**SC2** ALW OR SM-MAC-G1 OR SM-MAC-G2

**SC3** SM-MAC-G1 OR SM-MAC-G2

TCS\_149 Все структуры EF прозрачны.

TCS\_150 Приложение карточки водителя первого поколения имеет следующую структуру данных:

Файл/Элемент данных	Число записей	Размер (байты)		Значения по
		Мин.	Макс.	
└ 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}	
└└└ 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	{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	
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 <sub>1</sub>	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 <sub>2</sub>	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 <sub>6</sub>	5544	13776	{00..00}

EF Vehicles_Used		2606	6202	
└ CardVehiclesUsed		2606	6202	
└─ vehiclePointerNewestRecord		2	2	{00 00}
└─ cardVehicleRecords		2604	6200	
└─┬ cardVehicleRecords	n <sub>3</sub>	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		841	1121	
└ CardPlaceDailyWorkPeriod		841	1121	
└─ placePointerNewestRecord		1	1	{00}
└─ placeRecords		840	1120	
└─┬ PlaceRecord	n <sub>4</sub>	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 размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки водителя в приложении первого поколения:

Мин.	Макс.
------	-------

---

n <sub>1</sub>	NoOfEventsPerType	6	12
n <sub>2</sub>	NoOfFaultsPerType	12	24
n <sub>3</sub>	NoOfCardVehicleRecords	84	200
n <sub>4</sub>	NoOfCardPlaceRecords	84	112
n <sub>6</sub>	CardActivityLengthRange	5544 байтов (28 дней * 93 изменений вида деятельности)	13776 байтов (28 дней * 240 изменений вида деятельности)



## 4.2.2 Приложение карточки водителя второго поколения

TCS\_152 После персонализации приложение карточки водителя второго поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

Примечание: Короткий идентификатор SFID файла EF присваивается как десятичное число, например, значение 30 в двоичной системе соответствует величине 11110.

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 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

В настоящей таблице для условия безопасности используется следующее сокращение:

**SC1** ALW OR SM-MAC-G2

TCS\_153 Все структуры EF прозрачны.

TCS\_154 Приложение карточки водителя второго поколения имеет следующую структуру данных:

Файл/Элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
└─DF Tachograph_G2		19510	39306	
└─EF Application_Identification		15	15	
└─└─DriverCardApplicationIdentification		15	15	
└─└─└─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}
└─└─└─noOfGNSSCDRecords		2	2	{00 00}
└─└─└─noOfSpecificConditionRecords		2	2	{00}
└─EF CardMA_Certificate		204	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		143	143	
└ CardIdentification		65	65	
└└ cardIssuingMemberState		1	1	{00}
└└ cardNumber		16	16	{20..20}
└└ cardIssuingAuthorityName		36	36	{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	
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		1584	3168	
└ CardEventData		1584	3168	
└└ cardEventRecords	11	144	288	
└└└ CardEventRecord	n <sub>1</sub>	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 <sub>2</sub>	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 <sub>6</sub>	5544	13776	{00..00}
EF Vehicles_Used		4034	9602	
└ CardVehiclesUsed		4034	9602	
└ vehiclePointerNewestRecord		2	2	{00 00}
└ cardVehicleRecords		4032	9600	
└ cardVehicleRecords	n <sub>3</sub>	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		1766	2354	
└ CardPlaceDailyWorkPeriod		1766	2354	
└ placePointerNewestRecord		2	2	{00 00}
└ placeRecords		1764	2352	
└ PlaceRecord	n <sub>4</sub>	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	Specific_Conditions	282	562	
	└ SpecificConditions	282	562	
	└┐ conditionPointerNewestRecord	2	2	{00 00}
	└┐ specificConditionRecords	280	560	
	└┐┐ SpecificConditionRecord	n <sub>9</sub>	5	5
	└┐┐┐ entryTime	4	4	{00..00}
	└┐┐┐ specificConditionType	1	1	{00}
EF	VehicleUnits_Used	842	2002	
	└ CardVehicleUnitsUsed	842	2002	
	└┐ vehicleUnitPointerNewestRecord	2	2	{00 00}
	└┐ cardVehicleUnitRecords	840	2000	
	└┐┐ CardVehicleUnitRecord	n <sub>7</sub>	10	10
	└┐┐┐ timeStamp	4	4	{00..00}
	└┐┐┐ manufacturerCode	1	1	{00}
	└┐┐┐ deviceID	1	1	{00}
	└┐┐┐ vuSoftwareVersion	4	4	{00..00}
EF	GNSS_Places	3782	5042	
	└ GNSSContinuousDriving	3782	5042	
	└┐ gnssCDPointerNewestRecord	2	2	{00 00}
	└┐ gnssContinuousDrivingRecords	3780	5040	{00}
	└┐┐ GNSSContinuousDrivingRecord	n <sub>8</sub>	15	15
	└┐┐┐ timeStamp	4	4	{00..00}
	└┐┐┐ gnssPlaceRecord	11	11	
	└┐┐┐┐ timeStamp	4	4	{00..00}
	└┐┐┐┐ gnssAccuracy	1	1	{00}
	└┐┐┐┐ geoCoordinates	6	6	{00..00}

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 <sub>1</sub>	NoOfEventsPerType	6	12
n <sub>2</sub>	NoOfFaultsPerType	12	24
n <sub>3</sub>	NoOfCardVehicleRecords	84	200
n <sub>4</sub>	NoOfCardPlaceRecords	84	112
n <sub>6</sub>	CardActivityLengthRange	5544 байтов (28 дней * 93 изменений вида деятельности)	13776 байтов (28 дней * 240 изменений вида деятельности)
n <sub>7</sub>	NoOfCardVehicleUnitRecords	84	200
n <sub>8</sub>	NoOfGNSSCDRecords	252	336
n <sub>9</sub>	NoOfSpecificConditionRecords	56	112

### 4.3. Приложения карточки мастерской

#### 4.3.1 Приложение карточки мастерской первого поколения

TCS\_156 После персонализации приложение карточки мастерской первого поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

Файл	ИД файла	Правила доступа		
		Read	Select	Update
└ 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	<b>SC1</b>
└└ EF Calibration	'050Ah'	SC2	SC1	SC3
└└ EF Sensor_Installation_Data	'050Bh'	<b>SC4</b>	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 OR SM-MAC-G2

**SC2** ALW OR SM-MAC-G1 OR SM-MAC-G2

**SC3** SM-MAC-G1 OR SM-MAC-G2

**SC4** Для команды READ BINARY с чётным байтом INS:

(PLAIN-C AND SM-R-ENC-G1) OR (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 нечётным байтом INS (если поддерживается): NEV

TCS\_157 Все структуры EF прозрачны.

TCS\_158 Приложение карточки мастерской первого поколения 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}

---

└─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	n <sub>5</sub>	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}
└└└└ 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	
└└└└ 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		126	250	
└ CardVehiclesUsed		126	250	
└└ vehiclePointerNewestRecord		2	2	{00 00}
└└ cardVehicleRecords		124	248	
└└└ cardVehicleRecords	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	
└└└└ 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	{00..00}
SpecificConditionType		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 первого поколения:

		Мин.	Макс.
n <sub>1</sub>	NoOfEventsPerType	3	3
n <sub>2</sub>	NoOfFaultsPerType	6	6
n <sub>3</sub>	NoOfCardVehicleRecords	4	8
n <sub>4</sub>	NoOfCardPlaceRecords	6	8
n <sub>5</sub>	NoOfCalibrationRecords	88	255
n <sub>6</sub>	CardActivityLengthRange	198 байтов (1 день * 93 изменения вида деятельности)	492 байта (1 день * 240 изменений вида деятельности)

### 4.3.2 Приложение карточки мастерской второго поколения

TCS\_160 После персонализации приложение карточки мастерской второго поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

Примечание: Короткий идентификатор SFID файла EF присваивается как десятичное число, например, значение 30 в двоичной системе соответствует величине 11110.

Файл	ИД файла	SFID	Правила доступа		
			Read	Select	Update
└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	<b>SC5</b>	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

В настоящей таблице для условий безопасности используются следующие сокращения:

**SC1** ALW OR SM-MAC-G2

**SC5** Для команды Read Binary с чётным байтом INS: SM-C-MAC-G2 AND SM-R-ENC-MAC-G2  
Для команды Read Binary с нечётным байтом INS (если поддерживается): NEV

TCS\_161 Все структуры EF прозрачны.

TCS\_162 Приложение карточки мастерской второго поколения имеет следующую структуру данных:

Файл/Элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		Мин.	Макс.	
└DF Tachograph_G2		17837	47163	
└EF Application_Identification		17	17	
└└ WorkshopCardApplicationIdentification		17	17	
└└└ 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}
noOfCalibrationRecords	2	2	{00}
noOfGNSSCDRecords	2	2	{00..00}
noOfSpecificConditionRecords	2	2	{00..00}
EF CardMA_Certificate	204	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	14788	42844	
└ WorkshopCardCalibrationData	14788	42844	
└ calibrationTotalNumber	2	2	{00 00}
└ calibrationPointerNewestRecord	2	2	{00}
└ calibrationRecords	14784	42840	
└ WorkshopCardCalibrationRecord	n5	168	168
└ 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		46	46	
noOfSealRecords		1	1	{00}
SealRecords		45	45	
SealRecord	5	9	9	
equipmentType		1	1	{00}
extendedSealIdentifier		8	8	{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	n <sub>1</sub>	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	n <sub>2</sub>	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	n <sub>6</sub>	198	492	{00..00}
EF Vehicles_Used		194	386	
└─CardVehiclesUsed		194	386	
└─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		192	384	
└─cardVehicleRecords	n <sub>3</sub>	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	n <sub>4</sub>	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	n <sub>7</sub>	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		262	362	
└─GNSSContinuousDriving		262	362	
└─gnssCDPointerNewestRecord		2	2	{00 00}
└─gnssContinuousDrivingRecords		260	360	
└─GNSSContinuousDrivingRecord	n <sub>8</sub>	15	15	
└─timeStamp		4	4	{00..00}
└─gnssPlaceRecord		11	11	
└─timeStamp		4	4	{00..00}
└─gnssAccuracy		1	1	{00}
└─geoCoordinates		6	6	{00..00}
EF Specific_Conditions		12	22	
└─SpecificConditions		12	22	
└─conditionPointerNewestRecord		2	2	{00 00}
└─specificConditionRecords		10	20	
└─SpecificConditionRecord	n <sub>9</sub>	5	5	
└─entryTime		4	4	{00..00}
└─specificConditionType		1	1	{00}



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 второго поколения:

		Мин.	Макс.
n <sub>1</sub>	NoOfEventsPerType	3	3
n <sub>2</sub>	NoOfFaultsPerType	6	6
n <sub>3</sub>	NoOfCardVehicleRecords	4	8
n <sub>4</sub>	NoOfCardPlaceRecords	6	8
n <sub>5</sub>	NoOfCalibrationRecords	88	255
n <sub>6</sub>	CardActivityLengthRange	198 байтов (1 день * 93 изменения вида деятельности)	492 байта (1 день * 240 изменений вида деятельности)
n <sub>7</sub>	NoOfCardVehicleUnitRecords	4	8
n <sub>8</sub>	NoOfGNSSCDRecords	18	24
n <sub>9</sub>	NoOfSpecificConditionRecords	2	4

## 4.4. Приложения контрольной карточки

### 4.4.1 Приложение контрольной карточки первого поколения

TCS\_164 После персонализации приложение контрольной карточки первого поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

Файл	ИД файла	Правила доступа		
		Read	Select	Update
└ 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 прозрачны.

TCS\_166 Приложение контрольной карточки первого поколения 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}
└─ 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 контрольной карточки в приложении первого поколения:

		Мин.	Макс.
n7	NoOfControlActivityRecords	230	520

#### 4.4.2 Приложение контрольной карточки второго поколения

TCS\_168 После персонализации приложение контрольной карточки второго поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

Примечание: Короткий идентификатор SFID файла EF присваивается как десятичное число, например, значение 30 в двоичной системе соответствует величине 11110.

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

В настоящей таблице для условия безопасности используется следующее сокращение:  
**SC1** ALW OR SM-MAC-G2

TCS\_169 Все структуры EF прозрачны.

TCS\_170 Приложение контрольной карточки второго поколения имеет следующую структуру данных:

Файл/Элемент данных	Число записей	Размер (байты)	
		Мин.	Макс.
└ DF Tachograph_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,
└ cardIssueDate		4	4 {00..00}
└ cardValidityBegin		4	4 {00..00}
└ cardExpiryDate		4	4 {00..00}
└ ControlCardHolderIdentification		146	146
└ controlBodyName		36	36 {00,
└ controlBodyAddress		36	36 {00,
└ cardHolderName			
└ holderSurname		36	36 {00,
└ holderFirstNames		36	36 {00,

EF Controller_Activity_Data		10582	23922	{00..20}
└─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}

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 контрольной карточки в приложении второго поколения:

		Мин.	Макс.
n7	NoOfControlActivityRecords	230	520

## 4.5. Приложения карточки предприятия

### 4.5.1 Приложение карточки предприятия первого поколения

TCS\_172 После персонализации приложение карточки предприятия первого поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

Файл	ИД файла	Правила доступа		
		Read	Select	Update
└─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 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\_173 Все структуры EF прозрачны.

TCS\_174 Приложение карточки предприятия первого поколения имеет следующую структуру данных:

Файл/Элемент данных	Число	Размер (байты)	Значения
256			

	записей	Мин.	Макс.	по умолчанию
DF Tachograph	11114	24454		ю
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	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}	

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 первого поколения:

		Мин.	Макс.
n8	NoOfCompanyActivityRecords	230	520

## 4.5.2 Приложение карточки предприятия второго поколения

TCS\_176 После персонализации приложение карточки предприятия второго поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

Примечание: Короткий идентификатор SFID файла EF присваивается как десятичное число, например, значение 30 в двоичной системе соответствует величине 11110.

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 Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

В настоящей таблице для условия безопасности используется следующее сокращение:

**SC1** ALW OR SM-MAC-G2

TCS\_177 Все структуры EF прозрачны.

TCS\_178 Приложение карточки предприятия второго поколения 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}

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 второго поколения:

		Мин.	Макс.
n8	NoOfCompanyActivityRecords	230	520

RU

### Приложение 3. Пиктограммы

PIС\_001 Тахограф факультативно может использовать следующие пиктограммы и их комбинации (или пиктограммы и комбинации, достаточно похожие, чтобы их можно было недвусмысленно связать со следующими):

#### 5. Базовые пиктограммы

	<u>Люди</u>	<u>Действия</u>	<u>Режимы работы</u>
▢	Предприятие		Режим предприятия
▣	Контролёр	Контроль	Контрольный режим
⊖	Водитель	Управление	Рабочий режим
⊕	Мастерская/станция	Инспекция/калибровка	Режим калибровки
⊞	Производитель		
	<u>Деятельность</u>	<u>Продолжительность</u>	
⊞	Готовность	Текущий период готовности	
⊖	Управление	Непрерывное время управления	
⊞	Отдых	Текущий период отдыха	
⊞	Другая работа	Текущий период работы	
⊞	Перерыв	Суммарное время перерыва	
?	Неизвестно		
	<u>Оборудование</u>		<u>Функции</u>
1	Считывающее устройство водителя		
2	Считывающее устройство второго водителя		
▣	Карточка		
⊖	Часы		
▣	Дисплей		Отображение
⊕	Внешнее хранение		Загрузка
⊕	Питание		
⊕	Принтер/распечатка		Печать
⊞	Датчик		
⊞	Размер шин		
⊞	Транспортное средство/бортовое устройство		
⊞		Устройство ГНСС	
⊕	Средство удалённой связи		
⊞	Интерфейс ИТС		
	<u>Особые условия</u>		
OUT	Вне области применения		
⊞	Паром/ж/д переезд		
	<u>Разное</u>		



!	События	×	Неисправности
▮	Начало дневного периода работы	▮	Конец дневного периода работы
•	Местоположение		
M	Ручной ввод данных о деятельности водителя		
▮	Защита		
>	Скорость		
⊙	Время		
Σ	Итого/сумма		

### Уточнители

24 ч	Ежедневно
I	Еженедельно
II	Две недели
+	От и до

### 6. Сочетания пиктограмм

#### Разное

▮ •	Место контроля		
• ▮	Место начала дневного периода работы	▮ •	Место конца дневного периода работы
⊙ +	Со времени	+ ⊙	До времени
▮ +	Из транспортного средства		
OUT +	Вне области применения – начало	+ OUT	Вне области применения – конец

#### Карточки

⊙ ▮	Карточка водителя
▮ ▮	Карточка предприятия
▮ ▮	Контрольная карточка
T ▮	Карточка мастерской
▮---	Карточки нет

#### Управление

⊙ ⊙	Управление экипажем
⊙ I	Время управления за одну неделю
⊙ II	Время управления за две недели

#### Распечатки

24 ч ▮ ▮	Ежедневная распечатка данных о деятельности водителя, записанных на карточке
24 ч ▮ ▮	Ежедневная распечатка данных о деятельности водителя, записанных в БУ
! × ▮ ▮	Распечатка данных о событиях и неисправностях, хранящихся на карточке
! × ▮ ▮	Распечатка данных о событиях и неисправностях, хранящихся в БУ
T ⊙ ▮	Распечатка технических данных
> > ▮	Распечатка данных о превышении скорости

#### 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
- ! 📏 Ошибочные данные о движении
- ! 🗃 📏 Противоречивые данные о движении транспортного средства
- ! 🗃 Нарушение защиты
- ! ☉ Корректировка времени (в мастерской)
- > 🗃 Контроль превышения скорости

### **Неисправности**

- × 🗃 1 Неисправность карточки (считывающее устройство водителя)
- × 🗃 2 Неисправность карточки (считывающее устройство второго водителя)
- × 🗃 Неисправность дисплея
- × ⚡ Ошибка при загрузке
- × 🖨 Неисправность принтера
- × 📏 Неисправность датчика
- × 🗃 Внутренние неполадки в БУ
- × 🗃 Неисправность ГНСС
- × 🗃 Неисправность удалённого обнаружения

### **Процедура ручного ввода данных**

- 🗃 ? 🗃 Всё ещё тот же дневной период работы?
- 🗃 ? Конец предыдущего рабочего периода?
- 🗃 \* ? Подтвердить или ввести пункт окончания рабочего периода
- ☉ 🗃 ? Ввести время начала
- \* 🗃 ? Ввести пункт начала рабочего периода.

Примечание: Дополнительные комбинации пиктограмм, используемые в качестве идентификаторов блоков или записей данных при распечатке, представлены в приложении 4.

## RU

## Приложение 4. Распечатки

## СОДЕРЖАНИЕ

<b>1.</b>	<b>Общие положения .....</b>	<b>263</b>
<b>2.</b>	<b>Спецификация блоков данных.....</b>	<b>264</b>
<b>3.</b>	<b>Спецификации распечаток.....</b>	<b>272</b>
3.1.	Ежедневная распечатка данных о деятельности водителя, записанных на карточке .....	272
3.2.	Ежедневная распечатка данных о деятельности водителя, записанных в БУ .....	273
3.3.	Распечатка данных о событиях и неисправностях, хранящихся на карточке .....	274
3.4.	Распечатка данных о событиях и неисправностях, хранящихся в БУ .....	275
3.5.	Распечатка технических данных .....	275
3.6.	Распечатка данных о превышении скорости .....	276
3.7.	Архив вставленных карточек .....	276

**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 не печатается.

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 нуждается 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 (названия, фамилии, адреса) печатаются в форме, усечённой до размеров элемента данных.

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 (поля для пиктограмм или виды данных), вместо которых распечатываются соответствующие пиктограммы или значения,
- К названиям переменных параметров добавлены символы подчёркивания, 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: вид карточки, обозначаемый комбинацией соответствующих пиктограмм, код государства-члена, выдавшего карточку, наклонная черта вправо и номер карточки с индексом замены и индексом обновления, отделёнными пробелом:

Р	■	x	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 карточку				Первые 14 знаков номера карточки (могут включать порядковый индекс)															Индекс замены		Индекс								

PRT\_006 При распечатке данные делятся на блоки и/или записи данных, перечисляемые ниже с указанием их значения и формата:

Номер блока или записи  
Значение

Data Format

1 *Дата и время распечатки документа*

▼ dd/mm/yyyy hh:mm  
(UTC)

2 *Вид распечатки*

Идентификатор блока  
Комбинация пиктограмм распечатки (см. пр. 3),  
установка устройства ограничения скорости  
(только распечатка данных о превышении скорости)

-----▼-----  
Picto xxx **km/h**

3 **Идентификационные данные владельца карточки**

Идентификатор блока P = пиктограмма «люди»  
 Фамилия владельца карточки  
 Имя (имена) держателя карточки (если имеются)  
 Идентификационные данные карточки

Дата истечения срока действия карточки (если  
 есть) и номер поколения карточки (GEN 1 или  
 GEN 2)\*

-----P-----
P Last_Name_____
First_Name_____
Card_Identification_____
dd/mm/yyyy - GEN 2

На карточки, не принадлежащие конкретным лицам, вместо фамилии держателя наносится название предприятия, мастерской или контрольного органа.

\* Номер поколения карточки может печатать только «умный» тахограф.

4 **Идентификационные данные транспортного средства**

Идентификатор блока  
 VIN  
 Государство-член регистрации и VRN

-----A-----
A VIN_____
Nat/VRN_____

5 **Идентификационные данные БУ**

Идентификатор блока  
 Название производителя БУ  
 Номер детали БУ

Номер поколения БУ\*

-----B-----
B VU_Manufacturer_____
VU_Part_Number__
GEN 2

\* Номер поколения карточки может печатать только «умный» тахограф.

6 **Последняя калибровка тахографа**

Идентификатор блока  
 Название мастерской  
 Идентификационные данные карточки  
 мастерской  
 Дата калибровки

-----T-----
T
Last_Name_____
Card_Identification_____
T dd/mm/yyyy

7 **Последний контроль (проверка контролёром)**

Идентификатор блока  
 Идентификационные данные карточки контролёра  
 Дата, время и вид контроля

-----C-----
Card_Identification_____
C dd/mm/yyyy hh:mm ppppp

Вид контроля: До пяти пиктограмм Возможные виды контроля (по отдельности или в сочетании друг с другом):  
 ■: Загрузка данных карточки, ⚡: загрузка данных БУ, ♣: печать, □: Отображение, †: Придорожные проверки калибровки

8 **Данные о деятельности водителя, сохраняемые на карточке в хронологической последовательности**

Идентификатор блока

-----D-----
dd/mm/yyyy xxx

	Проверяемая дата (календарный день, данные за который подлежат распечатке) + календарный счётчик вводов карточки	----- -----
8a	<i>Условие вне области применения в начале дня</i> (оставить пустым, если условия вне области применения нет)	-----OUT----- --
8.1	<i>Период, в течение которого карточка находилась вне устройства</i>	
8.1a	Идентификатор записи (начало периода)	----- ?
8.1b	Неизвестный период Время начала, продолжительность	hh:mm hhhmm
8.1c	<i>Действие, введённое вручную</i> Пиктограмма действия, время начала, продолжительность	A hh:mm hhhmm
8.2	<i>Ввод карточки в считывающее устройство S</i> Идентификатор записи; S = пиктограмма считывающего устройства Государство-член регистрации транспортного средства и VRN Показание одометра транспортного средства в момент ввода карточки	-----S----- A Nat/VRN _____ x xxx xxx km
8.3	<i>Деятельность (между вводом и извлечением карточки)</i> Пиктограмма действия, время начала, продолжительность, статус экипажа (пиктограмма экипажа, если CREW, пусто, если SINGLE).	A hh:mm hhhmm ☐☐
8.3a	<i>Особое условие</i> Время ввода данных, пиктограмма (или комбинация пиктограмм) особого условия.	hh:mm ---pppp- --
8.4	<i>Извлечение карточки</i> Показания одометра и расстояние, пройденное с момента последнего ввода карточки, при котором были зафиксированы показания одометра	x xxx xxx km; x xxx km
9	<i>Данные о деятельности водителей, сохраненные в БУ отдельно для каждого считывающего устройства в хронологическом порядке</i> Идентификатор блока Проверяемая дата (календарный день, данные за который подлежат распечатке) Показания одометра на 00:00 часов и на 24:00 часа	-----☐----- dd/mm/yyyy x xxx xxx - x xxx xxx km
10	<i>Данные о деятельности со считывающего устройства S</i> Идентификатор блока	-----S-----
10a	<i>Условие вне области применения в начале дня</i> (оставить пустым, если условия вне области применения нет)	-----OUT-----
10.1	<i>Период отсутствия карточки в считывающем устройстве S</i> Идентификатор записи Карточка не введена Показания одометра на начало периода	----- ☐☐--- x xxx xxx km

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)\*

Государство-член регистрации предыдущего транспортного средства, которым управлял водитель, и его VRN

Дата и время извлечения карточки из предыдущего транспортного средства  
Пустая строка

Показания одометра на момент ввода карточки, метка ручного ввода данных о деятельности водителя (M, если да, пробел, если нет).

Если в течение дня, за который выводится распечатка, карточка водителя не вводилась, используется блок данных показаний одометра 10.2, зафиксированный во время последнего ввода карточки до данного дня.

-----
☐
Last_Name_____
First_Name_____
Card_Identification_____
dd/mm/yyyy - GEN 2
☐ +Nat/VRN_____
dd/mm/yyyy hh:mm
x xxx xxx km M

10,3 *Вид деятельности*

Пиктограмма действия, время начала, продолжительность, статус экипажа (пиктограмма экипажа, если CREW, пусто, если SINGLE).

A	hh:mm	hhmm	☐☐
---	-------	------	----

10,3 *Особое условие* Время ввода данных, а пиктограмма (или комбинация пиктограмм) особого условия.

hh:mm	---pppp-
--	

10,4 *Извлечение карточки или окончание периода отсутствия карточки*

Показания одометра 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 km; x xxx km
------------------------

\* Номер поколения карточки может печатать только «умный» тахограф.

11 *Суточная сводка*

Идентификатор блока

-----Σ-----
-------------

11,1 *Сводка данных БУ за периоды отсутствия карточки в считывающем устройстве для карточки водителя*

Идентификатор блока

1 ☐ ---
---------

11,2 *Сводка данных БУ за периоды отсутствия карточки в считывающем устройстве для карточки второго водителя*















Идентификатор блока

2 ☐ ---
---------




11,3 *Суточная сводка данных БУ по каждому водителю*

Идентификатор записи

-----
-------

Фамилия водителя	 Last_Name _____
Имя (имена) водителя	First_Name _____
Идентификационные данные карточки водителя	Card_Identification _____
11.4 Ввод данных о месте, в котором начинается и/или заканчивается дневной период работы	
pi = пиктограмма места начала / окончания, время, страна, регион	 hh:mm Cou Reg
Одометр	x xxx xxx km
11.5 Ввод данных о месте, в котором начинается и/или заканчивается дневной период работы и после 3 часов непрерывного времени управления	
Одометр	 hh:mm x xxx xxx km
11.6 Сводка данных (с карточки)	
Общее время управления, пройденное расстояние	 hh:mm x xxx km
Общее время работы и готовности	* hh:mm  hh:mm
Общее время отдыха и отсутствия данных	h hh:mm ? hh:mm
Суммарное время деятельности экипажа	  hh:mm
11.7 Сводка данных (периоды отсутствия карточки считывающем устройстве водителя)	
Общее время управления, пройденное расстояние	 hh:mm x xxx km
Общее время работы и готовности	* hh:mm  hh:mm
Общее время отдыха	h hh:mm
11.8 Сводка данных (периоды отсутствия карточки считывающем устройстве второго водителя)	
Общее время работы и готовности	* hh:mm  hh:mm
Общее время отдыха	h hh:mm
11.9 Сводка данных (каждого водителя из обоих считывающих устройств)	
Общее время управления, пройденное расстояние	 hh:mm x xxx km
Общее время работы и готовности	* hh:mm  hh:mm
Общее время отдыха	h hh:mm
Суммарное время деятельности экипажа	  hh:mm

При вводе команды на распечатку суточной сводки за текущий день имеющиеся данные за сутки суммируются по состоянию на момент распечатки.

12 <b>События и/или неисправности, зарегистрированные на карточке</b>	
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	Pic (p) dd/mm/yyyy hh:mm
Дополнительный код события/неисправности (если имеется), продолжительность	!xx hhmm
Государство-член регистрации транспортного средства, в котором имело место событие или неисправность, и его VRN	▣ Nat/VRN _____

13 **События и/или неисправности, зарегистрированные или происходящие в БУ**

13.1 Идентификатор блока данных: последние 5 событий и неисправностей, зарегистрированных в БУ	----- !x▣-----
--	----------------

13.2 Идентификатор блока данных: все события, зарегистрированные или происходящие в БУ	----- !▣-----
--	---------------

13.3 Идентификатор блока данных: все неисправности, зарегистрированные или происходящие в БУ	----- x▣-----
--	---------------

13.4 **Запись о событии и/или неисправности**

Идентификатор записи	-----
Пиктограмма события/неисправности, назначение записи, дата и время начала	Pic (p) dd/mm/yyyy hh:mm
Дополнительный код события/неисправности (если имеется), количество аналогичных событий за текущий день, продолжительность	!xx (xxx) hhmm
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)	Card_Identification_____ Card_Identification_____ Card_Identification_____ Card_Identification_____
Случай, когда карточка не была введена	▣---
Данные, касающиеся конкретного производителя	< Literal><ErrorCode>

Цель записи (p) указывается числовым кодом, обозначающим цель регистрации события или неисправности и определяемым в порядке, предусмотренном для элемента данных EventFaultRecordPurpose.

Literal – константа, связанная с конкретным производителем тахографа, которую составляет не более 12 символов.

ErrorCod – код ошибки, связанный с конкретным производителем тахографа, который составляет не более 12 символов.

14 **Идентификационные данные БУ**

Идентификатор блока	----- ▣-----
Название производителя БУ	▣ Name_____
Адрес производителя БУ	Address_____
Номер детали БУ	PartNumber_____
Номер официального утверждения БУ	Apprv_____
Серийный номер БУ	S/N_____
Год выпуска БУ	yyyy

Версия программного обеспечения БУ и дата её установки V xxxx dd/mm/yyyy

15 **Идентификационные данные датчика**

Идентификатор блока ----- П -----

15.1 **Запись о соединении**

Серийный номер датчика  
 Номер официального утверждения датчика  
 Дата подсоединения датчика

П S/N \_\_\_\_\_  
 Apprv \_\_\_\_\_  
 dd/mm/yyyy hh:mm

16 **Идентификационные данные ГНСС**

Идентификатор блока ----- ☒ -----

16.1 **Запись о подсоединении**

Серийный номер внешнего устройства ГНСС  
 Номер официального утверждения внешнего устройства ГНСС  
 Дата подсоединения внешнего устройства ГНСС

☒ S/N \_\_\_\_\_  
 Apprv \_\_\_\_\_  
 dd/mm/yyyy hh:mm

17 **Данные калибровки**

Идентификатор блока ----- Т -----

17.1 **Запись о калибровке**

Идентификатор записи  
 Мастерская, проводившая калибровку

-----  
 Т Workshop\_name \_\_\_\_\_  
 Workshop\_address \_\_\_\_\_  
 Card\_Identification \_\_\_\_\_  
 dd/mm/yyyy  
 Т dd/mm/yyyy (p)  
 Д VIN \_\_\_\_\_  
 Nat/VRN \_\_\_\_\_  
 w xx xxx **Imp/km**  
 k xx xxx **Imp/km**  
 l xx xxx **mm**  
 • TyreSize \_\_\_\_\_  
 > xxx **km/h**  
 x xxx xxx - x xxx xxx **km**

Адрес мастерской  
 Идентификационные данные карточки мастерской  
 Дата истечения срока действия карточки мастерской  
 Пустая строка  
 Дата калибровки + цель калибровки  
 VIN  
 Государство-член регистрации и VRN  
 Характеристический коэффициент транспортного средства  
 Постоянная величина записывающего оборудования  
 Фактическая окружность шин колёс  
 Размер шин, установленных на транспортном средстве  
 Положение устройства ограничения скорости  
 Показания одометра до и после калибровки

Цель калибровки (p) указывается числовым кодом, поясняющим, зачем зафиксированы данные параметры калибровки, и определяемым в порядке, предусмотренном для элемента данных CalibrationPurpose.

18 **Корректировка времени**

Идентификатор блока ----- Ⓜ -----

18.1 **Запись о корректировке времени**

Идентификатор записи -----

Старые дата и время	! Ⓞ dd/mm/yyyy hh:mm
Новые дата и время	Ⓞ dd/mm/yyyy hh:mm
Мастерская, проводившая корректировку времени	Ⓡ Workshop_name_____
Адрес мастерской	Workshop_address_____
Идентификационные данные карточки мастерской	Card_Identification_____
Дата истечения срока действия карточки мастерской	dd/mm/yyyy
<b>19 Зарегистрированные БУ данные о последних по времени событиях и неисправности</b>	
Идентификатор блока	-----!×Ⓡ-----
Дата и время последнего события	! dd/mm/yyyy hh:mm
Дата и время последней неисправности	× dd/mm/yyyy hh:mm
<b>20 Информация о контроле превышения скорости</b>	
Идентификатор блока	----->>-----
Дата и время последнего КОНТРОЛЯ ЗА ПРЕВЫШЕНИЕМ СКОРОСТИ	>Ⓡdd/mm/yyyy hh:mm
Дата и время первого превышения скорости и количество последующих превышений скорости	>>dd/mm/yyyy hh:mm (nnn)
<b>21 Запись о превышении скорости</b>	
21.1 Идентификатор блока данных: первое превышение скорости со времени последней калибровки	----->>Ⓡ-----
21.2 Идентификатор блока данных: 5 самых серьезных случаев за последние 365 дней	----->>(365)-----
21.3 Идентификатор блока данных: самое серьезное событие за каждый из последних 10 дней данного случая	----->>(10)-----
21.4 Идентификатор записи	-----
Дата, время и продолжительность	>>dd/mm/yyyy hh:mm hhmm
Максимальная и средняя скорость, количество аналогичных событий за данный день	xxx km/h xxx km/h (xxx)
Фамилия водителя	Ⓞ Last_Name_____
Имя (имена) водителя	First_Name_____
Идентификационные данные карточки водителя	Card_Identification_____
21.5 Если в блоке данных записи о превышении скорости отсутствуют	>>---

22 **Информация, вписываемая от руки**

- Идентификатор блока  
 22.1 Место контроля  
 22.2 Подпись контролёра  
 22.3 Время: от  
 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 подписи.

23 **Последние карточки, вставленные в БУ**

- Идентификатор блока  
 23.1 Вставленная карточка  
 Идентификатор записи  
 Тип карточки, поколение, версия, производитель\*  
 Идентификационные данные карточки  
 Card Serial Number  
 Дата и время последнего ввода карточки

----- □ □ ⊕ -----
-----
T <gen> <version> <MC>
Card Identification
Card Serial Number
dd/mm/yyyy hh:mm

\* (всё в одной строке)

с

*типом карточки:* Пиктограмма, один символ + пробел

*поколением:* GEN1 или GEN2, 4 символа + пробел

*версией:* до 10 символов

MC: код производителя, 3 символа

## 3. Спецификации распечатки данных

В тексте данной главы применяются следующие условные обозначения:

N
---

Печатать номер блока или записи N

N
---

Печатать номер блока или записи N нужное количество раз

X / Y
-------

При необходимости печатать блоки или записи X и/или Y  
нужное количество раз

### 3.1. Ежедневная распечатка данных о деятельности водителя, записанных на карточке

PRT\_008 При распечатке сохранённых на карточке данных о деятельности водителя за сутки соблюдается следующий формат:

1
2
3

Дата и время распечатки документа

Вид распечатки

Идентификационные данные контролёра (если в БУ введена карточка контролёра)

3	Идентификационные данные водителя (согласно карточке, с которой распечатываются данные + поколение)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
5	Идентификационные данные БУ (с которого получены распечатываемые данные + поколение)
6	Последняя калибровка этого БУ
7	Последний контроль инспектируемого водителя
8	Ограничитель деятельности водителя
8a	Условие вне области применения в начале дня
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Деятельность водителя в хронологическом порядке
11	Ограничитель суточной сводки
11.4	Въезд в географические пункты в хронологическом порядке
11.5	Данные ГНСС
11.6	Сводка данных деятельности
12.1	Ограничитель данных о событиях или неисправностях, хранящихся на карточке
12.4	Записи о событиях/неисправностях (последние 5 событий или неисправностей, зарегистрированные на карточке)
13.1	Ограничитель данных о событиях или неисправностях, хранящихся в БУ
13.4	Записи о событиях/неисправностях (последние 5 событий или неисправностей, зарегистрированные или происходящие в БУ)
22.1	Место контроля
22.2	Подпись контролёра
22.5	Подпись водителя

### **3.2. Ежедневная распечатка данных о деятельности водителя, записанных в БУ**

PRT\_009 При распечатке сохранённых в БУ данных о деятельности водителя за сутки соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные владельца карточки (для всех карточек, введённых в БУ + поколение)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
5	Идентификационные данные БУ (с которого получены распечатываемые данные + поколение)
6	Последняя калибровка этого БУ
7	Последний контроль данного тахографа
9	Ограничитель деятельности водителя
10	Ограничитель данных со считывающего устройства водителя (считывающее устройство 1)
10a	Условие вне области применения в начале дня

10.1 / 10.2 / 10.3 /10.3a / 10.4	Деятельность в хронологическом порядке (данные со считывающего устройства водителя)
10	Ограничитель данных со считывающего устройства второго водителя (считывающее устройство 2)
10a	Условие вне области применения в начале дня
10.1 / 10.2 / 10.3 /10.3a / 10.4	Деятельность в хронологическом порядке (данные со считывающего устройства второго водителя)
11	Ограничитель 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
11.6	Сводка данных 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
11.7	Сводка данных деятельности
11.3	Суммарные данные о деятельности водителя по данным обоих считывающих устройств
11.4	Въезд данного водителя в географические пункты в хронологическом порядке
11.5	Данные ГНСС
11.8	Суммарные данные о деятельности данного водителя
13.1	Ограничитель событий и неисправностей
12.4	Записи о событиях/неисправностях (последние 5 событий или неисправностей, зарегистрированные или происходящие в БУ)
13.1	Место контроля
22.2	Подпись контролёра
22.3	Время: с (место для указания водителем, не имеющим карточки,
22.4	Время: до относящихся к нему периодов времени)
22.5	Подпись водителя

### **3.3. Распечатка данных о событиях и неисправностях, хранящихся на карточке**

PRT\_010 При распечатке сохранённых на карточке данных о событиях и неисправностях соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные контролёра (если в БУ введена карточка контролёра + поколение)
3	Идентификационные данные водителя (согласно карточке, с которой распечатываются данные)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)

12.2	Ограничитель событий
12.4	Записи о событиях (все события, зарегистрированные на карточке)
12.3	Ограничитель неисправностей
12.4	Записи о неисправностях (все неисправности, зарегистрированные на карточке)
22.1	Место контроля
22.2	Подпись контролёра
22.5	Подпись водителя

### 3.4. Распечатка данных о событиях и неисправностях, хранящихся в БУ

PRT\_011 При распечатке сохранённых в БУ данных о событиях и неисправностях соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные владельца карточки (для всех карточек, введённых в БУ + поколение)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
13.2	Ограничитель событий
13.4	Записи о событиях (все события, зарегистрированные или происходящие в БУ)
13.3	Ограничитель неисправностей
13.4	Записи о неисправностях (все неисправности, зарегистрированные или происходящие в БУ)
22.1	Место контроля
22.2	Подпись контролёра
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 владельца карточки (для всех карточек, введённых в БУ + поколение)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
14	Идентификационные данные БУ
15	Идентификационные данные датчика
15.1	Данные о подсоединении датчика (все имеющиеся данные в хронологическом порядке)
16	Идентификационные данные ГНСС
16.1	Данные о подсоединении внешнего устройства ГНСС (все имеющиеся данные в хронологическом порядке)

17	Ограничитель данных калибровки
17.1	Записи о калибровке (все имеющиеся записи в хронологическом порядке)
18	Ограничитель данных корректировки времени
18.1	Записи о корректировке времени (все имеющиеся записи о корректировке времени, в том числе относящиеся к калибровке)
19	Зарегистрированные БУ данные о последних по времени событиях и неисправности

### 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 владельца карточки (для всех карточек, введённых в БУ + поколение)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
20	Информация о контроле превышения скорости
21.1	Идентификатор данных о превышениях скорости
21.4 / 21.5	Первое превышение скорости со времени последней калибровки
21.2	Идентификатор данных о превышениях скорости
21.4 / 21.5	5 самых серьёзных событий превышения скорости за последние 365 дней
21.3	Идентификатор данных о превышениях скорости
21.4 / 21.5	Самое серьёзное событие превышения скорости за каждый из последних 10 дней данного случая
22.1	Место контроля
22.2	Подпись контролёра
22.5	Подпись водителя

### 3.7. Архив вставленных карточек

PRT\_014 При распечатке архивных данных вставленных карточек соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные владельца карточки (для всех карточек, введённых в БУ)
23	Последняя карточка, вставленная в БУ
23.1	Вставленные карточки (до 88 записей)
12.3	Ограничитель неисправностей



## RU

## Приложение 5. Дисплей

В тексте данного приложения 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:
- \* dd mm уууу: день, месяц, год,
- \* hh: часы,
- \* mm: минуты,
- \* D: пиктограмма продолжительности,
- \* EF: комбинация пиктограмм события или неисправности,
- \* O: пиктограмма режима работы.

DIS\_001 При отображении данных тахографа соблюдаются следующие форматы:

Данные	Формат
<b>Вид дисплея с исходными настройками</b>	
Местное время	hh:mm
Режим работы	O
Информация, касающаяся водителя	<b>1</b> Dhh <b>h</b> mm <b>■</b> hh <b>h</b> mm
Информация, касающаяся второго водителя	<b>2</b> Dhh <b>h</b> mm
Начало действия условия вне области применения	<b>OUT</b>
<b>Отображение предупреждения</b>	
Превышение непрерывного времени управления	<b>1</b> <b>⊗</b> hh <b>h</b> mm <b>■</b> hh <b>h</b> mm
Событие или неисправность	EF
<b>Другие отображаемые данные</b>	
Дата UTC время	<b>UTC</b> <sup>⊗</sup> dd/mm/yyyy или <b>UTC</b> <sup>⊗</sup> dd.mm.yyyy hh:mm
Продолжительность непрерывного управления и совокупное время перерывов водителя	<b>1</b> <b>⊗</b> hh <b>h</b> mm <b>■</b> hh <b>h</b> mm
Продолжительность непрерывного управления и совокупное время перерывов второго водителя	<b>2</b> <b>⊗</b> hh <b>h</b> mm <b>■</b> hh <b>h</b> mm

Совокупное время управления водителя за предыдущую и текущую недели	1 ☐    hhhhmm
Совокупное время управления второго водителя за предыдущую и текущую недели	2 ☐    hhhhmm

RU

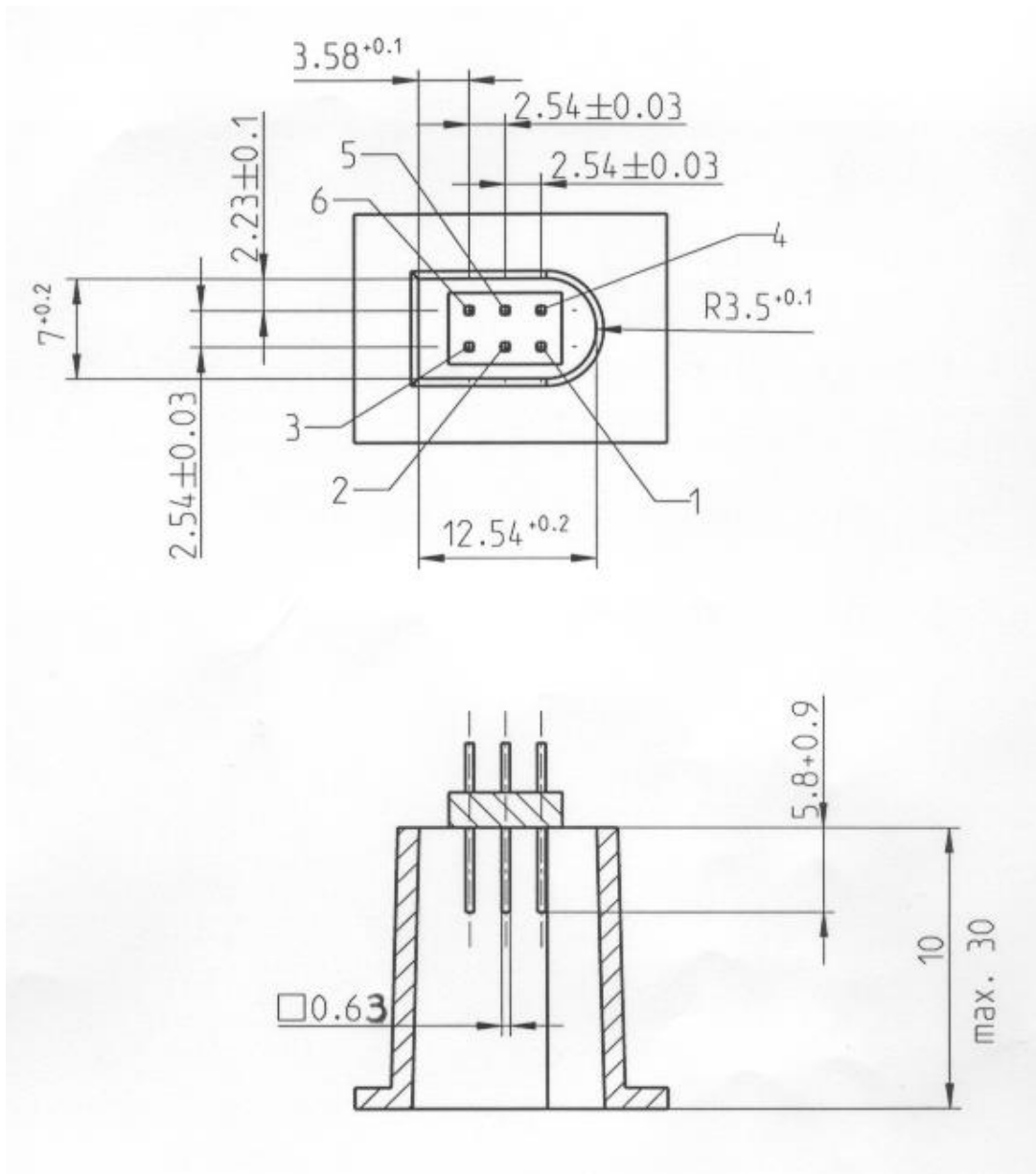
**Приложение 6. Передний соединитель для калибровки и загрузки****СОДЕРЖАНИЕ**

<b>1.</b>	<b>Аппаратное обеспечение .....</b>	<b>280</b>
1.1.	Соединитель .....	280
1.2.	Расположение контактов .....	282
1.3.	Структурная схема.....	282
<b>2.</b>	<b>Интерфейс загрузки данных .....</b>	<b>282</b>
<b>3.</b>	<b>Интерфейс калибровки .....</b>	<b>283</b>

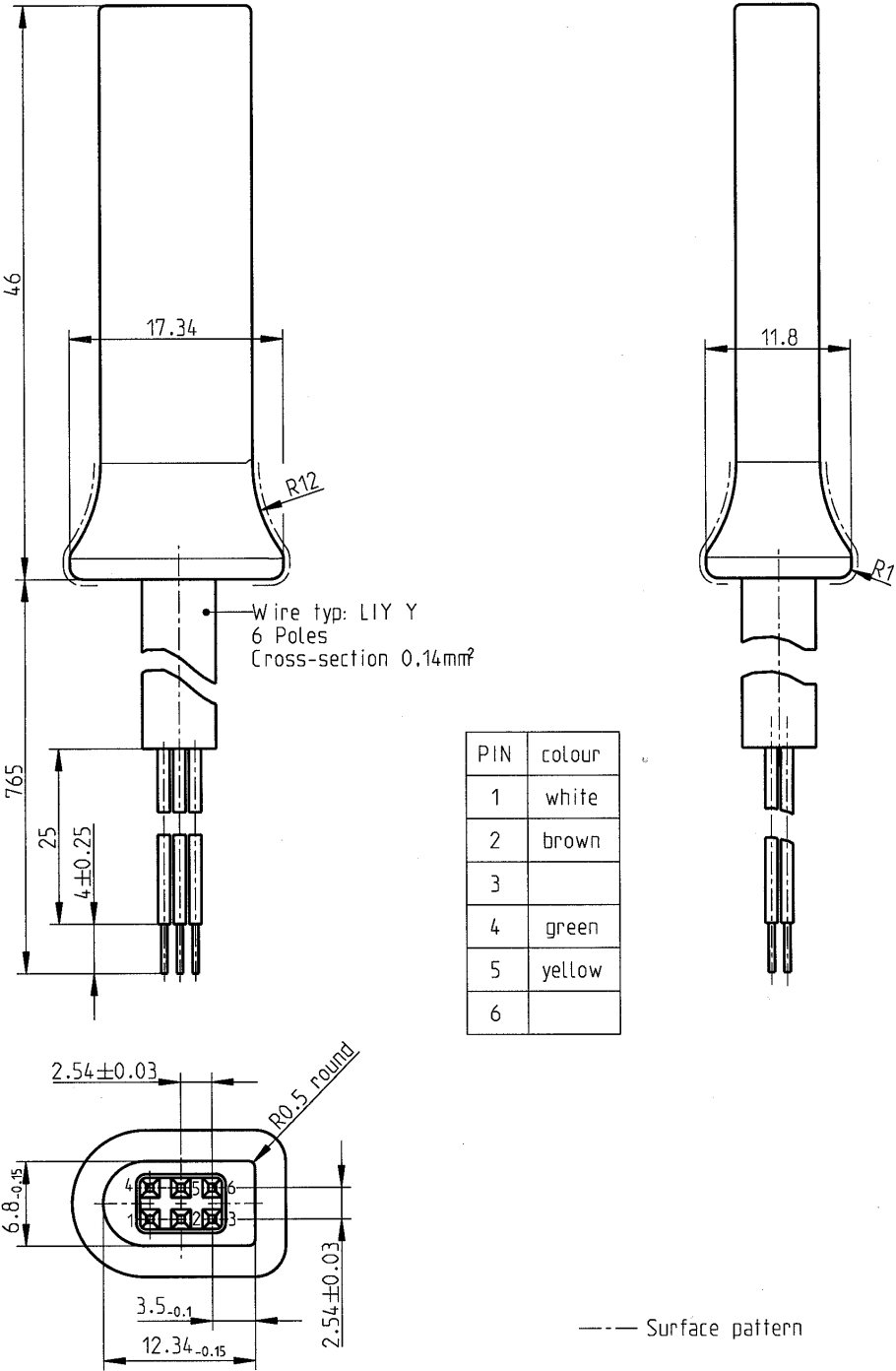
## 1. Аппаратное обеспечение

### 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 разъём, выполненный в соответствии с нижеследующим чертежом (все размеры указаны в миллиметрах):



Типовая схема вилки 6-контактного штепсельного разъёма:



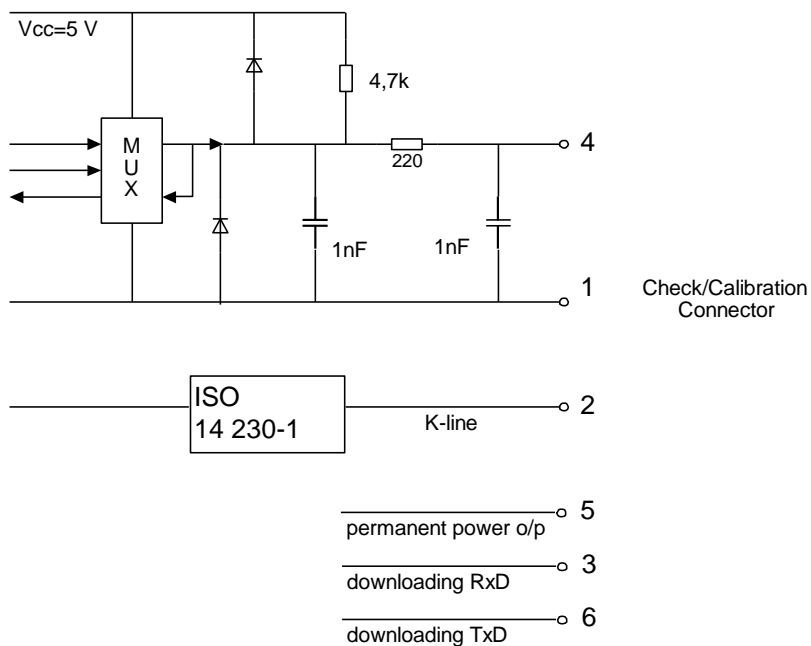
### 1.2. Расположение контактов

INT\_002 Контакты расположены в соответствии со следующей таблицей:

Конт акт	Описание	Примечание
1	Аккумулятор минус	Соединённый с аккумулятором минус транспортного средства
2	Передача данных	К-линия (ISO 14230-1)
3	RxD – Загрузка данных	Ввод данных в тахограф
4	Сигнал ввода/вывода	Калибровка
5	Постоянная выходная мощность	Диапазон напряжений равен напряжению бортовой сети питания минус 3 V с учётом падения напряжения на предохранительных цепях Выход 40 мА
6	TxD – Загрузка данных	Выход данных с тахографа

### 1.3. Структурная схема

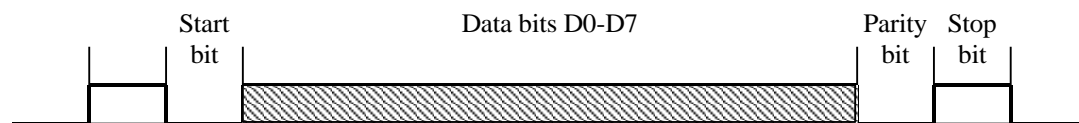
INT\_003 Структурная схема соответствует приведённой ниже:



### 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 чётности, один стоп-бит.



**Структура байта данных**

Стартовый бит: один бит с уровнем логического нуля;

Биты данных: бит младшего разряда (LSB) передаётся первым;

Бит контроля по чётности: положительная чётность;

Стоп-бит: один бит с уровнем логической единицы

При передаче числовых данных объёмом больше одного байта байт старшего разряда передаётся первым, байт младшего разряда – последним.

INT\_006 Скорость передачи данных в бодах регулируется в диапазоне от 9 600 бит/с до 115 200 бит/с. При инициализации обмена данными задаётся начальная скорость передачи в бодах 9 600 бит/с; затем скорость доводится до максимальной возможной величины.

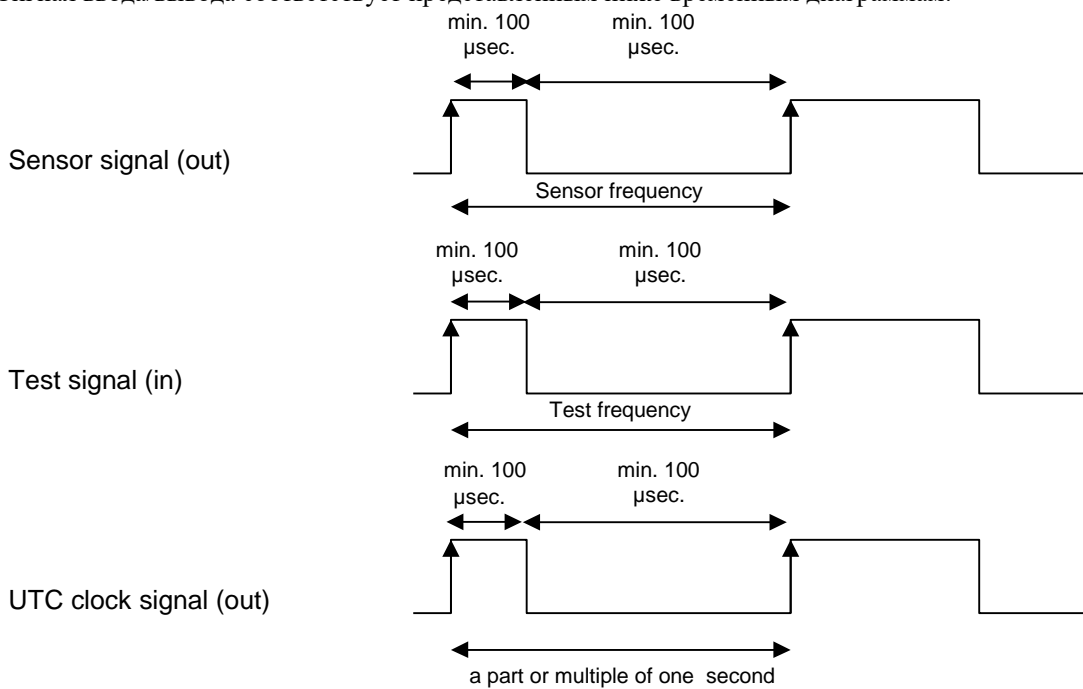
**3. Интерфейс калибровки**

INT\_007 Передача данных соответствует ISO 14230-1 Дорожные транспортные средства. Диагностические системы. Ключевой протокол 2000. Часть 1: физический слой, 1-е издание: 1999.

INT\_008 Электрические характеристики сигнала ввода/вывода соответствуют указанным ниже:

Параметр	Минимальный	Стандартный	Максимальный	Примечание
$U_{low}$ (ВВОД)			1,0 V	$I = 750 \mu A$
$U_{high}$ (ВВОД)	4 V			$I = 200 \mu A$
Частота			4 кГц	
$U_{low}$ (ВЫВОД)			1,0 V	$I = 1 mA$
$U_{high}$ (ВЫВОД)	4 V			$I = 1 mA$

INT\_009 Сигнал ввода/вывода соответствует представленным ниже временным диаграммам:





**RU**

**Приложение 7. Протоколы загрузки данных**

## СОДЕРЖАНИЕ

<b>1.</b>	<b>Введение .....</b>	<b>287</b>
1.1.	Область применения .....	287
1.2.	Сокращения и обозначения .....	287
<b>2.</b>	<b>Загрузка данных из БУ .....</b>	<b>288</b>
2.1.	Процедура загрузки .....	288
2.2.	Протокол загрузки данных .....	288
2.2.1	Структура сообщения .....	288
2.2.2	Типы сообщений .....	290
2.2.2.1	Запрос инициализации обмена данными (SID 81) .....	292
2.2.2.2	Положительный ответ: начало обмена данными (SID C1) .....	292
2.2.2.3	Запрос инициализ. диагност. сеанса (SID 10) .....	292
2.2.2.4	Положительный ответ: начало диагностики (SID 50) .....	292
2.2.2.5	Функция управления передачей данных (SID 87) .....	292
2.2.2.6	Положительный ответ: функция управления передачей данных (SID C7) .....	292
2.2.2.7	Запрос загрузки (SID 35) .....	293
2.2.2.8	Положительный ответ: запрос загрузки (SID 75) .....	293
2.2.2.9	Запрос передачи данных (SID 36) .....	293
2.2.2.10	Положительный ответ: передача данных (SID 76) .....	293
2.2.2.11	Запрос завершения передачи (SID 37) .....	293
2.2.2.12	Положит. ответ: запрос на завершение передачи (SID 77) .....	294
2.2.2.13	Запрос завершения обмена данными (SID 82) .....	294
2.2.2.14	Положительный ответ: конец обмена данными (SID C2) .....	294
2.2.2.15	Подтверждение приёма подсообщения (SID 83) .....	294
2.2.2.16	Отрицательный ответ (SID 7F) .....	294
2.2.3	Поток сообщений .....	295
2.2.4	Время .....	296
2.2.5	Обработка ошибок .....	296
2.2.5.1	Этап инициализации обмена данными .....	296
2.2.5.2	Этап обмена данными .....	297
2.2.6	Содержание ответного сообщения .....	300
2.2.6.1	Положительный ответ: передача обзорных данных .....	300
2.2.6.2	Положительный ответ: передача данных о действиях .....	302
2.2.6.3	Положительный ответ на запрос передачи данных о событиях и неисправностях .....	306
2.2.6.4	Положительный ответ: передача подробных данных о скорости .....	309
2.2.6.5	Положительный ответ: передача технических данных .....	311
2.3.	Хранение файлов на ВН .....	312
<b>3.</b>	<b>Протокол загрузки данных с карточек тахографа .....</b>	<b>313</b>
3.1.	Область применения .....	313
3.2.	Определения .....	313
3.3.	Загрузка данных карточки .....	313
3.3.1	Процедура инициализации .....	313
3.3.2	Процедура для неподписанных файлов данных .....	314
3.3.3	Процедура для подписанных файлов данных .....	314
3.3.4	Процедура обнуления счётчика калибровок .....	315
3.4.	Формат хранения данных .....	316
3.4.1	Введение .....	316
3.4.2	Формат файла .....	316
<b>4.</b>	<b>Загрузка данных с карточки тахографа через бортовое устройство .....</b>	<b>317</b>

## 1. Введение

В настоящем приложении 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 контролёр имел возможность ознакомиться с этими данными и перед началом их анализа убедиться в их подлинности и целостности.

### 1.1. Область применения

На ВН могут загружаться данные:

- из бортового устройства при помощи подключённой к БУ специализированной программируемой аппаратуры (СПА),
- с карточки тахографа при помощи СПА, оснащённой 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 11 «Общие механизмы защиты». В состав загружаемой информации включаются идентификационные данные аппаратного источника (БУ или карточки) и соответствующие ему сертификаты безопасности (государства-члена и аппаратуры). Лицо, осуществляющее проверку данных, должно иметь собственный открытый криптографический ключ от надежного европейского поставщика.

DDP\_001 Данные, загруженные за один сеанс загрузки, должны сохраняться на ВН в виде одного файла.

### 1.2. Сокращения и обозначения

В настоящем приложении используются следующие сокращения:

**AID** Идентификатор приложения

**ATR** Отклик на сигнал сброса

**CS** Байт контрольной суммы

**DF** Выделенный файл.

**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 с интегральной схемой

**IDE (СПА)** Специализированная программируемая аппаратура: аппаратура, используемая для загрузки данных на ВН (например, персональный компьютер)

**IFD** Устройство интерфейса

**KWP** Ключевой протокол 2000

**LEN** Байт длины (последний байт в заголовке сообщения)

**PPS** Выбор параметра протокола

**PSO** Выполнение операции обеспечения безопасности

**SID** Идентификатор функции

**SRC** Байт адреса источника

**TGT** Байт адреса приёмника

**TLV** Значение длины метки

**TREP** Ответный параметр передачи данных

**TRTP** Параметр запроса передачи данных

**VU (БУ)** Бортовое устройство

## 2. Загрузка данных из БУ

### 2.1. Процедура загрузки

Для загрузки данных из БУ оператору необходимо выполнить следующие действия:

- Ввести свою карточку тахографа в считывающее устройство БУ(\*);
- Подсоединить СПА к выходному разъёму 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, введённой в одно из считывающих устройств БУ, если в другое считывающее устройство не вставлена никакая карточка другого типа.

### 2.2. Протокол загрузки данных

Протокол построен по принципу «ведущий-ведомый», при котором в роли ведущего выступает СПА, а в роли ведомого – БУ.

Структура сообщений, их типы и потоки, как правило, основываются на ключевом протоколе 2000 (KWP) (ISO 14230-2 Дорожные транспортные средства. Диагностические системы. Ключевой протокол 2000. Часть 2: Уровень канала передачи данных).

Уровень приложения, в принципе, опирается на действительную редакцию стандарта ISO 14229-1 (Дорожные транспортные средства. Диагностические системы. Часть 1: услуги диагностики, версия 6 от 22 февраля 2001 г.).

#### 2.2.1 Структура сообщения

DDP\_002 Все сообщения, которыми обмениваются СПА и БУ, форматируются в соответствии с трёхкомпонентной структурой:

- Заголовок, состоящий из байта формата (FMT), байта адреса приёмника (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					Контрольн ая сумма
FMT	TGT	SRC	LEN	SID	DATA	.....	.....	.....	CS
4 байта				Макс. 255 байтов					1 байт

Байты TGT и SRC указывают физические адреса получателя и отправителя сообщения. Их значения – F0 Нех для СПА и EE Нех 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 объём передаваемых в сообщении данных превышает длину поля данных, сообщение фактически высылается в виде нескольких подсообщений. Каждое подсообщение содержит заголовок, одни и те же байты SID и TREP, а также 2-байтовый счётчик 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 её.

DDP\_004 Если поле данных последнего подсообщения содержит ровно 255 байтов, к нему должно добавляться заключительное подсообщение с пустым (то есть содержащим только SID, TREP и счётчик подсообщений) полем данных, означающее конец сообщения.

Пример:

Заголов ок	SID	TRE P	Сообщение			CS
4 байта	Более 255 байтов					

Передаётся как:

Заголов ок	SID	TRE P	00	01	Подсообщение 1	CS
4 байта	255 байтов					

Заголов ок	SID	TRE P	00	02	Подсообщение 2	CS
4 байта	255 байтов					

...

Заголов ок	SID	TRE P	xx	yy	Подсообщение n	CS
4 байта	Менее 255 байтов					

или как:

Заголов ок	SID	TRE P	00	01	Подсообщение 1	CS
4 байта	255 байтов					

Заголов ок	SID	TRE P	00	02	Подсообщение 2	CS
4 байта	255 байтов					

...

Заголов ок	SID	TRE P	xx	yy	Подсообщение n	CS
4 байта	255 байтов					

Заголов ок	SID	TRE P	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 сообщения	Макс. 4 байта Заголовок				Макс. 255 байтов Данные			1 байт Контроль ная сумма
	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DATA	CS
СПА ->	<- БУ							
Запрос инициализации обмена данными	81	EE	F0		81			E0
Положительный ответ: начало обмена данными	80	F0	EE	03	C1		EA, 8F	9B
Запрос инициализ. диагност. сеанса	80	EE	F0	02	10	81		F1
Положительный ответ: начало диагностики	80	F0	EE	02	50	81		31
Функция управления передачей данных Проверка скорости передачи данных бодами (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
Положит. ответ: проверка скорости передачи бодами	80	F0	EE	02	C7		01	28
Скорость передачи данных бодами (этап 2)	80	EE	F0	03	87		02,03	ED
Запрос загрузки	80	EE	F0	0A	35		00,00,00,0 0,00,FF,FF, FF,FF	99
Положит. ответ: запрос загрузки	80	F0	EE	03	75		00,FF	D5
Запрос передачи данных								
Обзор	80	EE	F0	02	36	01		97
Действия	80	EE	F0	06	36	02	Дата	CS
События и неисправности	80	EE	F0	02	36	03		99
Данные о скорости	80	EE	F0	02	36	04		9A
Технические данные	80	EE	F0	02	36	05		9B
Загрузка данных карточки	80	EE	F0	02	36	06	Считываю щее устройство	CS
Положит. ответ: передача данных	80	F0	EE	Len	76	TREP	Данные	CS
Запрос завершения передачи	80	EE	F0	01	37			96
Положит. ответ: запрос на завершение передачи	80	F0	EE	01	77			D6
Запрос прекращения обмена данными	80	EE	F0	01	82			E1
Положительный ответ: конец обмена данными	80	F0	EE	01	C2			21
Подтверждение приёма 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
Неверная длина сообщения	80	F0	EE	03	7F	Sid Req	13	CS
Недопустимые условия или ошибка очередн.	80	F0	EE	03	7F	Sid Req	22	CS
Нештатный запрос	80	F0	EE	03	7F	Sid Req	31	CS
Отказ в приёме загружаемых данных	80	F0	EE	03	7F	Sid Req	50	CS
Ожидается ответ	80	F0	EE	03	7F	Sid Req	78	CS

Данных нет	80	F0	EE	03	7F	Sid Req	FA	CS
------------	----	----	----	----	----	---------	----	----

## Примечания:

- Sid Req = Sid соответствующего запроса.
- TREP = TRTP соответствующего запроса.
- Тёмный 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).
- 2-байтные счётчики 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 если его конкретно выбрал пользователь.

### 2.2.2.1 Запрос инициализации обмена данными (SID 81)

DDP\_005 Данное сообщение высылается СПА для 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: начало обмена данными (SID C1)

DDP\_006 Данное сообщение высылается БУ в качестве положительного ответа на запрос инициализации обмена данными. Оно включает в себя два байта ключей 'EA' и '8F', указывающие на поддержку данного протокола устройством, и заголовок с информацией о получателе, источнике и длине сообщения.

### 2.2.2.3 Запрос инициализ. диагност. сеанса (SID 10)

DDP\_007 Сообщение с запросом инициализации диагностического сеанса высылается СПА, чтобы начать новый сеанс обмена диагностическими данными с БУ. Подфункция «default session» (81 Hex) указывает на то, что будет начат стандартный диагностический сеанс.

### 2.2.2.4 Положительный ответ: начало диагностики (SID 50)

DDP\_008 Сообщение с положительным ответом на запрос инициализации диагностики высылает БУ, чтобы подтвердить начало диагностического сеанса.

### 2.2.2.5 Функция управления передачей данных (SID 87)

DDP\_052 Функция управления передачей данных используется СПА для того, чтобы инициировать изменение скорости передачи данных бодами. Это происходит в два этапа. На первом этапе СПА предлагает изменение скорости 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 Положительный ответ: функция управления передачей данных (SID C7)

DDP\_053 Положительный ответ о функции управления передачей данных 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 об адресе, объёме и формате 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 объём памяти задается максимальным.

### 2.2.2.8 Положительный ответ: запрос загрузки (SID 75)

DDP\_010 Сообщение с положительным ответом на запрос загрузки 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 о том, что последующие положительные ответы на запросы передачи данных будут содержать максимум 00FF Hex байт.

### 2.2.2.9 Запрос передачи данных (SID 36)

DDP\_011 Запрос передачи данных высылается СПА с целью указать БУ тип данных, которые должны быть загружены. Тип данных указывается однобайтовым параметром запроса передачи (TRTP).

Возможна передача шести типов данных:

- Обзор (TRTP 01),
- Деятельность на указанную дату (TRTP 02),
- События и неисправности (TRTP 03),
- Подробные данные о скоростном режиме (TRTP 04),
- Технические данные (TRTP 05),
- Загрузка данных с карточки (TRTP06).

DDP\_054 В ходе сеанса загрузки СПА в обязательном порядке запрашивает передачу обзорных данных (TRTP 01), так как только при этом в загружаемом файле регистрируются сертификаты БУ (что создаёт возможность проверки цифровой подписи).

Во втором случае (TRTP 02) сообщение с запросом передачи 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 передачи данных высылается БУ по получении запроса передачи данных. Это сообщение содержит запрошенные данные и параметр ответа на запрос передачи (TREP), который соответствует TRTP запроса.

DDP055 В первом случае (TREP 01) БУ высылает данные, помогающие оператору СПА выбрать информацию, загрузку которой он желает продолжить. Сообщение содержит данные о:

- Сертификатах защиты,
- Идентификационных данных транспортного средства,
- Текущих дате и времени БУ,
- Самой ранней и самой поздней дате, данные за которую могут быть загружены из БУ,
- Наличии карточек в считывающих устройствах БУ,
- Предыдущей загрузке данных представителем предприятия,
- Блокировках, установленных предприятием,
- Предыдущих проверках.

### 2.2.2.11 Запрос завершения передачи (SID 37)

DDP\_013 Сообщение о запросе завершения передачи высылается СПА с целью указать БУ на завершение сеанса загрузки.

### 2.2.2.12 Положит. ответ: запрос на завершение передачи (SID 77)

DDP\_014 Положительный ответ на запрос завершения передачи данных высылается БУ в качестве подтверждения получения запроса завершения передачи.

### 2.2.2.13 Запрос завершения обмена данными (SID 82)

DDP\_015 Данное сообщение высылается СПА для отключения канала обмена данными с БУ.

### 2.2.2.14 Положительный ответ: конец обмена данными (SID C2)

DDP\_016 Положительный ответ на запрос завершения обмена данными высылается БУ в качестве подтверждения получения запроса завершения обмена данными.

### 2.2.2.15 Подтверждение приёма подсообщения (SID 83)

DDP\_017 Подтверждение приёма подсообщения высылается СПА, подтверждая этим 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 – подтверждение правильного приёма подсообщения номер MsgC.  
Запрос от СПА к БУ на отправку следующего подсообщения
- MsgC – проблема приёма подсообщения номер MsgC.  
Запрос от СПА к БУ на повторную отправку подсообщения.
- FFFF – запрос прекращения передачи сообщения.  
Эта функция может использоваться СПА для прекращения по каким-либо причинам передачи сообщения от БУ.

Приём последнего подсообщения в сообщении (LEN < 255 байт) может подтверждаться любым из вышеуказанных кодов или оставаться без подтверждения.

К ответам БУ, которые состоят из нескольких подсообщений, относятся:

- Положительный ответ: передача 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. Могут использоваться следующие коды:

- 10 Общее отклонение запроса  
Действие не может быть выполнено по причине, не входящей в число нижеперечисленных.
- 11 Услуга не поддерживается  
Не опознан SID запроса.
- 12 Подфункция не поддерживается  
Не опознан DS\_ или TRTP запроса либо отсутствуют другие подсообщения для передачи.
- 13 Неверная длина сообщения  
Получено сообщение неверной длины.
- 22 Недопустимые условия или ошибка очередности  
Требуемая функция не активирована либо неверная очередность запросов.
- 31 Нештатный запрос  
Значение параметра запроса (поле данных) недействительно.
- 50 Отказ в приёме 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.
- FA данных нет  
Запрошенный к передаче объект данных отсутствует в БУ (например, не введена карточка, ...).

### 2.2.3 Поток сообщений

При нормальной загрузке данных поток сообщений, как правило, выглядит следующим образом:

СПА		БУ
Запрос инициализации обмена данными	⇒ ⇐	Положительный ответ
Запрос инициализации функции диагностики	⇒ ⇐	Положительный ответ
Запрос загрузки	⇒ ⇐	Положительный ответ
Обзор запроса передачи данных	⇒ ⇐	Положительный ответ
Запрос передачи данных № 2	⇒ ⇐	Положительный ответ № 1  Положительный ответ № 2  Положительный ответ № m  Положительный ответ (поле данных <255 байт)
Подтверждение приёма подсообщения № 1	⇒ ⇐	
Подтверждение приёма подсообщения № 2	⇒ ⇐	
Подтверждение приёма подсообщения № m	⇒ ⇐	
Подтверждение приёма подсообщения № m	⇒ ⇐	
Подтверждение приёма подсообщения (факультативно)	⇒ ⇐	
...		
Запрос передачи данных № n	⇒ ⇐	Положительный ответ
Запрос завершения передачи	⇒ ⇐	Положительный ответ
Запрос прекращения обмена данными	⇒ ⇐	Положительный ответ

## 2.2.4 Время

DDP\_019 Временные параметры для нормального режима работы указаны в таблице ниже:

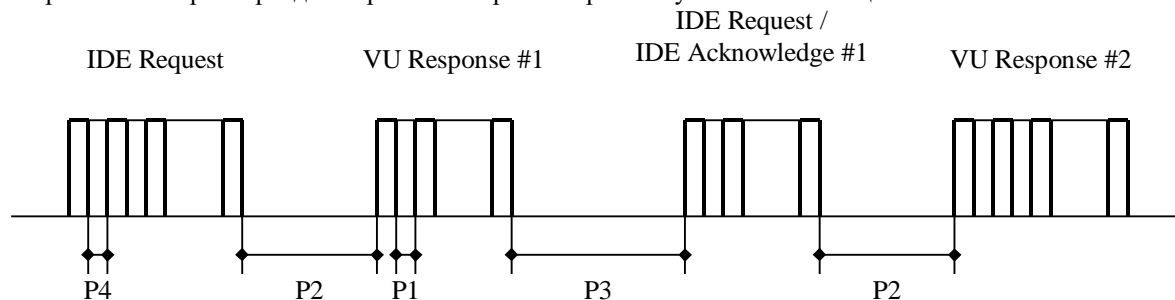


Рисунок 1 – Поток сообщений и временные параметры

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 = Увеличенное значение P3 для загрузки данных с карточек.

Допустимые значения временных параметров приводятся в нижеследующей таблице (расширенный диапазон временных параметров протокола KWP для использования при физической адресации в целях ускорения передачи данных).

Время Параметр	Нижний предел Значение (мс)	Верхний предел 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», это значение увеличивается до соответствующего верхнего предельного значения P3.

## 2.2.5 Обработка ошибок

При возникновении ошибки в процессе обмена сообщениями схема потока сообщений модифицируется в зависимости от того, каким из приборов обнаружена 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 Этап инициализации обмена данными

DDP\_020 Если СПА обнаруживает ошибку синхронизации или ошибку в битовом потоке на стадии инициализации обмена данными, период ожидания СПА перед повторением запроса равняется P3 min.

DDP\_021 Если БУ обнаруживает ошибку в очередности сообщений от СПА, оно не высылает ответа и ожидает нового сообщения с запросом инициализации обмена данными в течение периода, равного P3 max.

### **2.2.5.2 Этап обмена данными**

На этой стадии можно выделить две разных области 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 высылает ответа 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 подобном случае БУ высылает СПА отрицательный ответ с указанием характера ошибки.

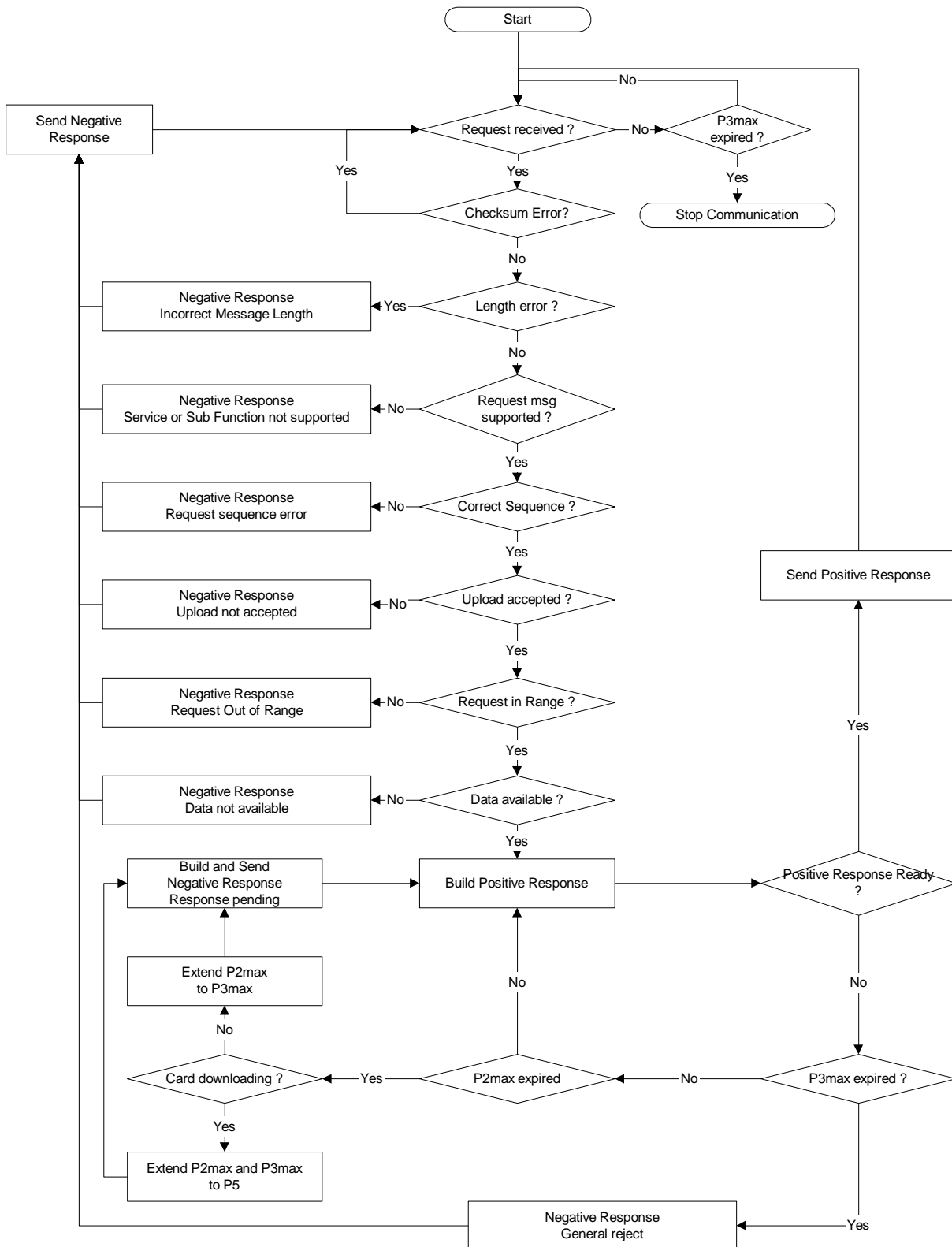


Рисунок 2 – Обработка ошибок в БУ

## 2. СПА обнаруживает ошибку в передаче данных из БУ.

DDP\_025 СПА 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\_026 СПА проверяет поступающие сообщения на ошибки очередности, такие как сбои возрастания 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, причём общее число передач ограничивается тремя. Для случаев обнаружения ошибок данного вида подтверждение приёма подсообщения рассматривается как запрос к БУ.

DDP\_028 СПА ждёт хотя бы в течение периода, равного P3min, прежде чем начать каждую передачу; период ожидания измеряется с последнего вычисленного случая стоп-бита после обнаружения ошибки.

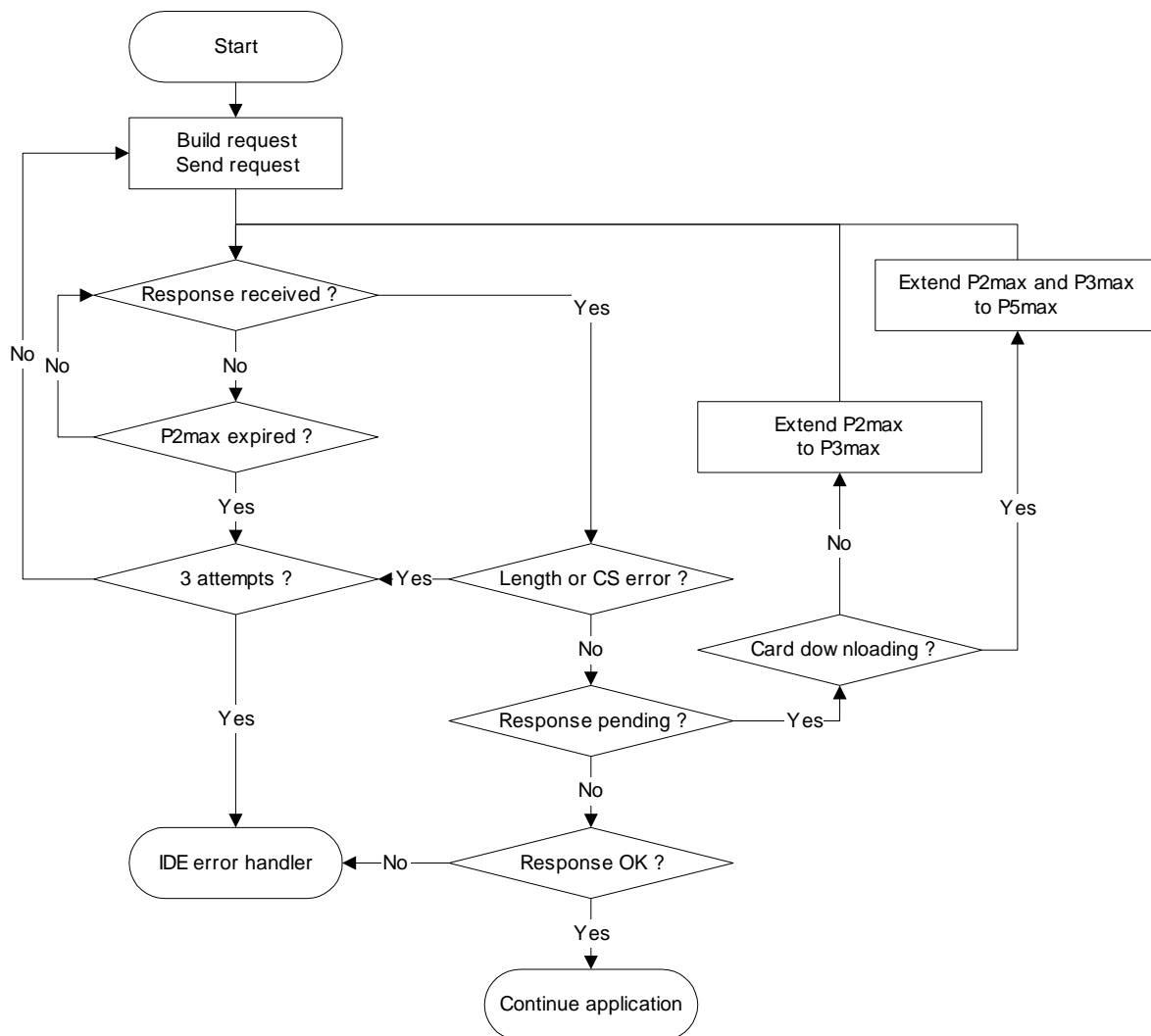


Рисунок 3 – Обработка ошибок в СПА

## 2.2.6 Содержание ответного сообщения

В данном пункте указано содержание полей данных различных сообщений с положительным ответом.

Элементы данных определены в словаре данных в приложении 1.

Примечание: При загрузке данных второго поколения каждый элемент данных высшего уровня представлен массивом 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 называются «...RecordArray» (с заголовком).

### 2.2.6.1 Положительный ответ: передача обзорных данных

DDP\_029 В поле данных сообщения «Положительный ответ на запрос передачи обзорных данных» включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 01 Hex, с соответствующим выделением и нумерацией подсообщений:

Структура данных первого поколения

Элемент данных	Комментарий
MemberStateCertificate VUCertificate	Сертификаты защиты БУ
VehicleIdentificationNumber VehicleRegistrationIdentification	Идентификационные данные транспортного средства
CurrentDateTime VuDownloadablePeriod	Текущие дата и время БУ Период, за который могут быть загружены данные
CardSlotsStatus VuDownloadActivityData	Тип карточек, вставляемых в БУ Предыдущая загрузка данных из БУ
VuCompanyLocksData	Все хранящиеся блокировки, установленные предприятием. Если раздел не заполнен, высылается только noOfLocks = 0.
VuControlActivityData	Все сохранённые в БУ контрольные записи. Если раздел не заполнен, высылается только noOfControls = 0.



Signature
-----------

Подпись RSA для всех данных (кроме сертификатов), от VehicleIdentificationNumber до последнего байта последней VuControlActivityData.
---

## Структура данных второго поколения

Элемент данных
MemberStateCertificateRecordArray
VUCertificateRecordArray
VehicleIdentificationNumberRecordArray
VehicleRegistrationNumberRecordArray
CurrentDateTimeRecordArray
VuDownloadablePeriodRecordArray
CardSlotsStatusRecordArray
VuDownloadActivityDataRecordArray
VuCompanyLocksRecordArray
VuControlActivityRecordArray
SignatureRecordArray

Комментарий
Сертификат государства-члена
Сертификат БУ
Идентификационные данные транспортного средства
Регистрационный номер транспортного средства
Текущие дата и время БУ
Период, за который могут быть загружены данные
Тип карточек, вставляемых в БУ
Предыдущая загрузка данных из БУ
Все хранящиеся блокировки, установленные предприятием. Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.
Все сохранённые в БУ контрольные записи. Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.
Подпись ECC всех предшествующих данных, кроме сертификатов.

### **2.2.6.2 Положительный ответ: передача данных о действиях**

DDP\_030 В поле данных сообщения «Положительный ответ на запрос передачи данных о действиях» включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 02 Hex, с соответствующим выделением и нумерацией подсообщений:

Структура данных первого поколения

Элемент данных	Комментарий
TimeReal	Дата загрузки
OdometerValueMidnight	Показания счётчика пробега на конец суток, к которым относятся загружаемые данные
VuCardIWData	<p>Информация о циклах ввода/извлечения карточек.</p> <ul style="list-style-type: none"> <li>– Если в разделе нет данных, высылаются только noOfVuCardIWRecords = 0.</li> <li>– 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 объёме включается в данные за оба дня.</li> </ul>
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, высылаются только noOfPlaceRecords = 0.
VuSpecificConditionData	Данные об особых условиях, зарегистрированные в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылаются только noOfSpecificConditionRecords = 0.

Signature	Подпись RSA для всех данных от TimeReal до последнего байта последней записи особого условия.
-----------	---

Структура данных второго поколения:

---

Элемент данных	Комментарий
DateOfDayDownloadedRecordArray	Дата загрузки
OdometerValueMidnightRecordArray	Показания счётчика пробега на конец суток, к которым относятся загружаемые данные
VuCardIWRecordArray	<p>Информация о циклах ввода/извлечения карточек.</p> <ul style="list-style-type: none"> <li>– Если раздел не содержит данных, высылается заголовок массива с noOfRecords = 0.</li> <li>– 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 объёме включается в данные за оба дня.</li> </ul>
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 заголовок массива с noOfRecords = 0.
VuGNSSCDRecordArray	Местоположение транспортного средства по ГНСС, где непрерывное время вождения достигает значения, кратного трём часам. Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.
VuSpecificConditionRecordArray	Данные об особых условиях, зарегистрированные в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.
SignatureRecordArray	Подпись ЕСС всех предшествующих данных.

### **2.2.6.3 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, при SID 76 Hex и TREP 03 Hex, с соответствующим выделением и нумерацией подсообщений:

Структура данных первого поколения

Элемент данных	Комментарий
VuFaultData	<p>Записи о всех неисправностях, зарегистрированные или происходящие в БУ. Если раздел не заполнен, высылается только noOfVuFaults = 0.</p>
VuEventData	<p>Все события (кроме превышения скорости), зарегистрированные или происходящие в БУ. Если раздел не заполнен, высылается только noOfVuEvents = 0.</p>
VuOverSpeedingControlData	<p>Данные, относящиеся к последнему контролю за превышениями скорости (при отсутствии данных – значение по умолчанию).</p>
VuOverSpeedingEventData	<p>Все сохранённые в БУ события превышения скорости. Если раздел не заполнен, высылается только noOfVuOverSpeedingEvents = 0.</p>

VuTimeAdjustmentData
Signature

Вся сохранённая в БУ информация о корректировках времени (кроме производимых в процессе общей калибровки). Если раздел не заполнен, высылается только noOfVuTimeAdjRecords = 0.
Подпись RSA для всех данных от noOfVuFaults до последнего байта последней записи о корректировке времени

Структура данных второго поколения:



Элемент данных	Комментарий
VuFaultRecordArray	Записи о всех неисправностях, зарегистрированные или происходящие в БУ. Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.
VuEventRecordArray	Все события (кроме превышения скорости), зарегистрированные или происходящие в БУ. Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	Данные, относящиеся к последнему контролю за превышениями скорости (при отсутствии данных – значение по умолчанию).
VuOverSpeedingEventRecordArray	Все сохранённые в БУ события превышения скорости. Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.
VuTimeAdjustmentRecordArray	Вся сохранённая в БУ информация о корректировках времени (кроме производимых в процессе общей калибровки). Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Подпись ЕСС всех предшествующих данных.

#### 2.2.6.4 Положительный ответ: передача подробных данных о скорости

DDP\_032 В поле данных сообщения «Положительный ответ на запрос передачи подробных данных о скорости» включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 04 Hex, с соответствующим выделением и нумерацией подсообщений:

Структура данных первого поколения

Элемент данных	Комментарий
VuDetailedSpeedData	Вся сохранённая в БУ подробная информация о скоростном режиме (один блок данных о скорости за каждую минуту)

Signature

<p>движения транспортного средства) 60 значений скорости в минуту (одно в секунду)</p>
<p>Подпись RSA для всех данных от noOfSpeedBlocks до последнего байта последней записи блока данных о скорости.</p>

Структура данных второго поколения:

<b>Элемент данных</b>
VuDetailedSpeedBlockRecordArray
SignatureRecordArray

<b>Комментарий</b>
<p>Вся сохранённая в БУ подробная информация о скоростном режиме (один блок данных о скорости за каждую минуту движения транспортного средства) 60 значений скорости в минуту (одно в секунду)</p>
<p>Подпись ECC всех предшествующих данных.</p>

### 2.2.6.5 Положительный ответ: передача технических данных

DDP\_033 В поле данных сообщения «Положительный ответ на запрос передачи технических данных» включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 05 Hex, с соответствующим выделением и нумерацией подсообщений:

Структура данных первого поколения

Элемент данных	Комментарий
VuIdentification	
SensorPaired	
VuCalibrationData	Все сохранённые в БУ записи калибровки.
Signature	Подпись RSA для всех данных от VuManufacturerName последнего байта последней записи VuCalibrationRecord.

Структура данных второго поколения:

Элемент данных	Комментарий
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Все пары MS, сохранённые в БУ
VuSensorExternalGNSSCoupledRecordArray	Все данные о подключении внешнего устройства ГНСС, хранящиеся в БУ
VuCalibrationRecordArray	Все сохранённые в БУ записи калибровки.
VuCardRecordArray	Все сохранённые в БУ данные ввода карточек.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Подпись ECC всех предшествующих данных.

### 2.3. Хранение файлов на ВН

DDP\_034 В случаях, когда сеанс загрузки данных включает в себя 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 в себя заголовки сообщений, счётчики 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. Область применения

В настоящем пункте изложен порядок прямой загрузки данных с карточки тахографа на СПА. СПА не является частью защищённой среды; поэтому процедура аутентификации между карточкой и СПА не предусмотрена.

#### 3.2. Определения

**Сеанс загрузки данных:** Каждая загрузка данных с ICC. Сеанс включает в себя всю процедуру, от перезапуска карточки считывающим устройством до деактивации ICC (т.е. извлечения или новой перезагрузки карточки).

**Файл подписанных данных:** Файл из ICC. Файл передаётся на IFD в текстовой форме. В ICC происходит хеширование и подпись файла, а подпись передаётся в IFD.

#### 3.3. Загрузка данных карточки

DDP\_035 Процесс загрузки данных с карточки тахографа состоит из следующих этапов:

- Загрузка общей информации, записанной на карточке в элементарных файлах ICC и IC. Эта информация не является обязательной и не защищена цифровой подписью.
- Загрузка элементарных файлов Card\_Certificate (или CardSignCertificate) и CA\_Certificate. Эта информация не защищена цифровой подписью.  
Вышеуказанные файлы загружаются в обязательном порядке при каждом сеансе загрузки.
- Загрузка элементарных файлов данных других приложений (в Tachograph DF и Tachograph\_G2 DF, если уместно), за исключением EF Card\_Download. Эта информация защищена цифровой подписью.
- При каждом сеансе загрузки обязательно загружаются как минимум элементарные файлы Application\_Identification и ID.
  - При загрузке данных с карточки водителя в обязательном порядке загружаются также следующие элементарные файлы:
    - Events\_Data,
    - Faults\_Data,
    - Driver\_Activity\_Data,
    - Vehicles\_Used,
    - Places,
    - GNSS\_Places (если уместно),
    - Control\_Activity\_Data,
    - Specific\_Conditions.
- При загрузке данных с карточки водителя обновляется дата LastCardDownload в элементарном файле Card\_Download,
- При загрузке данных с карточки мастерской сбрасывается счётчик калибровки в элементарном файле Card\_Download.
- При загрузке данных с карточки мастерской элементарный файл EF Sensor\_Installation\_Data не загружается.

#### 3.3.1 Процедура инициализации

DDP\_036 IDE иницирует следующую последовательность:

Карточка	Направление	IDE / IFD	Значение / Примечания
	⇐	Перезагрузка аппаратного обеспечения	
<b>ATR</b>	⇒		

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 элементарных файлов ICC, IC, Card\_Certificate (или CardSignCertificate) и CA\_Certificate выглядит следующим образом:

Карточка	Направление	IDE / IFD	Значение / Примечания
	⇐	<b>Select File</b>	Выбор файла по идентификаторам
<b>OK</b>	⇒		
	⇐	<b>Read Binary</b>	Если файл содержит больше данных, чем позволяет объём буфера считывателя или карточки, команду следует повторять до тех пор, пока не будет прочитан весь файл.
<b>File Data OK</b>	⇒	Сохранение данных на ВН	в соответствии с 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 также могут выполняться в один приём 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
	⇐	Select File	
<b>OK</b>	⇒		
	⇐	<b>Perform Hash of File</b>	Рассчитывает хеш-функцию по данным, содержащимся в выбранном файле, на основе хеш-алгоритма в соответствии с приложением 11. Эта команда не является ISO-командой.
Расчёт и временное хранение хеш-функции файла			
<b>OK</b>	⇒		
	⇐	<b>Read Binary</b>	Если файл содержит больше данных, чем может сохранить буфер считывателя или карточки, команду следует повторять до тех пор, пока не будет прочитан весь файл.
<b>File Data OK</b>	⇒	Сохранение полученных данных на ВН	в соответствии с 3.4 Формат хранения данных
	⇐	<b>PSO: Compute Digital Signature</b>	
На основе временно сохраненной хеш-функции выполняется защитная операция генерирования цифровой подписи			
<b>Signature OK</b>	⇒	Данные приобщаются к данным, сохраненным на ВН ранее	в соответствии с 3.4 Формат хранения данных

Примечание: выбор и чтение файла также могут выполняться в один приём 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 счётчика калибровок

DDP\_039 Для обнуления счетчика NoOfCalibrationsSinceDownload в элементарном файле EF Card\_Download, хранящемся на карточке мастерской, применяется следующая процедура:

Карточка	Направление	IDE / IFD	Значение / Примечания
	⇐	Select File EF Card_Download	Выбор файла по идентификаторам
OK	⇒		
	⇐	Update Binary NoOfCalibrationsSinceDownload = '00 00'	
Обнуляется значение загрузок данных карточки			
OK	⇒		

Примечание: выбор и обновление файла также могут выполняться в один приём при помощи команды 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 сохраняются прозрачно. Это означает, что последовательность байтов, а также последовательность битов внутри каждого байта переносимых с карточки данных должна при их сохранении оставаться неизменной;
- Все файлы, загружаемые с карточки за один сеанс загрузки, сохраняются на ВН в виде одного файла.

#### 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 нём 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)	3 байта
FID (2 байта)    „01“	Метка подписи EF (FID)	3 байта
xx xx	Поле длины значения	2 байта

Пример данных в файле, загруженном на ВН:

Метка:	Длина	Значение
00 02 00	00 11	Данные EF ICC
C1 00 00	00 C2	Данные EF Card_Certificate
		...
05 05 00	0A 2E	Данные EF Vehicles_Used
05 05 01	00 80	Подпись EF Vehicles_Used



#### 4. Загрузка данных с карточки тахографа через бортовое устройство

- DDP\_047 БУ должно обеспечивать возможность загрузки данных с введённой в него карточки водителя на подключённую СПА.
- DDP\_048 Для инициализации данного режима СПА направляет БУ сообщение «Запрос передачи данных, загружаемых с карточки» (см. 2.2.2.9).
- DDP\_049 После этого БУ файл за файлом загружает с карточки все имеющиеся на ней данные в соответствии с протоколом загрузки, который определён в пункте 3, и передаёт все полученные таким образом данные на СПА в соответствующем формате TLV (см. 3.4.2), заключённые внутри сообщения «Положительный ответ: передача данных».
- DDP\_050 СПА извлекает данные карточки из сообщения «Положительный ответ: передача данных» (освобождая их от всех заголовков, SID, TREP, счётчиков подсообщений и контрольных сумм) и сохраняет их в одном физическом файле, как указано в пункте 2.3.
- DDP\_051 Затем БУ при необходимости обновляет содержание файла Control\_Activity\_Data или Card\_Download на карточке водителя.

## RU

## Приложение 8. Протокол калибровки

## СОДЕРЖАНИЕ

<b>1.</b>	<b>Введение .....</b>	<b>319</b>
<b>2.</b>	<b>Термины, определения и ссылки .....</b>	<b>319</b>
<b>3.</b>	<b>Обзор функций.....</b>	<b>320</b>
3.1.	Поддерживаемые функции .....	320
3.2.	Коды ответов .....	320
<b>4.</b>	<b>Функция обмена данными.....</b>	<b>321</b>
4.1.	Функция StartCommunication .....	321
4.2.	Функция StopCommunication .....	324
4.2.1	Описание сообщения .....	324
4.2.2	Формат сообщения.....	324
4.2.3	Определение параметров.....	325
4.3.	Функция TesterPresent .....	325
4.3.1	Описание сообщения .....	325
4.3.2	Формат сообщения.....	325
<b>5.</b>	<b>Функции управления.....</b>	<b>326</b>
5.1.	Функция StartDiagnosticSession .....	326
5.1.1	Описание сообщения .....	326
5.1.2	Формат сообщения.....	327
5.1.3	Определение параметров.....	328
5.2.	Функция SecurityAccess .....	328
5.2.1	Описание сообщения .....	328
5.2.2	Формат сообщения – SecurityAccess-requestSeed.....	329
5.2.3	Формат сообщения – SecurityAccess-sendKey .....	330
<b>6.</b>	<b>Функции передачи данных.....</b>	<b>332</b>
6.1.	Функция ReadDataByIdentifier .....	332
6.1.1	Описание сообщения .....	332
6.1.2	Формат сообщения.....	332
6.1.3	Определение параметров.....	333
6.2.	Функция WriteDataByIdentifier .....	334
6.2.1	Описание сообщения .....	334
6.2.2	Формат сообщения.....	334
6.2.3	Определение параметров.....	335
<b>7.</b>	<b>Настройка проверочных импульсов – функциональный блок регулировки сигнала ввода/вывода.....</b>	<b>335</b>
7.1.	Функция InputOutputControlByIdentifier .....	335
7.1.1	Описание сообщения .....	335
7.1.2	Формат сообщения.....	336
7.1.3	Определение параметров.....	337
<b>8.</b>	<b>Форматы dataRecords.....</b>	<b>339</b>
8.1.	Диапазоны передаваемых параметров .....	339
8.2.	Форматы dataRecords.....	339

## 1. Введение

В настоящем приложении описано, как происходит обмен данными между бортовым устройством и тестером через К-линию, составляющую часть интерфейса калибровки в соответствии с приложением 6. Также описывается управление сигнальной линией ввода/вывода соединителя калибровки.

Процедура установления связи по К-линии описана в разделе 4 «Функция обмена данными».

Для определения задач управления обменом данными по К-линии при различных условиях в данном приложении используется понятие диагностических сеансов. По умолчанию под этим понимается сеанс StandardDiagnosticSession, при котором с бортового устройства могут быть считаны все имеющиеся данные, однако сохранение данных в бортовом устройстве невозможно.

Выбор вида диагностического сеанса рассмотрен в разделе 5 «Функции управления».

Настоящее приложение должно рассматриваться как относящееся к обоим поколениям БУ и карточек мастерской в соответствии с требованиями эксплуатационной совместимости, изложенными в настоящем регламенте.

CPR\_001 Сеанс ECUProgrammingSession позволяет вводить данные в бортовое устройство. При этом для ввода калибровочных данных бортовое устройство должно быть переведено в режим CALIBRATION.

Процесс передачи данных по К-линии описан в разделе 6 «Функции передачи данных». Форматы передаваемых данных подробно указаны в разделе 8 «Форматы dataRecords».

CPR\_002 ECUAdjustmentSession позволяет осуществлять выбор режима «ввод-вывод» относительно канала ввода-вывода калибровочных данных через интерфейс К-линии. Способ управления каналом ввода-вывода калибровочных данных изложен в разделе 7 «Настройка проверочных импульсов – функциональный блок регулировки сигнала ввода/вывода».

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 ссылки

Протоколы, сообщения и коды ошибок, в принципе, опираются на проект стандарта ISO 14229-1 (Дорожные транспортные средства. Диагностические системы. Часть 1: услуги диагностики, версия 6 от 22 февраля 2001 г.).

Для идентификаторов функций, запросов функций и ответов на них, а также для стандартных параметров используются байтовое кодирование и шестнадцатеричные величины.

Под термином «тестер» понимается аппаратура, используемая для ввода программных/калибровочных данных в БУ.

Под терминами «клиент» и «сервер» понимаются, соответственно, тестер и БУ.

Под аббревиатурой «ECU», означающей «электронный контрольный блок», понимается БУ.

### Ссылки:

ISO 14230-2: Дорожные транспортные средства. Диагностические системы. Ключевой протокол 2000.  
 Часть 2: уровень канала передачи данных.  
 1-е издание: 1999.

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** приведён перечень имеющихся функций.
- Во **2-м столбце** перечислены номера пунктов данного приложения, содержащих развёрнутые 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 разъёма 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 №	Sid Треб. знач.	Диагностические сеансы		
			SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

Таблица 1 – Сводная таблица значений идентификаторов функций

- Символ, означающий обязательность функции для данного диагностического сеанса.

Символа, означающего, что функция для диагностического сеанса применяться не может, не существует.

#### 3.2. Коды ответов

Для каждой функции предусмотрены определённые коды ответов.

#### 4. Функция обмена данными

Ряд функций необходим для установления и поддержания канала обмена данными. На уровне приложений они не отображаются. Описание имеющихся функций приведено в таблице ниже.

Название услуги	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 в БУ, которое уже инициализировано (и уже находится в процессе того или иного диагностического сеанса), поступает новый запрос StartCommunication (например, при восстановлении работы тестера после сбоя), этот запрос принимается и производится повторная инициализация БУ.

CPR\_009 Если по каким-либо причинам канал обмена данными не может быть инициализирован, 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,

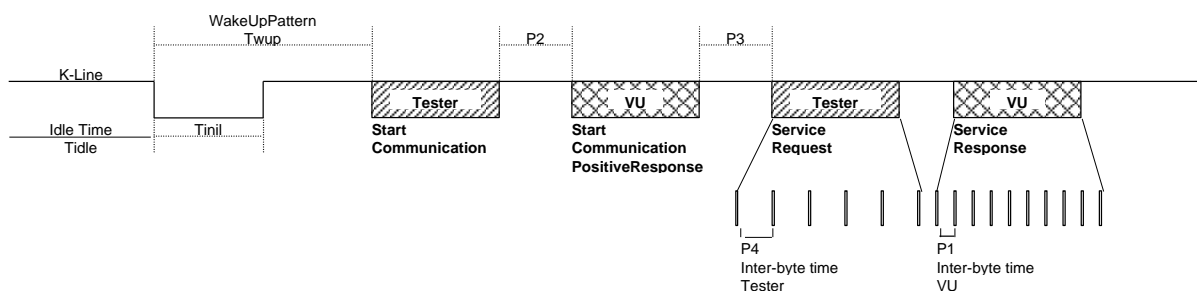
- Любой операции предшествует определённый период бездействия шины.
- Затем тестер высылает шаблон инициализации.
- Ответ БУ содержит всю информацию, необходимую для установления канала обмена данными.

CPR\_012 По завершении инициализации,

- Значения всех параметров обмена данными задаются такими, как определено в Таблица 4 в соответствии с ключевыми байтами.
- БУ ожидает первого запроса от тестера.
- БУ находится в диагностическом режиме, 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 Tini1. Тестер высылает первый бит сообщения StartCommunicationService по истечении периода Twup 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: Tidle = 300 мс.
- После завершения функции StopCommunication: Tidle = P3 мин.
- После перерыва обмена данными в течение периода P3 макс., Tidle = 0.

Параметр	Мин. значение	Макс. значение
Tinil	25 ± 1 мс	26 мс
Twup	50 ± 1 мс	51 мс

Таблица 3 – Временные параметры ускоренной инициализации

Время Параметр	Описание параметра	Нижние предельные значения [мс]	Верхние предельные значения [мс]
		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	5000
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: Нех – шестнадцатеричный)

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	81	FMT
#2	Байт целевого адреса	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	<b>Идентификатор функции запроса StartCommunication</b>	<b>81</b>	<b>SCR</b>
#5	Контрольная сумма	00-FF	CS

Таблица 5 – Сообщение запроса StartCommunication

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
<b>#5</b>	<b>Идентификатор функции положительного ответа на запрос StartCommunication</b>	<b>C1</b>	<b>SCRPR</b>
#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 передаётся, и БУ остаётся в режиме обычной работы.

## 4.2. Функция StartCommunication

### 4.2.1 Описание сообщения

Эта функция уровня обмена данными предназначена для прекращения сеанса обмена.

CPR\_020 По получении примитива индикации StopCommunication БУ проверяет возможность прекращения текущего обмена данными. Если это возможно, БУ выполняет все действия, необходимые для прекращения сеанса обмена данными.

CPR\_021 Если обмен данными может быть прекращён, 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, БУ возвращает примитив ответа StopCommunication с выбранными параметрами отрицательного ответа.

CPR\_023 Если БУ фиксирует истечение периода ожидания P3max, обмен данными прекращается без направления какого-либо примитива ответа.

### 4.2.2 Формат сообщения

CPR\_024 Формат сообщений для примитивов StopCommunication подробно указан в нижеследующих таблицах.

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	01	LEN
#5	<b>Идентификатор функции запроса StopCommunication</b>	<b>82</b>	<b>SPR</b>
#6	Контрольная сумма	00-FF	CS

Таблица 7 – Сообщение запроса StopCommunication

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	01	LEN
#5	<b>Идентификатор функции положительного ответа на запрос StopCommunication</b>	<b>C2</b>	<b>SPRPR</b>
#6	Контрольная сумма	00-FF	CS

Таблица 8 – Сообщение положительного ответа на запрос StopCommunication

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC



#4	Дополнительный байт длины	03	LEN
#5	<b>Идентификатор функции отрицательного ответа</b>	<b>7F</b>	<b>NR</b>
#6	Идентификация функции запроса StopCommunication	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 посылаемый запрос данной функции позволяет поддерживать непрерывный сеанс диагностики/обмена данными, так как счётчик времени P3 обнуляется при каждом очередном поступлении этого запроса.

### 4.3.2 Формат сообщения

CPR\_079 Формат сообщений для примитивов TesterPresent подробно указан в нижеследующих таблицах.

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	02	LEN
#5	<b>Идентификатор функции запроса TesterPresent</b>	<b>3E</b>	<b>TP</b>
#6	Sub Function = responseRequired = [ yes no ]	01 02	RESPREQ_Y RESPREQ_NO
#7	Контрольная сумма	00-FF	CS

Таблица 10 – Сообщение запроса TesterPresent

CPR\_080 Если параметр responseRequired установлен на ответ «да», сервер возвращает положительный ответ, показанный ниже. Если параметр установлен на ответ «нет», на данный запрос сервер не отвечает.

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	01	LEN
#5	<b>Идентификатор функции положительного ответа на запрос TesterPresent</b>	<b>7E</b>	<b>TPPR</b>
#6	Контрольная сумма	00-FF	CS

Таблица 11 – Сообщение положительного ответа на запрос TesterPresent

CPR\_081 В данной функции предусмотрены следующие коды отрицательного ответа:

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	<b>Идентификатор функции отрицательного ответа</b>	<b>7F</b>	<b>NR</b>
#6	Идентификация функции запроса TesterPresent	3E	TP
#7	responseCode = [ SubFunctionNotSupported-InvalidFormat incorrectMessageLength ]	12 13	RC_SFNS_IF RC_I ML
#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 с БУ.
SecurityAccess	Клиент запрашивает доступ к функциям, предназначенным только для санкционированных пользователей.

Таблица 13 – Функции управления

### 5.1. Функция StartDiagnosticSession

#### 5.1.1 Описание сообщения

CPR\_025 Функция StartDiagnosticSession используется для запуска различных диагностических сеансов на сервере. В ходе диагностического сеанса предоставляется доступ к определённому набору функций, указанному в Таблица 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 должно постоянно поддерживать только один текущий диагностический сеанс,
- При подаче питания БУ во всех случаях должно начинать стандартный сеанс диагностики (StandardDiagnosticSession). Если после этого не будет начат другой диагностический сеанс, 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, БУ сначала высылает положительный ответ на запрос StartDiagnosticSession, а затем запускает новый сеанс. Если БУ не имеет возможности начать новый диагностический сеанс в соответствии с запросом, оно возвращает отрицательный ответ на запрос StartDiagnosticSession, а текущий сеанс продолжается.

CPR\_026 Диагностический сеанс может быть начат только при условии, что между клиентом и БУ установлен канал обмена данными.

CPR\_027 Временные параметры, определённые в Таблица 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	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	02	LEN
#5	<b>Идентификатор функции запроса StartDiagnosticSession</b>	<b>10</b>	<b>STDS</b>
#6	diagnosticSession = [одно значение из Таблица 17]	xx	DS_...
#7	Контрольная сумма	00-FF	CS

Таблица 14 – Сообщение запроса StartDiagnosticSession

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	02	LEN
#5	<b>Идентификатор функции положительного ответа на запрос StartDiagnosticSession</b>	<b>50</b>	<b>STDSPR</b>
#6	diagnosticSession = [ такое же значение, как в байте #6 Таблица 14 ]	xx	DS_...
#7	Контрольная сумма	00-FF	CS

Таблица 15 – Сообщение положительного ответа на запрос StartDiagnosticSession

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	<b>Идентификатор функции отрицательного ответа</b>	<b>7F</b>	<b>NR</b>
#6	Идентификатор функции запроса StartDiagnosticSession	10	STDS
#7	ResponseCode = [subFunctionNotSupported <sup>a</sup> incorrectMessageLength <sup>b</sup> conditionsNotCorrect <sup>c</sup>	12 13 22	RC_SFNS RC_IML RC_CNC
#8	Контрольная сумма	00-FF	CS

Таблица 16 – Сообщение отрицательного ответа на запрос StartDiagnosticSession

<sup>a</sup> – значение, заданное в байте #6 запроса, не поддерживается и поэтому не фигурирует в Таблица 17,

<sup>b</sup> – получено сообщение неверной длины,

<sup>c</sup> – 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:

Hex	Описание	Мнемоника
81	<b>StandardDiagnosticSession</b> В ходе данного диагностического сеанса могут использоваться все функции, указанные в столбце 4 «SD» Таблица 1. Эти функции позволяют считывать данные, хранящиеся на сервере (БУ). Данный диагностический сеанс запускается после успешного завершения инициализации канала связи между клиентом (тестер) и сервером (БУ). Данный диагностический сеанс может быть впоследствии заменён другими диагностическими сеансами, о которых говорится в настоящем разделе.	<b>SD</b>
85	<b>ECUProgrammingSession</b> В ходе данного диагностического сеанса могут использоваться все функции, указанные в столбце 6 «ECUPS» Таблица 1. Данные функции поддерживают программирование памяти сервера (БУ). Данный диагностический сеанс может быть впоследствии заменён другими диагностическими сеансами, о которых говорится в настоящем разделе.	<b>ECUPS</b>
87	<b>ECUAdjustmentSession</b> В ходе данного диагностического сеанса могут использоваться все функции, указанные в столбце 5 «ECUAS» Таблица 1. Эти функции обеспечивают регулировку параметров сигнала ввода/вывода сервера (БУ). Данный диагностический сеанс может быть впоследствии заменён другими диагностическими сеансами, о которых говорится в настоящем разделе.	<b>ECUAS</b>

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 доступ к линии ввода/вывода калибровки.

Функция SecurityAccess обеспечивает возможность введения ПИН-кода и получения тестером информации о том, находится ли БУ в режиме CALIBRATION.

Допустимы и другие методы введения ПИН-кода.

### 5.2.1 Описание сообщения

Функция SecurityAccess предусматривает направление сообщения SecurityAccess requestSeed, за которым на соответствующем этапе следует сообщение SecurityAccess sendKey. Функция SecurityAccess выполняется в обязательном порядке после функции StartDiagnosticSession.

CPR\_033 Сообщение SecurityAccess requestSeed используется тестером для проверки готовности бортового устройства к приёму ПИН-кода.

- CPR\_034 Если бортовое устройство уже находится в режиме CALIBRATION, в ответ на запрос оно при помощи функции положительного ответа SecurityAccess возвращает стартовое значение 0x0000.
- CPR\_035 Если бортовое устройство готово принять ПИН-код для проверки карточки мастерской, в ответ на запрос оно при помощи функции положительного ответа SecurityAccess возвращает стартовое значение больше 0x0000.
- CPR\_036 Если бортовое устройство не готово принять от тестера ПИН-код, поскольку вставленная карточка мастерской недействительна или не была введена в устройство, либо потому, что бортовое устройство ожидает введения ПИН-кода другим способом, оно возвращает отрицательный ответ с кодом conditionsNotCorrectorRequestSequenceError.
- CPR\_037 В таких случаях тестер передает ПИН-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 ответ 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 тогда, когда оно находится в режиме CALIBRATION.
- CPR\_039 Ниже перечисляются случаи, когда бортовое устройство возвращает на данный запрос отрицательный ответ, и соответствующие коды 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 ПИН-код; допустимое количество попыток подтверждения ПИН-кода превышено,
  - generalReject: ПИН-код верен, но взаимную аутентификацию устройства и карточки мастерской произвести не удалось.

## 5.2.2 Формат сообщений SecurityAccess-requestSeed

CPR\_040 Формат сообщений для примитивов SecurityAccess requestSeed подробно указан в нижеследующих таблицах.

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	02	LEN
#5	<b>Идентификатор функции запроса SecurityAccess</b>	<b>27</b>	<b>SA</b>
#6	accessType-requestSeed	7D	AT_RSD
#7	Контрольная сумма	00-FF	CS

Таблица 18 – Сообщение SecurityAccess Request-requestSeed

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC

#4	Дополнительный байт длины	04	LEN
#5	<b>Идентификатор функции положительного ответа на запрос SecurityAccess</b>	<b>67</b>	<b>SAPR</b>
#6	accessType-requestSeed	7D	AT_RSD
#7	Верхнее исходное значение	00-FF	SEEDH
#8	Нижнее исходное значение	00-FF	SEEDL
#9	Контрольная сумма	00-FF	CS

Таблица 19 – Сообщение положительного ответа на запрос SecurityAccess-requestSeed

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	<b>Идентификатор функции отрицательного ответа</b>	<b>7F</b>	<b>NR</b>
#6	Идентификатор функции запроса SecurityAccess	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength]	22 13	RC_CNC RC_IML
#8	Контрольная сумма	00-FF	CS

Таблица 20 – Сообщение отрицательного ответа на запрос SecurityAccess

### 5.2.3 Формат сообщений SecurityAccess-sendKey

CPR\_041 Формат сообщений для примитивов SecurityAccess sendKey подробно указан в нижеследующих таблицах.

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	m+2	LEN
#5	<b>Идентификатор функции запроса SecurityAccess</b>	<b>27</b>	<b>SA</b>
#6	accessType-sendKey	7E	AT_SK
#7-#m+6	Ключ #1 (верхний) ... Ключ #m (нижний, m должно составлять не менее 4 и не более 8)	xx ... xx	KEY
#m+7	Контрольная сумма	00-FF	CS

Таблица 21 – Сообщение SecurityAccess Request-sendKey

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	02	LEN

#5	<b>Идентификатор функции положительного ответа на запрос SecurityAccess</b>	67	SAPR
#6	accessType-sendKey	7E	AT_SK
#7	Контрольная сумма	00-FF	CS

Таблица 22 – Сообщение положительного ответа на запрос SecurityAccess-sendKey

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	<b>Идентификатор функции отрицательного ответа</b>	<b>7F</b>	<b>NR</b>
#6	Идентификатор функции запроса SecurityAccess	27	SA
#7	ResponseCode = [generalReject subFunctionNotSupported incorrectMessageLength conditionsNotCorrectOrRequestSequenceError invalidKey exceededNumberOfAttempts requestCorrectlyReceived-ResponsePending]	10 12 13 22 35 36 78	RC_GR RC_SFNS RC_IML RC_CNC RC_IK RC_ENA RC_RCR_RP
#8	Контрольная сумма	00-FF	CS

Таблица 23 – Сообщение отрицательного ответа 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.
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. Производитель БУ должен обеспечить, чтобы эта функция выполнялась с соблюдением заданных условий работы сервера.

#### 6.1.2 Формат сообщения

CPR\_051 Формат сообщений для ReadDataByIdentifier подробно указан в нижеследующих таблицах.

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	03	LEN
#5	<b>Идентификатор функции запроса ReadDataByIdentifier</b>	<b>22</b>	<b>RDBI</b>
#6-#7	recordDataIdentifier = [значение из Таблица 28]	xxxx	RDI_...
#8	Контрольная сумма	00-FF	CS

Таблица 25 – Сообщение запроса ReadDataByIdentifier

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	m+3	LEN
#5	<b>Идентификатор функции положительного ответа на запрос ReadDataByIdentifier</b>	<b>62</b>	<b>RDBIPR</b>
#6 и #7	recordDataIdentifier = [то же значение, что и у байтов #6 и #7 в Таблица 25]	xxxx	RDI_...
#8-#m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Контрольная сумма	00-FF	CS

Таблица 26 – Сообщение положительного ответа на запрос ReadDataByIdentifier



Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	<b>Идентификатор функции отрицательного ответа</b>	<b>7F</b>	<b>NR</b>
#6	Идентификатор функции запроса ReadDataByIdentifier	22	RDBI
#7	ResponseCode=[requestOutOfRange incorrectMessageLength conditionsNotCorrect]	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, определённые в настоящем документе, указаны в таблице ниже.

Таблица значений параметра recordDataIdentifier состоит из четырех столбцов и ряда строк.

- В **1-м столбце (Шестн. значение)** приведено шестнадцатеричное значение, закреплённое за идентификатором recordDataIdentifier, который указан в 3-м столбце.
- **Во 2-м столбце (Элемент данных)** указан элемент данных согласно приложению 1, лежащий в основе параметра recordDataIdentifier (в некоторых случаях требуется перекодирование).
- В **3-м столбце (Описание)** указано наименование соответствующего идентификатора recordDataIdentifier.
- В **4-м столбце (Мнемокод)** указан мнемокод данного идентификатора recordDataIdentifier.

Шестнадцатеричное значение	Элемент данных	Название recordDataIdentifier (см. формат в разделе 8.2)	Мнемоника
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_VRN
F190	VehicleIdentificationNumber	VIN	RDI_VIN

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 с целью запроса у сервера значения записей данных. Данные опознаются по идентификатору recordDataIdentifier. Производитель БУ должен обеспечить, чтобы эта функция выполнялась с соблюдением заданных условий работы сервера. Для обновления значений параметров, перечисленных в Таблица 28, БУ должно быть переведено в режим CALIBRATION.

### 6.2.2 Формат сообщения

CPR\_057 Формат сообщений для WriteDataByIdentifier подробно указан в нижеследующих таблицах.

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	m+3	LEN
<b>#5</b>	<b>Идентификатор функции запроса WriteDataByIdentifier</b>	<b>2E</b>	<b>WDBI</b>
#6-#7	recordDataIdentifier = [значение из Таблица 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	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
<b>#5</b>	<b>Идентификатор функции положительного ответа на запрос WriteDataByIdentifier</b>	<b>6E</b>	<b>WDBIPR</b>
#6-#7	recordDataIdentifier = [то же значение, что и у байтов #6 и #7 в Таблица 29]	xxxx	RDI_...
#8	Контрольная сумма	00-FF	CS

Таблица 30 – Сообщение положительного ответа на запрос WriteDataByIdentifier

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	<b>Идентификатор функции отрицательного ответа</b>	<b>7F</b>	<b>NR</b>
#6	Идентификатор функции запроса WriteDataByIdentifier	2E	WDBI
#7	ResponseCode=[requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31	RC_ROOR
		13	RC_IML
		22	RC_CNC
#8	Контрольная сумма	00-FF	CS

Таблица 31 – Сообщение отрицательного ответа на запрос WriteDataByIdentifier

## 6.2.3 Определение параметров

Определение *recordDataIdentifier (RDI\_)* приводится в Таблица 28.

Параметр *dataRecord (DREC\_)* используется в положительном ответе на запрос WriteDataByIdentifier для сообщения серверу (БУ) значений записи данных, опознаваемой по идентификатору recordDataIdentifier. Форматы данных указаны в разделе 8.

## 7. Настройка проверочных импульсов – функциональный блок регулировки сигнала ввода/вывода

Описание имеющихся функций приведено в таблице ниже:

Название функции	Описание
InputOutputControlByIdentifier	Клиент запрашивает управление параметрами сигнала ввода/вывода данного сервера.

Таблица 32 – Функциональный блок контроля ввода/вывода

## 7.1. Функция InputOutputControlByIdentifier

### 7.1.1 Описание сообщения

Подключение соответствующего тестера к разъёму 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 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 четырёх 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 приёма сигнала скорости в реальном времени, когда канал ввода/вывода калибровочных данных переключён на ввод, канал ввода/вывода калибровочных данных переключается на вывод или возвращается в отключённое 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 (очерёдность выполнения этих двух операций значения не имеет).
- Изменение состояния канала вывода данных с помощью функции InputOutputControlByIdentifier.

## 7.1.2 Формат сообщения

CPR\_062 Формат сообщений для примитивов InputOutputControlByIdentifier подробно указан в нижеследующих таблицах.

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	xx	LEN
#5	<b>Идентификатор функции запроса InputOutputControlByIdentifier</b>	<b>2F</b>	<b>IOCB I</b>
#6 и #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 или #8-#9	ControlOptionRecord = [ inputOutputControlParameter – одно значение из Таблица 36 controlState – одно значение из Таблица 37 (см. примечание ниже)]	xx xx	COR_... IOCP_... CS_...
# 9 или # 10	Контрольная сумма	00-FF	CS

Таблица 33 – Сообщение запроса InputOutputControlByIdentifier

**Примечание:** Параметр controlState присутствует лишь в некоторых случаях (см. 7.1.3).

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	xx	LEN
#5	<b>Идентификатор функции положительного ответа на запрос inputOutputControlByIdentifier</b>	<b>6F</b>	<b>IOCBIPR</b>
#6 и #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO

#8 или #8-#9	controlStatusRecord = [ inputOutputControlParameter (то же значение, что и у байта #8 Таблица 33) controlState (то же значение, что и у байта #9 Таблица 33)] (если применимо)	xx xx	CSR_ IOCP_ CS_...
# 9 или # 10	Контрольная сумма	00-FF	CS

Таблица 34 – Сообщение положительного ответа на запрос InputOutputControlByIdentifier

Байт №	Название параметра	Шестнадцатеричное значение	Мнемоника
#1	Байт формата – физическая адресация	80	FMT
#2	Байт целевого адреса	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	<b>Идентификатор функции отрицательного ответа</b>	<b>7F</b>	<b>NR</b>
#6	Идентификатор функции запроса InputOutputControlByIdentifier	2F	IOCBI
#7	responseCode=[ incorrectMessageLength conditionsNotCorrect requestOutOfRange deviceControlLimitsExceeded]	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 Определение параметра *inputOutputControlParameter (IOCP\_)* приведено в нижеследующей таблице.

Шестнадцатеричное значение	Описание	Мнемоника
00	<b>ReturnControlToECU</b> Это значение оповещает сервер (БУ) о том, что тестер перестал управлять каналом ввода/вывода калибровочных данных.	RCTECU
01	<b>ResetToDefault</b> Это значение оповещает сервер (БУ) о том, что ему следует вернуть канал ввода/вывода калибровочных данных в состояние, выбираемое по умолчанию.	RTD
03	<b>ShortTermAdjustment</b> Это значение оповещает сервер (БУ) о том, что ему следует привести канал ввода/вывода калибровочных данных в соответствие со значением параметра controlState.	STA

Таблица 36 – Определение значений inputOutputControlParameter

CPR\_065 Параметр *controlState* присутствует лишь в случаях, когда параметр inputOutputControlParameter установлен на

ShortTermAdjustment, и определён в нижеследующей таблице:

<b>Режим</b>	<b>Шестнадцатеричное значение</b>	<b>Описание</b>
Отключение	00	Канал ввода/вывода отключён (выбирается по умолчанию)
Включение	01	Канал ввода/вывода калибровочных данных функционирует в режиме speedSignalInput
Включение	02	Канал ввода/вывода калибровочных данных функционирует в режиме realTimeSpeedSignalOutputSensor
Включение	03	Канал ввода/вывода калибровочных данных функционирует в режиме RTCOutput

Таблица 37 – Определение значений controlState

## 8. Форматы dataRecords

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 разделе 6.

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).

### 8.1. Диапазоны передаваемых параметров

CPR\_069 В Таблица 38 определены диапазоны, по которым определяется допустимость передаваемых значений параметров.

CPR\_070 Используя значения диапазона «указатель ошибки», бортовое устройство может незамедлительно сообщать о том, что достоверные параметрические данные на текущий момент отсутствуют из-за той или иной ошибки тахографа.

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 сообщения 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, вместо этих данных используется указатель ошибки, приведённый в Таблица 38. Если же данные, полученные в результате расчётов или измерений, являются достоверными, но выходят за пределы заданного диапазона значений запрошенного параметра, указатель ошибки не используется. В этом случае при передаче данных используется соответствующее минимальное или максимальное значение параметра.

Название диапазона	1 байт (шестнадцатеричное значение)	2 байта (шестнадцатеричное значение)	4 байта (шестнадцатеричное значение)	ASCII
Действительный сигнал	от 00 до FA	от 0000 до FAFF	от 00000000 до FAFFFFFF	от 1 до 254
Указатель конкретного параметра	FB	от FB00 до FBFF	от FB000000 до FBFFFFFF	нет
Диапазон зарезервирован под разряды будущих указателей	от FC до FD	от FC00 до FDFF	от FC000000 до FDFFFFFF	нет
Указатель ошибки	FE	от FE00 до FEFF	от FE000000 до FEFFFFFF	0
Данные отсутствуют или не запрашиваются	FF	от FF00 до FFFF	от FF000000 до FFFFFFFF	FF

Таблица 38 – Диапазоны dataRecords

CPR\_073 Для параметров, представляемых с помощью кода ASCII, символ ASCII «\*» резервируется в качестве ограничителя.

### 8.2. Форматы dataRecords

В Таблица 39-Таблица 42 ниже подробно показаны форматы, используемые в связи с функциями ReadDataByIdentifier и WriteDataByIdentifier.

CPR\_074 В Таблица 39 указываются длина поля данных, разрешение и рабочий диапазон для каждого параметра, определяемого соответствующим идентификатором recordDataIdentifier:

Название параметра	Длина данных (в байтах)	Разрешение	Рабочий диапазон
TimeDate	8	Подробно см. в Таблица 40	
HighResolutionTotalVehicleDistance	4	увеличение 5 м/бит, смещение 0 м	от 0 до +21 055 406 км
Kfactor	2	увеличение 0,001 имп./м /бит, смещение 0	от 0 до 64,255 имп./м
LfactorTyreCircumference	2	увеличение 0,125 10 <sup>-3</sup> м/бит, смещение 0	от 0 до 8 031 м
WvehicleCharacteristicFactor	2	увеличение 0,001 имп./м /бит, смещение 0	от 0 до 64,255 имп./м
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Подробно см. в Таблица 41	
SpeedAuthorised	2	увеличение 1/256 км/ч/бит, смещение 0	от 0 до 250,996 км/ч
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Подробно см. в Таблица 42	
VIN	17	ASCII	ASCII

Таблица 39 – Формат dataRecords

CPR\_075 В Таблица 40 подробно указаны форматы различных байтов параметра TimeDate:

Байт	Определение параметра	Разрешение	Рабочий диапазон
1	Секунды	увеличение 0,25 с/бит, смещение 0 с	от 0 до 59,75 с
2	Минуты	увеличение 1 мин/бит, смещение 0 мин	от 0 до 59 мин
3	Часы	увеличение 1ч/бит, смещение 0 ч	от 0 до 23 ч
4	Месяц	увеличение 1 мес./бит, смещение 0 мес.	от 1 до 12 месяцев
5	День	увеличение 0,25 дня/бит, смещение 0 дней (см. ПРИМЕЧАНИЕ под Таблица 41)	от 0,25 до 31,75 дня
6	Год	увеличение 1 г./бит, смещение +1985 г. (см. ПРИМЕЧАНИЕ под Таблица 41)	от 1985 до 2235 г.
7	Поправка на местное время (мин)	увеличение 1 мин/бит, смещение -125 мин	от -59 до +59 мин
8	Поправка на местное время (ч)	увеличение 1ч/бит, смещение -125 ч	- от 23 до +23 ч

Таблица 40 – Подробный формат TimeDate (recordDataIdentifier, значение # F90B)

CPR\_076 В Таблица 41 подробно указаны форматы различных байтов параметра NextCalibrationDate.



Байт	Определение параметра	Разрешение	Рабочий диапазон
1	Месяц	увеличение 1 мес./бит, смещение 0 мес.	от 1 до 12 месяцев
2	День	увеличение 0,25 дня/бит, смещение 0 дней (см. ПРИМЕЧАНИЕ ниже)	от 0,25 до 31,75 дня
3	Год	увеличение 1 г./бит, смещение +1985 г. (см. ПРИМЕЧАНИЕ ниже)	от 1985 до 2235 г.

Таблица 41 – Подробный формат NextCalibrationDate (recordDataIdentifier, значение # F922)

ПРИМЕЧАНИЕ относительно использования параметра «День»:

- 1) Значение даты, равное 0, информации не содержит. 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 относительно использования параметра байта «Год»:

Значение года, равное 0, соответствует 1985 году; значение, равное 1, – 1986 году и т.д.

CPR\_078 В Таблица 42 подробно указаны форматы различных байтов параметра VehicleRegistrationNumber:

Байт	Определение параметра	Разрешение	Рабочий диапазон
1	Кодовая страница (согласно определению, содержащемуся в приложении 1)	ASCII	от 01 до 0A
2 – 14	Регистрационный номер транспортного средства (согласно определению, содержащемуся в приложении 1)	ASCII	ASCII

Таблица 42 – Подробный формат VehicleRegistrationNumber (recordDataIdentifier, значение # F97E)

## Приложение 9. Утверждение типа. Перечень минимальных требуемых испытаний

### СОДЕРЖАНИЕ

1.	ВВЕДЕНИЕ .....	342
1.1.	Утверждение типа .....	342
1.2.	Ссылки .....	343
2.	ФУНКЦИОНАЛЬНЫЕ ИСПЫТАНИЯ БОРТОВОГО УСТРОЙСТВА .....	345
3.	ФУНКЦИОНАЛЬНЫЕ ИСПЫТАНИЯ ДАТЧИКА ДВИЖЕНИЯ .....	350
4.	ФУНКЦИОНАЛЬНЫЕ ИСПЫТАНИЯ КАРТОЧЕК ТАХОГРАФА.....	353
5.	ИСПЫТАНИЯ ВНЕШНЕГО УСТРОЙСТВА ГНСС .....	362
6.	ИСПЫТАНИЯ СРЕДСТВА УДАЛЁННОЙ СВЯЗИ .....	365
7.	ФУНКЦИОНАЛЬНЫЕ ИСПЫТАНИЯ БУМАГИ .....	367
8.	ИСПЫТАНИЯ НА ЭКСПЛУАТАЦИОННУЮ СОВМЕСТИМОСТЬ.....	369

### 1. Введение

#### 1.1. Утверждение типа

Процедура официального утверждения типа регистрирующей аппаратуры (либо ее компонентов) или карточек тахографа состоит из следующих основных частей:

- **сертификация защиты** на основании спецификаций общих критериев с учётом цели безопасности, полностью соответствующей приложению 10 настоящего приложения (подлежит дополнению/изменению),
- **сертификация функциональности**, проводимая органом государства-члена в целях подтверждения того, что испытываемое изделие соответствует требованиям настоящего приложения по набору выполняемых функций, точности измерений и характеристикам относительно экологии,
- **сертификация эксплуатационной совместимости**, проводимая компетентным органом в целях подтверждения полной эксплуатационной совместимости контрольного устройства (или карточки тахографа) с необходимыми моделями карточек тахографа (или записывающего оборудования) (см. главу 8 настоящего приложения).

В данном приложении содержится перечень минимальных функциональных испытаний, которые должны быть проведены ответственным органом государства-члена, 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 приложении не рассматриваются. Если какие-либо из испытаний, необходимых для официального утверждения типа, уже были проведены в процессе аттестации и сертификации систем защиты, повторное их проведение не требуется. В таких случаях можно ограничиться проверкой результатов этих испытаний. Характеристики, которые должны испытываться при сертификации защиты (или которые тесно связаны с проводимыми при этом испытаниями) в справочных целях помечены в настоящем приложении знаком «\*».

Пронумерованные требования относятся к основной части приложения, а другие требования – к другим приложениям (например, PIC\_001 относится к требованию PIC\_001 приложения 3 «Пиктограммы»).

Официальное утверждение типа датчика движения, бортового устройства и внешнего устройства ГНСС рассматривается в настоящем приложении отдельно, так как речь идёт о разных компонентах записывающего оборудования. Каждому компоненту выдаётся собственный сертификат утверждения типа, в котором указываются другие совместимые компоненты. Функциональное испытание датчика движения (или внешнего устройства ГНСС) проводится вместе с бортовым устройством и наоборот.

Эксплуатационная совместимость между каждой моделью датчика движения (внешнего устройства ГНСС) и каждой моделью бортового устройства не требуется. В подобном случае утверждение типа датчика движения (внешнего устройства ГНСС) может выдаваться только в сочетании с утверждением типа соответствующего бортового устройства и наоборот.

## 1.2. Ссылки

В настоящем приложении используются следующие источники:

IEC 60068-2-1: Экологические испытания. Часть 2-1: испытания. Испытание А: холод

IEC 60068-2-2: Базовые процедуры экологических испытаний. Часть 2: испытания. Часть Б: сухое тепло (синусоида)

IEC 60068-2-6: Экологические испытания. Часть 2: испытания. Испытание Fc: вибрация

IEC 60068-2-14: Экологические испытания. Часть 2-14: испытания. Испытание N: изменение температуры

IEC 60068-2-27: Экологические испытания. Часть 2: испытания. Испытания Ea и руководство: удар

IEC 60068-2-30: Экологические испытания. Часть 2-30: испытания. Испытание Db: влажное тепло, циклично (цикл 12 ч + 12 ч)

IEC 60068-2-64: Экологические испытания. Часть 2-64: испытания. Испытание Fh: вибрация, широкий диапазон частот и руководство

IEC 60068-2-78 Экологические испытания. Часть 2-78: испытания. Помещения для испытаний: влажное тепло, стационарное состояние

ISO 16750-3 – Механическая нагрузка (2012-12)

ISO 16750-4 – Климатическая нагрузка (2010-04).

ISO 20653: Дорожные транспортные средства. Степень защиты (код ИП). Защита электрооборудования от инородных тел, воды и доступа

ISO 10605 :2008 + техническая поправка: 2010 + AMD1 :2014 Дорожные транспортные средства. Методы испытаний электрических помех от электростатического разряда

ISO 7637-1 :2002 + AMD1 : 2008 Дорожные транспортные средства. Электрические помехи от проводимости и соединений. Часть 1: определения и общие положения

ISO 7637-2 Дорожные транспортные средства. Электрические помехи от проводимости и соединений. Часть 2: временная электрическая проводимость только вдоль линий питания

- ISO 7637-3 Дорожные транспортные средства. Электрические помехи от проводимости и соединений. Часть 3: временная электрическая передача через ёмкостную и индуктивную связь по линиям, кроме линии питания
- ISO/IEC 7816-1 Идентификационные карточки – карточки с интегральными микросхемами с контактами. Часть 1: физические характеристики
- ISO/IEC 7816-2 Информационные технологии. Идентификационные карточки – карточки с интегральными микросхемами с контактами. Часть 2: размеры и расположение контактов.
- ISO/IEC 7816-3 Информационные технологии. Идентификационные карточки – карточки с интегральными микросхемами с контактами. Часть 3: электронные сигналы и протокол передачи данных
- ISO/IEC 10373-1 :2006 + AMD1 :2012 Идентификационные карточки. Методы испытаний. Часть 1: общие характеристики
- ISO/IEC 10373-3 :2010 + Техническая поправка :2013 Идентификационные карточки. Методы испытаний. Часть 3: карточки с интегральными микросхемами с контактами и связанные с ними устройства интерфейса
- ISO 16844-3:2004, поправка 1:2006 Дорожные транспортные средства. Системы тахографов. Часть 3: интерфейс датчика движения (с бортовыми устройствами)
- ISO 16844-4 Дорожные транспортные средства. Системы тахографов. Часть 4: интерфейс CAN
- ISO 16844-6 Дорожные транспортные средства. Системы тахографов. Часть 6: диагностика
- ISO 16844-7 Дорожные транспортные средства. Системы тахографов. Часть 7: параметры
- ISO 534 Бумага и картон. Определение толщины, плотности и удельного объёма
- R10 ЕЭК ООН Общие положения об утверждении транспортных средств с точки зрения электромагнитной совместимости (Европейская экономическая комиссия ООН)

## 2. Функциональные испытания бортового устройства

№	Испытание	Описание	Соответствующие требования
<b>1</b>	<b>Административная проверка</b>		
1.1	Документация	Правильность документации	
1.2	Результаты испытаний производителя	Результаты испытаний, проведённых производителем во время интеграции. Проверка технических характеристик по документам	88, 89,91
<b>2</b>	<b>Визуальный осмотр</b>		
2.1	Соответствие документации		
2.2	Идентификация/маркировка		224-226
2.3	Материалы		219-223
2.4	Пломбирование		398, 401-405
2.5	Внешние интерфейсы		
<b>3</b>	<b>Функциональные испытания</b>		
3.1	Предусмотренные функции		03, 04, 05, 07, 382,
3.2	Режимы работы		09-11*, 132, 133
3.3	Функции и права доступа к данным		12* 13*, , 382, 383, 386-389
3.4	Контроль за вводом и извлечением карточек		15, 16, 17, 18, 19*, 20*, 132
3.5	Измерение скорости и пробега		21-31
3.6	Измерение времени (испытание проводится при 20°C)		38-43
3.7	Контроль за деятельностью водителя		44-53, 132
3.8	Контроль за статусом управления		54, 55, 132
3.9	Ручной ввод данных		56-62
3.10	Реагирование на блокировку, установленную предприятием		63-68
3.11	Мониторинг деятельности контроля		69, 70
3.12	Обнаружение событий и/или неисправностей		71-88, 132
3.13	Идентификационные данные аппаратуры		93*, 94*, 97, 100
3.14	Данные о вводе и извлечении карточки водителя		102*-104*
3.15	Данные о деятельности водителя		105*-107*
3.16	Данные о местах и местоположении		108*-112*
3.17	Данные одометра		113*-115*
3.18	Подробные данные о скорости		116*
3.19	Данные о событиях		117*
3.20	Данные о неисправностях		118*
3.21	Данные калибровки		119*-121*
3.22	Данные корректировки времени		124*, 125*
3.23	Данные о контрольных действиях		126*, 127*
3.24	Данные блокировки, установленной предприятием		128*
3.25	Данные о действиях загрузки		129*
3.26	Данные об особых условиях		130*, 131*
3.27	Регистрация и хранение данных на карточках тахографов		134, 135,, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148

3.28	Отображение	90, 132, 149-166, PIC_001, DIS_001
3.29	Печать	90, 132, 167-179, PIC_001, PRT_001-PRT_014
3.30	Предупреждение	132, 180-189, PIC_001
3.31	Загрузка данных на внешние носители	90, 132, 190-194
3.32	Удалённая связь для целевых придорожных проверок	195-197
3.33	Вывод данных на дополнительные внешние устройства	198, 199
3.34	Калибровка	202-206*, 383, 384, 386-391
3.35	Придорожные проверки калибровки	207-209
3.36	Корректировка времени	210-212*
3.37	Отсутствие помех при выполнении дополнительных функций	06, 425
3.38	Интерфейс датчика движения	02, 122
3.39	Внешнее устройство ГНСС	03, 123
3.40	Проверка, что БУ обнаруживает, регистрирует и хранит событие (-я) и/или неисправность (-и), указанные производителем БУ, когда соединённый датчик движения реагирует на магнитные поля, вызывающие помехи при обнаружении движения транспортного средства.	217
3.41	Шифрование и стандартизированные параметры области	CSM_48, CSM_50
<b>4</b>	<b>Экологические испытания</b>	

4.1	Температура	<p>Проверка функциональности следующими средствами:          Испытания в соответствии с ISO 16750-4, глава 5.1.1.2: рабочие испытания при низкой температуре (72 ч при -20 °C)          Данные испытания опираются на IEC 60068-2-1: Экологические испытания. 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)          Данные испытания опираются на IEC 60068-2-2: Базовые процедуры экологических испытаний. Часть 2: испытания. Часть Б: сухое тепло</p> <p>Испытания в соответствии с ISO 16750-4: Глава 5.3.2: быстрая смена температуры с указанной продолжительностью перехода (-20°C/70 °C, 20 циклов, время выдержки 2 ч при каждой температуре)          Возможно проведение сокращённой 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	<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	Механическая часть	<p>1. Синусоидальные вибрации Проверка способности бортового устройства выдерживать синусоидальные вибрации со следующими характеристиками:</p> <p>постоянное смещение в диапазоне 5-1 Гц: пик 10 мм постоянное ускорение в диапазоне 11-300 Гц: 5 г</p> <p>Соответствие данному требованию проверяется согласно стандарту IEC 60068-2-6, испытание Fc минимальной продолжительностью 3x12 часов (по 12 часов на каждую ось)</p> <p>ISO 16750-3 не требует испытаний синусоидальных вибраций для устройств в отсоединённой кабине транспортного средства.</p> <p>2. Случайные колебания: Испытания в соответствии с ISO 16750-3: Глава 4.1.2.8: Испытание VIII: коммерческое транспортное средство, отсоединённая кабина транспортного средства</p> <p>Испытания случайных колебаний, 10...2000 Гц, вертикальные RMS 21,3 м/с<sup>2</sup>, продольные RMS 11,8 м/с<sup>2</sup>, поперечные RMS 13,1 м/с<sup>2</sup>, 3 оси, 32 ч на ось, включая температурный цикл -20...70°C.</p> <p>Данные испытания опираются на IEC 60068-2-64: Экологические испытания. Часть 2-64: испытания. Испытание Fh: вибрация, широкий диапазон частот и руководство</p> <p>3. Удары: механический удар с полусинусоидой 3 г в соответствии с ISO 16750.</p> <p>Вышеуказанные испытания проводятся с использованием разных экземпляров устройства испытываемого образца.</p>	219
4.4	Защита от попадания воды и посторонних предметов	Испытания в соответствии с ISO 20653: Дорожные транспортные средства. Степень защиты (код ИП). Защита электрооборудования от инородных тел, воды и доступа (параметры не меняются). Минимальное значение IP 40	220, 221
4.5	Защита от перегрузок по напряжению	<p>Проверка способности бортового устройства выдерживать следующее напряжение в цепи питания:</p> <p>Вариант на 24 V: 34 V при +40°C 1 час Вариант на 12V: 17 V при +40°C 1 час (ISO 16750-2)</p>	216



4.6	Защита от несоблюдения полярности	Проверка способности бортового устройства выдерживать подключение к источнику питания противоположной полярности (ISO 16750-2)	216
4.7	Защита от короткого замыкания	Проверка защищённости сигналов ввода/вывода от короткого замыкания на источник питания и на массу (ISO 16750-2)	216
<b>5</b>	<b>Испытания на ЭМС</b>		
5.1	Излучения и электромагнитная защищённость	Соответствие Регламенту ЕЭК R10	218
5.2	Электростатический разряд	Соответствие ISO 10605 :2008 + Техническая поправка :2010 + AMD1 :2014: +/- 4 kV для контакта и +/- 8 kV для расхода воздуха	218
5.3	Подверженность кондуктивным помехам в питании	Варианты на 24 V: соответствие с ISO 7637-2 + Регламент № 10 ЕЭК, ред. 3: импульс 1a: $V_s = -450 \text{ V}$ $R_i = 50 \text{ ом}$ импульс 2a: $V_s = +37 \text{ V}$ $R_i = 2 \text{ ом}$ импульс 2b: $V_s = +20 \text{ V}$ $R_i = 0,05 \text{ ом}$ импульс 3a: $V_s = -150 \text{ V}$ $R_i = 50 \text{ ом}$ импульс 3b: $V_s = +150 \text{ V}$ $R_i = 50 \text{ ом}$ импульс 4: $V_s = -16 \text{ V}$ $V_a = -12 \text{ V}$ $t_6 = 100 \text{ мс}$ импульс 5: $V_s = +120 \text{ V}$ $R_i = 2,2 \text{ ом}$ $t_d = 250 \text{ мс}$ Варианты на 12V: соответствие с ISO 7637-1 + Регламент № 10 ЕЭК, ред. 3: импульс 1: $V_s = -75 \text{ V}$ $R_i = 10 \text{ ом}$ импульс 2a: $V_s = +37 \text{ V}$ $R_i = 2 \text{ ом}$ импульс 2b: $V_s = +10 \text{ V}$ $R_i = 0,05 \text{ ом}$ импульс 3a: $V_s = -112 \text{ V}$ $R_i = 50 \text{ ом}$ импульс 3b: $V_s = +75 \text{ V}$ $R_i = 50 \text{ ом}$ импульс 4: $V_s = -6 \text{ V}$ $V_a = -5 \text{ V}$ $t_6 = 15 \text{ мс}$ импульс 5: $V_s = +65 \text{ V}$ $R_i = 3 \text{ ом}$ $t_d = 100 \text{ мс}$ 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-я ред., глава 4.6.4.	218

## 3. Функциональные испытания датчика движения

№	Испытание	Описание	Соответствующие требования
<b>1.</b>	<b>Административная проверка</b>		
1.1	Документация	Правильность документации	
<b>2.</b>	<b>Визуальный осмотр</b>		
2.1.	Соответствие документации		
2.2.	Идентификация/маркировка		225, 226,
2.3	Материалы		219-223
2.4.	Пломбирование		398, 401-405
<b>3.</b>	<b>Функциональные испытания</b>		
3.1	Идентификационные данные датчика		95-97*
3.2	Соединение датчика движения с бортовым устройством		122*, 204
3.3	Обнаружение движения Точность измерения движения		30-35
3.4	Интерфейс транспортного средства		02
3.5	Проверка, устойчив ли датчик движения к постоянному магнитному полю. Кроме того, проверка, что датчик движения реагирует на постоянные магнитные поля, вызывающие помехи при обнаружении движения транспортного средства, чтобы подсоединённое БУ могло обнаруживать, регистрировать и хранить неисправности датчика		217
<b>4.</b>	<b>Экологические испытания</b>		
4.1	Рабочая температура	Проверка работоспособности (в соответствии с определением, приведённым для испытания № 3.3) в температурном диапазоне [-40°C; +135°C] согласно следующим средствам: IEC 60068-2-1, испытание Ad: продолжительность испытания 96 часов при нижней предельной температуре $T_{\min}$ , IEC 60068-2-2, испытание Bd: продолжительность испытания 96 часов при верхней предельной температуре $T_{\max}$ Испытания в соответствии с ISO 16750-4: Глава 5.1.1.2: рабочие испытания при низкой температуре (24 ч при -40 °C) Данные испытания опираются на IEC 60068-2-1: Экологические испытания. Часть 2-1: испытания. Испытание A: холод IEC 68-2-2, испытание Bd: продолжительность испытания 96 часов при нижней предельной температуре -40°C. Испытания в соответствии с ISO 16750-4: Глава 5.1.2.2: рабочие испытания при высокой температуре (96 ч при 135°C) Данные испытания опираются на IEC 60068-2-2: Базовые процедуры экологических испытаний. Часть 2: испытания. Часть Б: сухое тепло	213

4.2	Термоциклы	Испытания в соответствии с ISO 16750-4: Глава 5.3.2: Быстрая смена температуры с указанной продолжительностью перехода (-40°C/135°C, 20 циклов, время выдержки 30 мин при каждой температуре) IEC 60068-2-14: Экологические испытания. Часть 2-14: испытания. Испытание N: изменение температуры	213
4.3	Циклы влажности	Проверка работоспособности (как указано в испытании № 3.3) согласно 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	214
4.4	Вибрация	ISO 16750-3: Глава 4.1.2.6: Испытание VI: Коммерческое транспортное средство, двигатель, коробка передач  Испытания на вибрацию в смешанном режиме, включая  а) Испытания на синусоидальные вибрации, 20...520 Гц, 11,4 ... 120 м/с <sup>2</sup> , ≤ 0,5 окт./мин.  б) Испытания на случайные колебания, 10...2000 Гц, RMS 177 м/с <sup>2</sup>  94 ч на каждую ось, включая термоцикл -20...70°C)  Данные испытания опираются на IEC 60068-2-80: Экологические испытания. Часть 2-80: испытания. Испытание Fi: вибрация, смешанный режим	219
4.5	Механический удар	ISO 16750-3: Глава 4.2.3: Испытание VI: Испытания устройств в или на коробке передач  полусинусоидальный удар, ускорение, подлежащее согласованию в пределах 3000...15000 м/с <sup>2</sup> , продолжительность импульса, подлежащая согласованию, но < 1 мс, число ударов: подлежит согласованию  Данные испытания опираются на IEC 60068-2-27: Экологические испытания. Часть 2: испытания. Испытания Ea и руководство: удар	219
4.6	Защита от попадания воды и посторонних предметов	Испытания в соответствии с ISO 20653: Дорожные транспортные средства. Степень защиты (код ИП). 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 защищённости сигналов ввода/вывода от короткого замыкания на источник питания и на массу	216
<b>5.</b>	<b>ЭМС</b>		
5.1	Излучения и электромагнитная защищённость	Проверка соответствия Регламенту ЕЭК R10	218

5.2	Электростатический разряд	Соответствие ISO 10605 :2008 + Техническая поправка :2010 + AMD1 :2014: +/- 4 kV для контакта и +/- 8 kV для расхода воздуха	218
5.3	Подверженность кондуктивным помехам в каналах передачи данных	<p>Варианты на 24 V: соответствие с ISO 7637-2 + Регламент № 10 ЕЭК, ред. 3: импульс 1a: <math>V_s = -450 \text{ V}</math> <math>R_i = 50 \text{ ом}</math> импульс 2a: <math>V_s = +37 \text{ V}</math> <math>R_i = 2 \text{ ом}</math> импульс 2b: <math>V_s = +20 \text{ V}</math> <math>R_i = 0,05 \text{ ом}</math> импульс 3a: <math>V_s = -150 \text{ V}</math> <math>R_i = 50 \text{ ом}</math> импульс 3b: <math>V_s = +150 \text{ V}</math> <math>R_i = 50 \text{ ом}</math> импульс 4: <math>V_s = -16 \text{ V}</math> <math>V_a = -12 \text{ V}</math> <math>t_6 = 100 \text{ мс}</math> импульс 5: <math>V_s = +120 \text{ V}</math> <math>R_i = 2,2 \text{ ом}</math> <math>t_d = 250 \text{ мс}</math></p> <p>Варианты на 12V: соответствие с ISO 7637-1 + Регламент № 10 ЕЭК, ред. 3: импульс 1: <math>V_s = -75 \text{ V}</math> <math>R_i = 10 \text{ ом}</math> импульс 2a: <math>V_s = +37 \text{ V}</math> <math>R_i = 2 \text{ ом}</math> импульс 2b: <math>V_s = +10 \text{ V}</math> <math>R_i = 0,05 \text{ ом}</math> импульс 3a: <math>V_s = -112 \text{ V}</math> <math>R_i = 50 \text{ ом}</math> импульс 3b: <math>V_s = +75 \text{ V}</math> <math>R_i = 50 \text{ ом}</math> импульс 4: <math>V_s = -6 \text{ V}</math> <math>V_a = -5 \text{ V}</math> <math>t_6 = 15 \text{ мс}</math> импульс 5: <math>V_s = +65 \text{ V}</math> <math>R_i = 3 \text{ ом}</math> <math>t_d = 100 \text{ мс}</math></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-я ред., глава 4.6.4</p>	218

#### 4. Функциональные испытания карточек тахографа

Испытания в соответствии с данным разделом 4,

№ 5 «Протокольные испытания»,

№ 6 «Структура карточки» и

№ 7 «Функциональные испытания»

может проводить оценщик или сертифицирующее лицо в рамках процедуры сертификации защиты по общим критериям, касающейся модуля микросхемы.

Испытания № 2.3 и № 4.2 одинаковы. Это механические испытания всего модуля основы карточки и микросхемы. Если меняется один из этих компонентов (основа карточки, модуль микросхемы), такие испытания необходимы.

№	Испытание	Описание	Соответствующие требования
<b>1.</b>	<b>Административная проверка</b>		
1.1	Документация	Правильность документации	
<b>2</b>	<b>Основа карточки</b>		
2.1	Дизайн печати	<p>Проверка правильности нанесения на карточку всех элементов защиты и визуальной информации и их соответствия установленным требованиям</p> <p>[Указатель] Приложение 1С, глава 4.1 «Визуальная информация», 227) На первой странице указываются: слова «Карточка водителя» или «Контрольная карточка», или «Карточка мастерской», или «Карточка предприятия», напечатанные заглавными буквами на официальном языке или языках государства-члена, выдавшего карточку, в соответствии с типом карточки.</p> <p>[название государства-члена] Приложение 1С, глава 4.1 «Визуальная информация», 228) На первой странице указываются: название государства-члена, выдавшего карточку (необязательно).</p> <p>[Знак] Приложение 1С, глава 4.1 «Визуальная информация», 229) На первой странице указываются: отличительный знак государства-члена, выдавшего карточку, напечатанный в виде негатива в синем прямоугольнике в окружении 12 жёлтых звёзд.</p> <p>[Перечисление] Приложение 1С, глава 4.1 «Визуальная информация», 232) На обратной стороне указываются: разъяснение пронумерованных позиций, содержащихся на лицевой стороне карточки.</p>	227-229, 232, 234-236

		<p>[Цвет] Приложение 1С, глава 4.1 «Визуальная информация», 234) Текст карточек тахографа печатается на фоне следующих основных цветов: - карточка водителя: белый, - карточка мастерской: красный, - контрольная карточка: синий, - карточка предприятия: жёлтый.</p> <p>[Защита] Приложение 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 1С, глава 4.1 «Визуальная информация», 236) Государства-члены могут включать цвета или маркировку, например, национальные символы и элементы защиты.</p> <p>[Знак официального утверждения] Карточки тахографа снабжаются знаком 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 свидетельства 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 Идентификационные карточки – физические характеристики, [5] Габариты карточки, [5.1] Размер карточки, [5.1.1] Габариты и погрешности карточки, тип карточки ID-1 Неиспользованная карточка</p>	240, 243 ISO/IEC 7810

		<p>[Края карточки] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Идентификационные карточки – 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 Идентификационные карточки – физические характеристики, [7] Материалы карточки</p> <p>[Жёсткость при сгибании] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Идентификационные карточки – физические характеристики, [8] Характеристики карточки, [8.1] Жёсткость при сгибании</p> <p>[Токсичность] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Идентификационные карточки – физические характеристики, [8] Характеристики карточки, [8.3] Токсичность</p> <p>[Стойкость к химическим веществам] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Идентификационные карточки – физические характеристики, [8] Характеристики карточки, [8.4] Стойкость к химическим веществам</p> <p>[Стабильность карточки] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Идентификационные карточки – 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 Идентификационные карточки – физические характеристики, [8] Характеристики карточки, [8.6] Освещение</p> <p>[Долговечность] Приложение 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 Идентификационные карточки – физические характеристики, [8] Характеристики карточки, [8.8] Прочность на отслаивание</p> <p>[Сцепление или блокирование] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Идентификационные карточки – физические характеристики, [8] Характеристики карточки, [8.9] Сцепление или блокирование</p> <p>[Коробление] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Идентификационные карточки – физические характеристики, [8] Характеристики карточки, [8.11] Общее коробление карточки</p> <p>[Теплостойкость] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Идентификационные карточки – физические характеристики, [8] Характеристики карточки, [8.12] Теплостойкость</p> <p>[Искажения поверхности] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Идентификационные карточки – физические характеристики, [8] Характеристики карточки, [8.13] Искажения поверхности</p>	
--	--	--	--



		[Загрязнение] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810 Идентификационные карточки – физические характеристики, [8] Характеристики карточки, [8.14] Загрязнение и взаимодействие компонентов карточки	
2.3	Механические испытания встроенного модуля микросхемы	[Сгибание] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810:2003/Amd. 1:2009, Идентификационные карточки – физические характеристики, поправка 1: Критерии для карточек с интегральными микросхемами [9.2] Динамическое напряжение при сгибании Общее число циклов сгибания: 4000. [Скручивание] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810:2003/Amd. 1:2009, Идентификационные карточки – физические характеристики, поправка 1: Критерии для карточек с интегральными микросхемами [9.2] Динамическое напряжение при скручивании Общее число циклов скручивания: 4000.	ISO/IEC 7810
<b>3</b>	<b>Модуль</b>		
3.1	Модуль	Модуль – это изоляция микросхемы и контактная пластинка. [Контур поверхности] Карточки тахографа должны соответствовать стандарту ISO/IEC 7816-1:2011 Идентификационные карточки – карточки с интегральными микросхемами. Часть 1: карточки с контактами – физические характеристики [4.2] Контур поверхности контактов [Механическая прочность] Карточки тахографа должны соответствовать стандарту ISO/IEC 7816-1:2011 Идентификационные карточки – карточки с интегральными микросхемами. Часть 1: карточки с контактами – физические характеристики [4.3] Механическая прочность (карточки и контактов) [Электрическое сопротивление] Карточки тахографа должны соответствовать стандарту ISO/IEC 7816-1:2011 Идентификационные карточки – карточки с интегральными микросхемами. Часть 1: карточки с контактами – физические характеристики [4.4] Электрическое сопротивление (контактов)	ISO/IEC 7816

		<p>[Габариты] Карточки тахографа должны соответствовать стандарту ISO/IEC 7816-1:2011 Идентификационные карточки – карточки с интегральными микросхемами. Часть 2: карточки с контактами – габариты и расположение контактов [3] Габариты контактов</p> <p>[Расположение] Карточки тахографа должны соответствовать стандарту ISO/IEC 7816-1:2011 Идентификационные карточки – карточки с интегральными микросхемами. Часть 2: карточки с контактами – габариты и расположение контактов [4] Число и расположение контактов В случае модулей с шестью контактами настоящее требование испытаний не относится к контактам C4 и C8.</p>	
<b>4</b>	<b>Микросхема</b>		
4.1	Микросхема	<p>[Рабочая температура] Микросхема карточки тахографа работает в диапазоне температур окружающей среды от -25°C до +85 °C.</p> <p>[Температура и влажность] Приложение 1С, глава 4.4 «Экологические и электрические спецификации», 241) Карточки тахографа способны надлежащим образом работать в любых климатических условиях, которые обычно встречаются на территории Сообщества, как минимум в диапазоне температур от -25°C до +70°C с нерегулярными пиковыми значениями до +85°C; при этом термин «нерегулярные» означает не более 4 часов каждый раз и не более 100 раз в течение всего срока службы карточки. Карточки тахографа через последовательные этапы на определённый период времени подвергаются воздействию следующих температур и влажности. После каждого этапа карточки тахографа проходят испытания на электрическую функциональность.</p> <ol style="list-style-type: none"> <li>1. Температура – 20°C на 2 ч.</li> <li>2. Температура +/- 0 °C на 2 ч.</li> <li>3. Температура + 20 °C, 50 % RH на 2 ч.</li> <li>4. Температура + 50 °C, 50 % RH на 2 ч.</li> <li>5. Температура + 70 °C, 50 % RH на 2 ч.</li> </ol> <p>Температура периодически повышается до + 85 °C, 50 % RH, на 60 мин.</p> <ol style="list-style-type: none"> <li>6. Температура + 70 °C, 85 % RH на 2 ч.</li> </ol> <p>Температура периодически повышается до + 85 °C, 85 % RH, на 30 мин.</p> <p>[Влажность] Приложение 1С, глава 4.4 «Экологические и электрические спецификации», 242) Карточки тахографа полностью работоспособны в диапазоне влажности от 10% до 90%.</p>	<p>241-244 ЕЭК R10 ISO/IEC 7810 ISO/IEC 10373</p>

		<p>[Электромагнитная совместимость (ЭМС)] Приложение 1С, глава 4.4 «Экологические и электрические спецификации» 244) В процессе работы карточки тахографа соответствуют Правилам ЕЭК № 10, касающимся электромагнитной совместимости.</p> <p>[Статическое электричество] Приложение 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, Идентификационные карточки – физические характеристики, поправка 1: Критерии для карточек с интегральными микросхемами [9.4] Статическое электричество [9.4.1] Контактные карточки с ИС Испытательное напряжение: 4000 V.</p> <p>[Рентгеновское излучение] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810:2003/Amd. 1:2009, Идентификационные карточки – физические характеристики, поправка 1: Критерии для карточек с интегральными микросхемами [9.1] Рентгеновское излучение</p> <p>[Ультрафиолетовое излучение] ISO/IEC 10373-1 :2006 Идентификационные карточки. Методы испытаний. Часть 1: Общие характеристики [5.11] Ультрафиолетовое излучение</p> <p>[3 колеса] Карточки тахографа должны соответствовать стандарту ISO/IEC 10373-1:2006/Amd. 1:2012, Идентификационные карточки. Методы испытаний. Часть 1: общие характеристики, поправка 1: [5.22] ICC – механическая прочность: 3-колёсное испытание для ICC с контактами</p> <p>[Перегиб] Карточки тахографа должны соответствовать стандарту MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Испытание прочности на перегиб [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 с интегральными микросхемами [9.2] Динамическое напряжение при сгибании Общее число циклов сгибания: 4000.</p>	ISO/IEC 7810

		[Скручивание] Карточки тахографа должны соответствовать стандарту ISO/IEC 7810:2003/Amd. 1:2009, Идентификационные карточки – физические характеристики, поправка 1: Критерии для карточек с интегральными микросхемами [9.2] Динамическое напряжение при скручивании Общее число циклов скручивания: 4000.	
<b>5</b>	<b>Протокольные испытания</b>		
5.1	ATR	Проверка, соответствует ли ATR	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Проверка, соответствует ли протокол T=0	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Проверка совместимости команды PTS путём задания протокола T=1 при исходном T=0	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Проверка, соответствует ли протокол T=1	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
<b>6</b>	<b>Структура данных на карточке</b>		
6.1		Подтверждение соответствия файловой структуры на карточке путём проверки наличия обязательных файлов и тестирования условий доступа к ним	TCS_22-TCS_28 TCS_140- TCS_179
<b>7</b>	<b>Функциональные испытания</b>		
7.1	Нормальная обработка	Хотя бы однократное испытание 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, путём считывания файла после исполнения команды на его обработку)	TCS_29-TCS_139
7.2	Сообщения об ошибке	Хотя бы однократное тестирование каждого сообщения об ошибке (из числа указанных в приложении 2) при исполнении каждой команды Хотя бы однократное тестирование на общую ошибку каждого вида (кроме ошибок целостности серии '6400', которые тестируются при сертификации систем защиты)	
7.3	Шифрование и стандартизированные параметры области		CSM_48, CSM_50
<b>8</b>	<b>Персонализация</b>		
8.1	Оптическая персонализация	Приложение 1С, глава 4.1 «Визуальная информация», 230) На первой странице указываются: конкретная информация, касающаяся выданной карточки.	230, 231, 235

	<p>Приложение 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> <hr/> <p>Приложение 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 перекрывает фотография.</p>	
--	---	--

## 5. Испытания внешнего устройства ГНСС

№	Испытание	Описание	Соответствующие требования
<b>1.</b>	<b>Административная проверка</b>		
1.1	Документация	Правильность документации	
<b>2.</b>	<b>Визуальный осмотр внешнего устройства ГНСС</b>		
2.1.	Соответствие документации		
2.2.	Идентификация/маркировка		224-226
2.3	Материалы		219-223
<b>3.</b>	<b>Функциональные испытания</b>		
3.1	Идентификационные данные датчика		98,99
3.2	Соединение внешнего модуля ГНСС и бортового устройства		123, 205
3.3	Расположение ГНСС		36, 37
3.4	Интерфейс бортового устройства, если приёмник ГНСС установлен как внешнее устройство относительно БУ		03
3.5	Шифрование и стандартизированные параметры области		CSM_48, CSM_50
<b>4.</b>	<b>Экологические испытания</b>		
4.1	Температура	<p>Проверка функциональности следующими средствами: Испытания в соответствии с ISO 16750-4, глава 5.1.1.2: рабочие испытания при низкой температуре (72 ч при -20 °C) Данные испытания опираются на IEC 60068-2-1: Экологические испытания. 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) Данные испытания опираются на IEC 60068-2-2: Базовые процедуры экологических испытаний. Часть 2: испытания. Часть Б: сухое тепло</p> <p>Испытания в соответствии с ISO 16750-4: Глава 5.3.2: быстрая смена температуры с указанной продолжительностью перехода (-20°C/70 °C, 20 циклов, время выдержки 1 ч при каждой температуре) Возможно проведение сокращённой 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 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	214

4.3	Механическая часть	<p>1. Синусоидальные вибрации Проверка способности бортового устройства выдерживать синусоидальные вибрации со следующими характеристиками:</p> <p>постоянное ускорение в диапазоне 5-1 Гц: пик 10 мм</p> <p>постоянное ускорение в диапазоне 11-300 Гц: 5 г</p> <p>Соответствие данному требованию проверяется согласно стандарту IEC 60068-2-6, испытание Fc минимальной продолжительностью 3x12 часов (по 12 часов на каждую ось)</p> <p>ISO 16750-3 не требует испытаний синусоидальных вибраций для устройств в отсоединённой кабине транспортного средства.</p> <p>2. Случайные колебания: Испытания в соответствии с ISO 16750-3: Глава 4.1.2.8: Испытание VIII: коммерческое транспортное средство, отсоединённая кабина транспортного средства</p> <p>Испытания случайных колебаний, 10...2000 Гц, вертикальные RMS 21,3 м/с<sup>2</sup>, продольные RMS 11,8 м/с<sup>2</sup>, поперечные RMS 13,1 м/с<sup>2</sup>, 3 оси, 32 ч на ось, включая температурный цикл -20...70°C.</p> <p>Данные испытания опираются на IEC 60068-2-64: Экологические испытания. Часть 2-64: испытания. Испытание Fh: вибрация, широкий диапазон частот и руководство</p> <p>3. Удары: механический удар с полусинусоидой 3 г в соответствии с ISO 16750.</p> <p>Вышеуказанные испытания проводятся с использованием разных экземпляров устройства испытываемого образца.</p>	219
4.4	Защита от попадания воды и посторонних предметов	Испытания в соответствии с ISO 20653: Дорожные транспортные средства. Степень защиты (код ИП). Защита электрооборудования от инородных тел, воды и доступа (параметры не меняются).	220, 221
4.5	Защита от перегрузок по напряжению	<p>Проверка способности бортового устройства выдерживать следующее напряжение в цепи питания:</p> <p>Вариант на 24 V: 34V при +40°C 1 час</p> <p>Вариант на 12V: 17 V при +40°C 1 час</p> <p>(ISO 16750-2, глава 4.3)</p>	216
4.6	Защита от несоблюдения полярности	<p>Проверка способности бортового устройства выдерживать подключение к источнику питания противоположной полярности</p> <p>(ISO 16750-2, глава 4.7)</p>	216

4.7	Защита от короткого замыкания	Проверка защищённости сигналов ввода/вывода от короткого замыкания на источник питания и на массу (ISO 16750-2, глава 4.10])	216
<b>5</b>	<b>Испытания на ЭМС</b>		
5.1	Излучения и электромагнитная защищённость	Соответствие Регламенту ЕЭК R10	218
5.2	Электростатический разряд	Соответствие ISO 10605 :2008 + Техническая поправка :2010 + AMD1 :2014: +/- 4 kV для контакта и +/- 8 kV для расхода воздуха	218
5.3	Подверженность кондуктивным помехам в питании	<p>Варианты на 24 V: соответствие с ISO 7637-2 + Регламент № 10 ЕЭК, ред. 3: импульс 1a: <math>V_s = -450 \text{ V}</math> <math>R_i = 50 \text{ ом}</math> импульс 2a: <math>V_s = +37 \text{ V}</math> <math>R_i = 2 \text{ ом}</math> импульс 2b: <math>V_s = +20 \text{ V}</math> <math>R_i = 0,05 \text{ ом}</math> импульс 3a: <math>V_s = -150 \text{ V}</math> <math>R_i = 50 \text{ ом}</math> импульс 3b: <math>V_s = +150 \text{ V}</math> <math>R_i = 50 \text{ ом}</math> импульс 4: <math>V_s = -16 \text{ V}</math> <math>V_a = -12 \text{ V}</math> <math>t_6 = 100 \text{ мс}</math> импульс 5: <math>V_s = +120 \text{ V}</math> <math>R_i = 2,2 \text{ ом}</math> <math>t_d = 250 \text{ мс}</math></p> <p>Варианты на 12V: соответствие с ISO 7637-1 + Регламент № 10 ЕЭК, ред. 3: импульс 1: <math>V_s = -75 \text{ V}</math> <math>R_i = 10 \text{ ом}</math> импульс 2a: <math>V_s = +37 \text{ V}</math> <math>R_i = 2 \text{ ом}</math> импульс 2b: <math>V_s = +10 \text{ V}</math> <math>R_i = 0,05 \text{ ом}</math> импульс 3a: <math>V_s = -112 \text{ V}</math> <math>R_i = 50 \text{ ом}</math> импульс 3b: <math>V_s = +75 \text{ V}</math> <math>R_i = 50 \text{ ом}</math> импульс 4: <math>V_s = -6 \text{ V}</math> <math>V_a = -5 \text{ V}</math> <math>t_6 = 15 \text{ мс}</math> импульс 5: <math>V_s = +65 \text{ V}</math> <math>R_i = 3 \text{ ом}</math> <math>t_d = 100 \text{ мс}</math></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-я ред., глава 4.6.4.</p>	218



## 6. Испытания средства удалённой связи

№	Испытание	Описание	Соответствующие требования
<b>1.</b>	<b>Административная проверка</b>		
1.1	Документация	Правильность документации	
<b>2.</b>	<b>Визуальный осмотр</b>		
2.1.	Соответствие документации		
2.2.	Идентификация/маркировка		225, 226
2.3	Материалы		219-223
<b>4.</b>	<b>Экологические испытания</b>		
4.1	Температура	<p>Проверка функциональности следующими средствами: Испытания в соответствии с ISO 16750-4, глава 5.1.1.2: рабочие испытания при низкой температуре (72 ч при -20 °C) Данные испытания опираются на IEC 60068-2-1: Экологические испытания. 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) Данные испытания опираются на IEC 60068-2-2: Базовые процедуры экологических испытаний. Часть 2: испытания. Часть Б: сухое тепло</p> <p>Испытания в соответствии с ISO 16750-4: Глава 5.3.2: быстрая смена температуры с указанной продолжительностью перехода (-20°C/70 °C, 20 циклов, время выдержки 1 ч (?) при каждой температуре) Возможно проведение сокращённой серии испытаний (из числа указанных в разделе 3 настоящей таблицы) при низкой и высокой температурах, а также на протяжении термоциклов</p>	213
4.4	Защита от попадания воды и посторонних предметов	Испытания в соответствии с ISO 20653: Дорожные транспортные средства. Степень защиты (код ИП). Защита электрооборудования от инородных тел, воды и доступа (целевое значение IP40).	220, 221
<b>5</b>	<b>Испытания на ЭМС</b>		
5.1	Излучения и электромагнитная защищённость	Соответствие Регламенту ЕЭК R10	218
5.2	Электростатический разряд	Соответствие ISO 10605 :2008 + Техническая поправка :2010 + AMD1 :2014: +/- 4 kV для контакта и +/- 8 kV для расхода воздуха	218

5.3	Подверженность кондуктивным помехам в питании	<p>Варианты на 24 V: соответствие с ISO 7637-2 + Регламент № 10 ЕЭК, ред. 3:  импульс 1a: <math>V_s = -450 \text{ V}</math> <math>R_i = 50 \text{ ом}</math>  импульс 2a: <math>V_s = +37 \text{ V}</math> <math>R_i = 2 \text{ ом}</math>  импульс 2b: <math>V_s = +20 \text{ V}</math> <math>R_i = 0,05 \text{ ом}</math>  импульс 3a: <math>V_s = -150 \text{ V}</math> <math>R_i = 50 \text{ ом}</math>  импульс 3b: <math>V_s = +150 \text{ V}</math> <math>R_i = 50 \text{ ом}</math>  импульс 4: <math>V_s = -16 \text{ V}</math> <math>V_a = -12 \text{ V}</math> <math>t_6 = 100 \text{ мс}</math>  импульс 5: <math>V_s = +120 \text{ V}</math> <math>R_i = 2,2 \text{ ом}</math> <math>t_d = 250 \text{ мс}</math></p> <p>Варианты на 12V: соответствие с ISO 7637-1 + Регламент № 10 ЕЭК, ред. 3:  импульс 1: <math>V_s = -75 \text{ V}</math> <math>R_i = 10 \text{ ом}</math>  импульс 2a: <math>V_s = +37 \text{ V}</math> <math>R_i = 2 \text{ ом}</math>  импульс 2b: <math>V_s = +10 \text{ V}</math> <math>R_i = 0,05 \text{ ом}</math>  импульс 3a: <math>V_s = -112 \text{ V}</math> <math>R_i = 50 \text{ ом}</math>  импульс 3b: <math>V_s = +75 \text{ V}</math> <math>R_i = 50 \text{ ом}</math>  импульс 4: <math>V_s = -6 \text{ V}</math> <math>V_a = -5 \text{ V}</math> <math>t_6 = 15 \text{ мс}</math>  импульс 5: <math>V_s = +65 \text{ V}</math> <math>R_i = 3 \text{ ом}</math> <math>t_d = 100 \text{ мс}</math></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-я ред., глава 4.6.4.</p>	218
-----	---	---	-----

## 7. Функциональные испытания бумаги

№	Испытание	Описание	Соответствующие требования
<b>1.</b>	<b>Административная проверка</b>		
1.1	Документация	Правильность документации	
<b>2</b>	<b>Общие испытания</b>		
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 1.	174
2.4	Определение распечаток	Проверка утверждения типа тахографа и визуальный осмотр распечаток	174
2.5	Читаемость и идентификационные данные распечаток	Проверка распечаток По отчётам испытаний и тестовым протоколам производителя. Все номера утверждения тахографов, с которыми может использоваться печатная бумага, указываются на бумаге.	175, 177, 178
2.6	Добавление рукописных заметок	Визуальный осмотр: Есть поле для подписи водителя. Есть поля для других дополнительных рукописных записей.	180
2.7	Дополнительные сведения о лицевых поверхностях 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
<b>3</b>	<b>Испытания хранения</b>		
3.1	Сухое тепло	Предварительное кондиционирование: 16 часов при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C} / 55\% \pm 3\%$ относительной влажности Тестовая среда: 72 часа при $+70^{\circ}\text{C} \pm 2^{\circ}\text{C}$ Восстановление: 16 часов при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C} / 55\% \pm 3\%$ относительной влажности	176, 178 IEC 60068-2-2-Bb
2.2	Влажное тепло	Предварительное кондиционирование: 16 часов при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C} / 55\% \pm 3\%$ относительной влажности Тестовая среда: 144 часа при $+55^{\circ}\text{C} \pm 2^{\circ}\text{C}$ и $93\% \pm 3\%$ относительной влажности Восстановление: 16 часов при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C} / 55\% \pm 3\%$ относительной влажности	176, 178 IEC 60068-2-78-Cab
<b>4</b>	<b>Испытания бумаги во время работы</b>		
4.1	Влагостойкий фон (бумага без печати)	Предварительное кондиционирование: 16 часов при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C} / 55\% \pm 3\%$ относительной влажности Тестовая среда: 144 часа при $+55^{\circ}\text{C} \pm 2^{\circ}\text{C}$ и $93\% \pm 3\%$ относительной влажности Восстановление: 16 часов при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C} / 55\% \pm 3\%$ относительной влажности	176, 178 IEC 60068-2-78-Cab

4.2	Печатные свойства	Предварительное кондиционирование: 24 часа при $+40^{\circ}\text{C} \pm 2^{\circ}\text{C}$ / $93\% \pm 3\%$ относительной влажности Тестовая среда: распечатка при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C}$ Восстановление: 16 часов при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C}$ / $55\% \pm 3\%$ относительной влажности	176, 178
4.3	Теплостойкость	Предварительное кондиционирование: 16 часов при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C}$ / $55\% \pm 3\%$ относительной влажности Тестовая среда: 2 часа при $+70^{\circ}\text{C} \pm 2^{\circ}\text{C}$ , сухое тепло Восстановление: 16 часов при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C}$ / $55\% \pm 3\%$ относительной влажности	176, 178 IEC 60068-2-2-Bb
4.4	Стойкость к низким температурам	Предварительное кондиционирование: 16 часов при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C}$ / $55\% \pm 3\%$ относительной влажности Тестовая среда: 24 часа при $-20^{\circ}\text{C} \pm 3^{\circ}\text{C}$ , сухой холод Восстановление: 16 часов при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C}$ / $55\% \pm 3\%$ относительной влажности	176, 178 ISO 60068-2-1-Ab
4.5	Светостойкость	Предварительное кондиционирование: 16 часов при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C}$ / $55\% \pm 3\%$ относительной влажности Тестовая среда: 100 часов при освещении 5000 лк при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C}$ / $55\% \pm 3\%$ относительной влажности Восстановление: 16 часов при $+23^{\circ}\text{C} \pm 2^{\circ}\text{C}$ / $55\% \pm 3\%$ 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
9.1. Испытания на эксплуатационную совместимость между бортовыми устройствами и карточками тахографов		
1	Взаимная аутентификация	Проверка нормального выполнения процедур взаимной аутентификации бортового устройства и карточки тахографа
2	Проверка записи/считывания данных	Отработка типового сценария функционирования бортового устройства. Сценарий выбирается с учётом 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.
9.2. Испытания на эксплуатационную совместимость между бортовыми устройствами и датчиками движения		
1	Соединение	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 создаёт 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.
9.3. Испытания на эксплуатационную совместимость между бортовыми устройствами и внешними устройствами ГНСС (если применимо)		
1	Взаимная аутентификация	Проверка нормального выполнения процедур взаимной аутентификации (соединения) бортового устройства и внешнего модуля ГНСС.
2	Рабочие испытания	Отработка типового сценария функционирования внешней ГНСС. Сценарий включает в себя нормальную деятельность и создаёт 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.

RU

## Приложение 10.

### Требования к безопасности

В настоящем приложении представлены требования по безопасности информационных технологий (ИТ) для компонентов систем «умных» тахографов (тахографов второго поколения).

SEC\_001 Защита нижеперечисленных компонентов систем «умных» тахографов подлежит сертификации в соответствии со схемой общих критериев:

- бортовое устройство,
- карточка тахографа,
- датчик движения,
- внешнее устройство ГНСС.

SEC\_002 Минимальные требования по безопасности ИТ, которым должен соответствовать каждый компонент, которому необходима сертификация защиты, определяются в характеристиках защиты компонента в соответствии со схемой общих критериев.

SEC\_003 Европейская комиссия заботится о том, чтобы четыре нижеперечисленных набора характеристик защиты по настоящему приложению были финансированы, разработаны и утверждены правительственными сертификационными органами безопасности ИТ в рамках объединённой рабочей группы по толкованию (JWG), поддерживающей взаимное признание сертификатов согласно европейскому соглашению SOGIS-MRA (соглашению о взаимном признании сертификатов оценки безопасности информационных технологий) и чтобы такие характеристики были зарегистрированы:

- Набор характеристик защиты бортового устройства,
- Набор характеристик защиты карточки тахографа,
- Набор характеристик защиты датчика движения,
- Набор характеристик защиты внешнего устройства ГНСС.

Набор характеристик защиты бортового устройства охватывает случаи, когда БУ эксплуатируется с внешним устройством ГНСС или без него. В первом случае требования к безопасности внешнего устройства ГНСС представлены в специальном наборе характеристик.

SEC\_004 Производители компонентов по мере необходимости уточняют и дополняют соответствующие наборы характеристик компонентов, не меняя или не удаляя установленные спецификации угроз, задач, процедур и функций обеспечения безопасности, чтобы сформировать целевой уровень защиты, относительно которого они будут добиваться сертификации компонента.

SEC\_005 В процессе оценки должно быть подтверждено строгое соответствие такого целевого уровня защиты соответствующему набору характеристик защиты.

SEC\_006 Уровень обеспечения выполнения каждого набора характеристик защиты соответствует EAL4 с компонентами обеспечения защиты ATE\_DPT.2 и AVA\_VAN.5.

**RU**

**Приложение 11. Общие механизмы безопасности**

## СОДЕРЖАНИЕ

Препамбула .....	374
<b>ЧАСТЬ А. СИСТЕМА ТАХОГРАФОВ ПЕРВОГО ПОКОЛЕНИЯ .....</b>	<b>375</b>
<b>1.    Введение .....</b>	<b>375</b>
1.1.    Ссылки .....	375
1.2.    Условные обозначения и сокращённые термины .....	375
<b>2.    Криптографические системы и алгоритмы .....</b>	<b>376</b>
2.1.    Криптографические системы .....	376
2.2.    Криптографические алгоритмы .....	377
2.2.1    Алгоритм RSA .....	377
2.2.2    Алгоритм хеширования .....	377
2.2.3    Алгоритм шифрования данных .....	377
<b>3.    Ключи и сертификаты .....</b>	<b>377</b>
3.1.    Генерация и рассылка ключей .....	377
3.1.1    Генерация и рассылка ключей RSA .....	377
3.1.2    Испытательные ключи RSA .....	379
3.1.3    Ключи датчика движения .....	379
3.1.4    Генерация и рассылка ключей сеанса T-DES .....	379
3.2.    Ключи .....	379
3.3.    Сертификаты .....	379
3.3.1    Содержание сертификатов .....	380
3.3.2    Выдаваемые сертификаты .....	382
3.3.3    Проверка и расшифровка сертификатов .....	382
<b>4.    Механизм взаимной аутентификации.....</b>	<b>383</b>
<b>5.    Механизмы обеспечения конфиденциальности, целостности и аутентификации данных при их передаче между БУ и карточками .....</b>	<b>386</b>
5.1.    Защищённый обмен сообщениями .....	386
5.2.    Обработка ошибок при защищённом обмене сообщениями .....	387
5.3.    Алгоритм расчёта криптографических контрольных сумм .....	388
5.4.    Алгоритм расчёта криптограмм для защиты конфиденциальности ОД .....	389
<b>6.    Механизмы цифровой подписи при загрузке данных.....</b>	<b>389</b>
6.1.    Генерация подписей .....	389
6.2.    Проверка подписей .....	389
<b>ЧАСТЬ Б. СИСТЕМА ТАХОГРАФОВ ВТОРОГО ПОКОЛЕНИЯ .....</b>	<b>391</b>
<b>7.    Введение .....</b>	<b>391</b>
7.1.    Ссылки .....	391
7.2.    Условные обозначения и сокращения .....	392
7.3.    Определения .....	393
<b>8.    Криптографические системы и алгоритмы .....</b>	<b>393</b>
8.1.    Криптографические системы .....	393
8.2.    Криптографические алгоритмы .....	394
8.2.1    Симметричные алгоритмы .....	394
8.2.2    Асимметричные алгоритмы и стандартизированные параметры области .....	394
8.2.3    Алгоритмы хеширования .....	394
8.2.4    Последовательности шифров .....	395
<b>9.    Ключи и сертификаты .....</b>	<b>395</b>



9.1.	Асимметричные пары ключей и сертификаты открытых ключей .....	395
9.1.1	Общие положения .....	395
9.1.2	Европейский уровень.....	395
9.1.3	Уровень государства-члена.....	396
9.1.4	Аппаратный уровень: бортовые устройства.....	397
9.1.5	Аппаратный уровень: карточки тахографа.....	398
9.1.6	Аппаратный уровень: внешние устройства ГНСС .....	399
9.1.7	Обзор: замена сертификата .....	400
9.2.	Симметричные ключи .....	402
9.2.1	Ключи для обеспечения связи между БУ и датчиком движения .....	402
9.2.1.1	Общие положения.....	404
9.2.1.2	Замена ключа старшего порядка датчика движения в оборудовании второго поколения .....	407
9.2.2	Ключи для обеспечения связи DSRC .....	406
9.2.2.1	Общие положения.....	408
9.2.2.2	Замена ключа старшего порядка DSRC .....	410
9.3.	Сертификаты .....	409
9.3.1	Общие положения.....	409
9.3.2	Содержание сертификатов .....	410
9.3.2.1	Идентификатор описания сертификата.....	412
9.3.2.2	Указатель сертифицирующего органа .....	412
9.3.2.3	Полномочия держателя сертификата .....	413
9.3.2.4	Открытый ключ.....	413
9.3.2.5	Указатель держателя сертификата .....	413
9.3.2.6	Дата вступления сертификата в силу .....	413
9.3.2.7	Дата истечения срока действия сертификата .....	413
9.3.2.8	Подпись сертификата .....	413
9.3.3	Заявки на сертификаты.....	412
<b>10.</b>	<b>Взаимная аутентификация БУ и карточки и защищённый обмен сообщениями</b>	<b>413</b>
10.1.	Общие положения.....	413
10.2.	Взаимная проверка цепочки сертификата .....	413
10.2.1	Проверка цепочки сертификата карточки, проводимая БУ .....	413
10.2.2	Проверка цепочки сертификата БУ, проводимая карточкой .....	416
10.3.	Аутентификация БУ .....	418
10.4.	Аутентификация микросхемы и согласование сеансовых ключей .....	419
10.5.	Защищённый обмен сообщениями.....	421
10.5.1	Общие положения.....	421
10.5.2	Структура защищённого сообщения.....	422
10.5.3	Отмена сеанса защищённого обмена сообщениями .....	424
<b>11.</b>	<b>Соединение, взаимная аутентификация и защищённый обмен сообщениями между БУ и внешним устройством ГНСС .....</b>	<b>426</b>
11.1.	Общие положения.....	426
11.2.	Соединение БУ и внешнего устройства ГНСС .....	426
11.3.	Взаимная проверка цепочки сертификата .....	426
11.3.1	Общие положения.....	426
11.3.2	Во время соединения БУ и EGF .....	426
11.3.3	Во время нормальной эксплуатации .....	427
11.4.	Аутентификация БУ, аутентификация микросхемы и согласование сеансовых ключей .....	428
11.5.	Защищённый обмен сообщениями.....	428
<b>12.</b>	<b>Соединение и связь между БУ и датчиком движения.....</b>	<b>429</b>
12.1.	Общие положения.....	429
12.2.	Соединение БУ и датчика движения с использованием различных поколений ключей .....	429

12.3.	Соединение и связь между БУ и датчиком движения с использованием AES .....	431
12.4.	Соединение БУ и датчика движения с использованием аппаратуры разных поколений .....	432
<b>13.</b>	<b>Защита удалённой связи через DSRC .....</b>	<b>432</b>
13.1.	Общие положения .....	432
13.2.	Шифрование данных тахографа и генерирование MAC .....	433
13.3.	Проверка и расшифровка данных тахографа .....	434
<b>14.</b>	<b>Подписание загружаемых данных и проверка подписей .....</b>	<b>435</b>
14.1.	Общие положения .....	435
14.2.	Генерирование подписей .....	435
14.3.	Проверка подписей .....	435

### Преамбула

Настоящее приложение описывает механизмы безопасности, обеспечивающие

- взаимную аутентификацию между различными компонентами системы тахографов.
- конфиденциальность, целостность, подлинность и/или неподдельности данных, передаваемых между различными компонентами системы тахографов или загружаемых на внешние носители.

Приложение состоит из двух частей. Часть А характеризует механизмы безопасности для системы тахографов первого поколения (цифрового тахографа). Часть Б характеризует механизмы безопасности для системы тахографов второго поколения («умного» тахографа).

Механизмы, представленные в части А настоящего приложения, применяются, если хотя бы один из компонентов системы тахографа, участвующий во взаимной аутентификации и/или передаче данных, принадлежит к первому поколению.

Механизмы, представленные в части Б настоящего приложения, применяются, если оба компонента системы тахографа, участвующие во взаимной аутентификации и/или передаче данных, принадлежат ко второму поколению.

В приложении 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. Ссылки

В настоящем приложении используются следующие источники:

SHA-1	Национальный институт стандартов и технологий (NIST). <i>Публикация FIPS 180-1: стандарт безопасного хеширования</i> . Апрель 1995 г.
PKCS1	Лаборатории RSA. PKCS # 1: <i>стандарт шифрования RSA</i> . Версия 2.0. Октябрь 1998 г.
TDES	Национальный институт стандартов и технологий (NIST). <i>Публикация FIPS 46-3: стандарт шифрования данных</i> . Проект 1999 г.
TDES-OP	ANSI X9.52, Рабочие режимы алгоритма тройного шифрования данных. 1998.
ISO/IEC 7816-4	Информационные технологии. Идентификационные карточки – карточки с интегральными микросхемами с контактами – Часть 4: межсекторные команды обмена данными. 1-е издание: 1995 + поправка 1: 1997.
ISO/IEC 7816-6	Информационные технологии. Идентификационные карточки – карточки с интегральными микросхемами с контактами – Часть 6: межсекторные элементы данных. 1-е издание: 1996 + поправка 1: 1998.
ISO/IEC 7816-8	Информационные технологии. Идентификационные карточки – карточки с интегральными микросхемами с контактами – Часть 8: Межсекторные команды, связанные с безопасностью. 1-е издание, 1999.
ISO/IEC 9796-2	Информационные технологии. Техника обеспечения безопасности. Схемы цифровой подписи с восстановлением сообщений. Часть 2: механизмы с использованием хэш-функции. 1-е издание: 1997.
ISO/IEC 9798-3	Информационные технологии. Техника обеспечения безопасности. Механизмы аутентификации субъектов. Часть 3: аутентификация субъектов с применением алгоритма открытого ключа. 2-е издание, 1998.
ISO 16844-3	Дорожные транспортные средства. Системы тахографов. Часть 3: интерфейс датчика движения.

#### 1.2. Условные обозначения и сокращённые термины

В настоящем приложении используются следующие условные обозначения и сокращённые термины:

(K <sub>a</sub> , K <sub>b</sub> , K <sub>c</sub> )	набор ключей, используемый в рамках алгоритма тройного шифрования данных,
CA	Сертифицирующий орган,
CAR	Указатель сертифицирующего органа,
CC	Криптографическая контрольная сумма,
CG	Криптограмма,
CH	Заголовок команды,
CHA	Полномочия держателя сертификата,
CHR	Указатель держателя сертификата,
D()	Расшифровка при помощи DES,
DE	Элемент данных,
DO (ОД)	Объект данных,
<i>d</i>	Закрытый ключ в криптосистеме RSA, закрытая экспонента,

<i>e</i>	Открытый ключ в криптосистеме RSA, открытая экспонента,
E()	Шифрование при помощи DES,
EQT	Аппаратура,
Hash()	Значение хеш-функции, выходные данные <i>хеширования</i> ,
Hash	Хеш-функция,
KID	Ключевой идентификатор,
Km	Ключ TDES. Ключ верхнего уровня, определение которого содержится в ISO 16844-3.
Km <sub>VU</sub>	Ключ TDES, вводимый в бортовые устройства.
Km <sub>WC</sub>	Ключ TDES, вводимый в карточки мастерской.
<i>m</i>	Репрезентативный параметр сообщения, целое число от 0 до <i>n</i> -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 подписи, целое число от 0 до <i>n</i> -1,
SSC	Счётчик исходящих сообщений,
SM	Защищённый обмен сообщениями,
TCBC	Режим сцепления криптоблоков при тройном шифровании данных TDEA
TDEA	Алгоритм тройного шифрования данных,
TLV	Значение длины метки,
VU (БУ)	Бортовое устройство,
X.C	Сертификат пользователя X, выданный сертификационным органом,
X.CA	Сертификационный орган пользователя X,
X.CA.PK <sub>o</sub> X.C	Операция по расшифровке сертификата с целью извлечения открытого ключа. Используется двухкомпонентный оператор, левым компонентом которого является открытый ключ сертификационного органа, а правым компонентом выданный этим сертификационный органом сертификат. Результатом операции является открытый ключ пользователя X, сертификат которого использовался в качестве правого компонента;
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	Закрытый ключ пользователя X в криптосистеме RSA,
X.SK[I]	Шифрование информации I по системе RSA с использованием закрытого 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 для решения следующих задач 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 её 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 выражается 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 расчётов RSA это целое число в диапазоне от 3 до  $n-1$ , удовлетворяющее условию  $\text{gcd}(e, \text{lcm}(p-1, q-1))=1$ .

### 2.2.2 Алгоритм хеширования

CSM\_004 В схемах цифровой подписи используется хеш-алгоритм SHA-1, описание которого приведено 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 трёх функциональных уровнях, которые образуют следующую иерархию:

- европейский уровень,
- уровень государства-члена,
- аппаратный уровень.

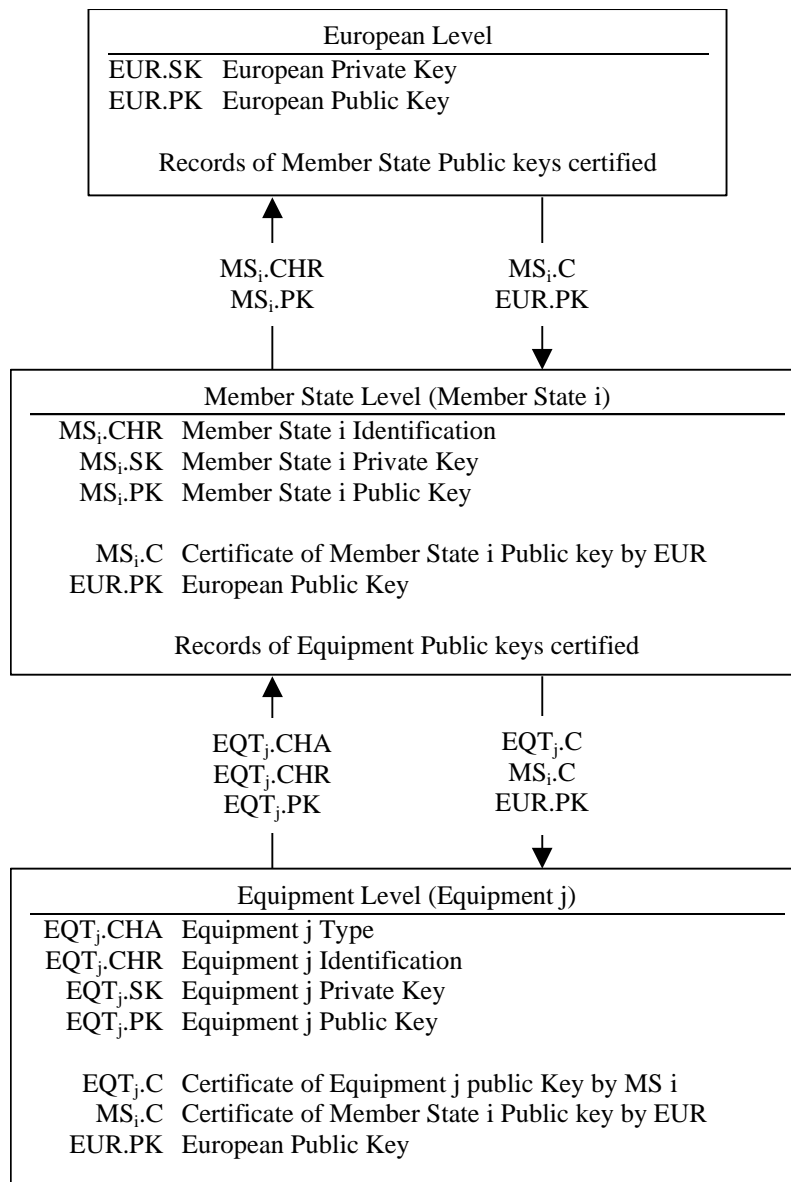
CSM\_007 На европейском уровне генерируется единая пара общеевропейских ключей (EUR.SK и EUR.PK). Закрытый европейский ключ служит для сертификации открытых ключей государств-членов. Все сертифицируемые ключи подлежат регистрации. Эти задачи выполняет европейский сертификационный орган под руководством и при ответственности Европейской комиссии.

CSM\_008 На уровне государств-членов генерируется пара ключей государств-членов (MS.SK и MS.PK). Открытые ключи государств-членов сертифицируются европейским сертификационным органом. Закрытый ключ государства-члена 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. Государство-член может регулярно менять свою пару ключей.

CSM\_009 На аппаратном уровне генерируется единая пара ключей (EQT.SK и EQT.PK), вводимых в каждое устройство. Открытые ключи аппаратного уровня сертифицирует сертификационный орган государства-члена. Эти функции могут также выполнять производители аппаратуры, предприятия, персонализирующие аппаратуру, или соответствующие органы государств-членов. 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 сертификационный орган генерирует отдельную единую пару общеевропейских испытательных ключей и не менее двух пар испытательных ключей для государств-членов, открытые ключи которых сертифицируются закрытым испытательным ключом общеевропейского уровня. При испытаниях, проводимых с целью официального утверждения типовых образцов, в испытываемую аппаратуру производителями вводятся испытательные ключи, сертифицированные одним из вышеупомянутых испытательных ключей государств-членов.

### 3.1.3 Ключи датчика движения

При генерации, транспортировке (если она необходима) и хранении трёх ключей TDES, о которых говорится ниже, соблюдается надлежащий режим конфиденциальности.

В целях обеспечения совместимости с компонентами тахографов, соответствующими стандарту ISO 16844, европейский сертификационный орган и сертификационные органы государств-членов предпринимают нижеследующие дополнительные меры:

CSM\_036 Европейский 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 европейский сертификационный орган высылает им эти ключи с соблюдением надлежащих процедур защиты.

CSM\_037 Сертификационные органы государств-членов:

- используют ключ  $K_m$  для шифрования показаний датчиков движения в соответствии с указаниями производителей этих датчиков (определение данных, подлежащих шифрованию ключом  $K_m$ , даётся в стандарте ISO 16844-3),
- с соблюдением надлежащих процедур защиты высылают  $K_{m_{VU}}$  производителям бортовых устройств для ввода в эти устройства,
- обеспечивают ввод  $K_{m_{WC}}$  во все карточки мастерских (запись `SensorInstallationSecData` в элементарном файле `Sensor_Installation_Data`) при персонализации карточек.

### 3.1.4 Генерация и рассылка ключей сеанса 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 Данный ключ используется при всех последующих операциях криптозащищённого обмена сообщениями. Он перестаёт действовать по окончании текущего сеанса (извлечение или перезагрузка карточки) и/или после 240-го использования (однократное использование ключа = передача на карточку одного защищённого 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 чётности не задаются.

## 3.3. Сертификаты

CSM\_016 Сертификаты открытых ключей RSA – «не самодокументирующие» сертификаты, поддающиеся проверке (источник: 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	Наблюдения
CPI	INTEGER	1	Идентификатор профиля сертификата (в данной версии – ‘01’)
CAR	OCTET STRING	8	Указатель сертифицирующего органа
CHA	OCTET STRING	7	Полномочия держателя сертификата
EOV	TimeReal	4	Дата истечения срока действия сертификата. Может не указываться; в этом случае поле заполняется байтами “FF”.
CHR	OCTET STRING	8	Указатель держателя сертификата
<i>n</i>	OCTET STRING	128	Открытый ключ (модуль)
<i>e</i>	OCTET STRING	8	Открытый ключ (открытая экспонента)
		<b>164</b>	

#### 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.

Данному сертификату соответствует следующий список заголовков:

Метка расширенного списка заголовков	‘4D’	Длина списка заголовков	‘16’	Метка CPI	‘5F 29’	Длина CPI	‘01’	Метка CAR	‘42’	Длина CAR	‘08’	Метка CHA	‘5F 4B’	Длина CHA	‘07’	Метка EOV	‘5F 24’	Длина EOV	‘04’	Метка CHR	‘5F 20’	Длина CHR	‘08’	Метка открытого ключа (генерируется)	‘7F 49’	Длина последующих элементов данных	‘05’	Метка модуля	‘81’	Длина модуля	‘81 80’	Метка открытой экспоненты	‘82’	Длина открытой экспоненты	‘08’
--------------------------------------	------	-------------------------	------	-----------	---------	-----------	------	-----------	------	-----------	------	-----------	---------	-----------	------	-----------	---------	-----------	------	-----------	---------	-----------	------	--------------------------------------	---------	------------------------------------	------	--------------	------	--------------	---------	---------------------------	------	---------------------------	------

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, посвящённом идентификаторам ключей).
3. Полномочия держателя сертификата (CHA) – указание на объём прав, предоставляемых сертификатом. Они включают в себя идентификатор приложения тахографа и типа аппаратуры, для которой предназначен сертификат (соответствует элементу данных EquipmentType; для государства-члена используется значение ‘00’).



4. 2. Указатель держателя сертификата (CHR) 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 оборудования	Дата	Тип	Производитель
Длина	4 байта	2 байта	1 байт	1 байт
Значение	Целое число	мм гг VCD-код	Относится к конкретному производителю	Код производителя

Когда речь идёт о БУ, его производитель, запрашивая сертификаты, не обязательно должен знать идентификационные данные аппаратуры, в которую будут вводиться соответствующие ключи.

Если эти идентификационные данные производителю известны, он направляет их вместе с открытым ключом на сертификацию в сертификационный орган своего государства-члена. Выданный в результате сертификат будет содержать идентификационные данные аппаратуры, и производителю необходимо будет принять меры к тому, чтобы ключи и сертификат вводились именно в ту аппаратуру, для которой они предназначены. Идентификатор ключа при этом имеет вид, показанный выше.

Если идентификационные данные производителю неизвестны, он должен однозначно идентифицировать каждый запрос на сертификат и направляет такие идентификационные данные вместе с открытым ключом на сертификацию в сертификационный орган своего государства-члена. В выданном сертификате будет указано индивидуальное обозначение заявки. После ввода ключа в аппаратуру производитель должен информировать сертификационный орган своего государства-члена о закреплении этого ключа за соответствующей аппаратурой (т.е. сообщить индивидуальное обозначение заявки на сертификат и идентификационные данные аппаратуры). При этом идентификатор ключа выглядит следующим образом:

Данные	Серийный номер заявки на выдачу сертификата	Дата	Тип	Производитель
Длина	4 байта	2 байта	1 байт	1 байт
Значение	Целое число	мм гг VCD-код	'FF'	Код производителя

#### 5.2 Сертифицирующий орган:

Данные	Идентификационные данные органа	Серийный номер ключа	Дополнительная информация	Идентификатор
Длина	4 байта	1 байт	2 байта	1 байт
Значение	Цифровой код государства 1 байт Буквенно-цифровой код государства 3 байта	Целое число	Дополнительное кодирование (относится к конкретному СА) 'FF FF', если не используется	'01'

Серийный номер ключа позволяет отличать друг от друга различные ключи государства-члена в случае смены им своего ключа.

6. Сторона, проверяющая сертификат, по косвенным признакам распознаёт 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 Выдаваемый сертификат представляет собой цифровую подпись с возможностью частичного восстановления содержания сертификата, соответствующую стандарту ISO/IEC 9796-2 (за исключением дополнения A4) и сопровождаемую указателем сертификационного органа.

$$X.C = X.CA.SK[‘6A’ \parallel C_r \parallel Hash(Cc) \parallel ‘BC’] \parallel C_n \parallel X.CAR$$

С содержанием сертификата =  $C_c = C_r \parallel C_n$   
 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	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  $CAR'$ :  $X.C = Sign \parallel C_n' \parallel CAR'$   
 128 байтов    58 байтов    8 байтов
- из  $CAR'$  выбирается открытый ключ соответствующего сертификационного органа (если он не выбран до этого иным способом)
- функция  $Sign$  открывается при помощи открытого ключа CA:  $Sr' = X.CA.PK [Sign]$ ,
- 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
- Восстанавливается содержание сертификата  $C' = C_r' \parallel C_n'$ ,
- проверяется  $Hash(C') = H'$

Положительный результат проверки указывает на подлинность сертификата, содержание которого соответствует С'.

Подтверждение действительности. Из С':

- если применимо, проверяется дата истечения срока действия сертификата.

Извлечение из С' 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

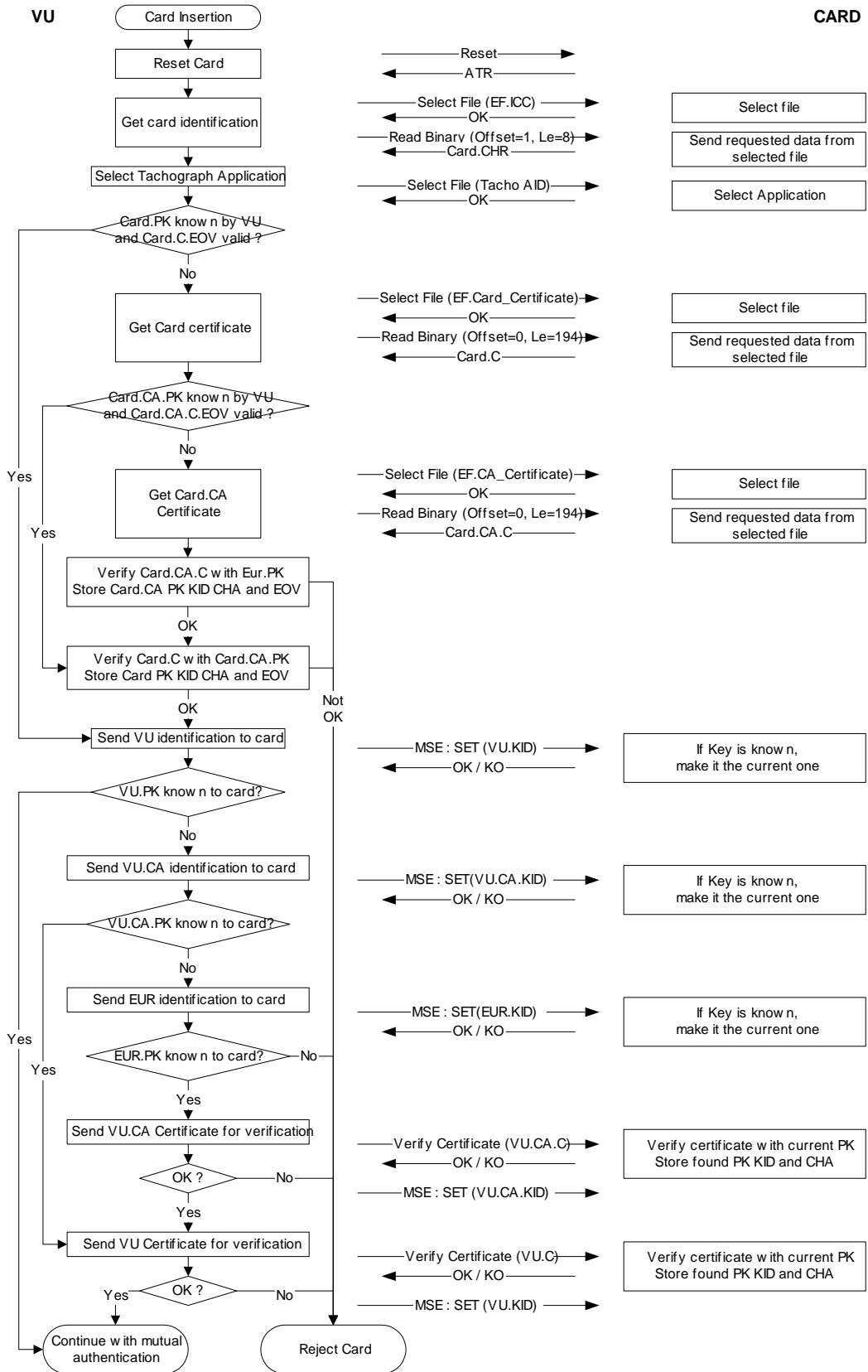
В основу механизма взаимной аутентификации карточек и БУ положен следующий принцип:

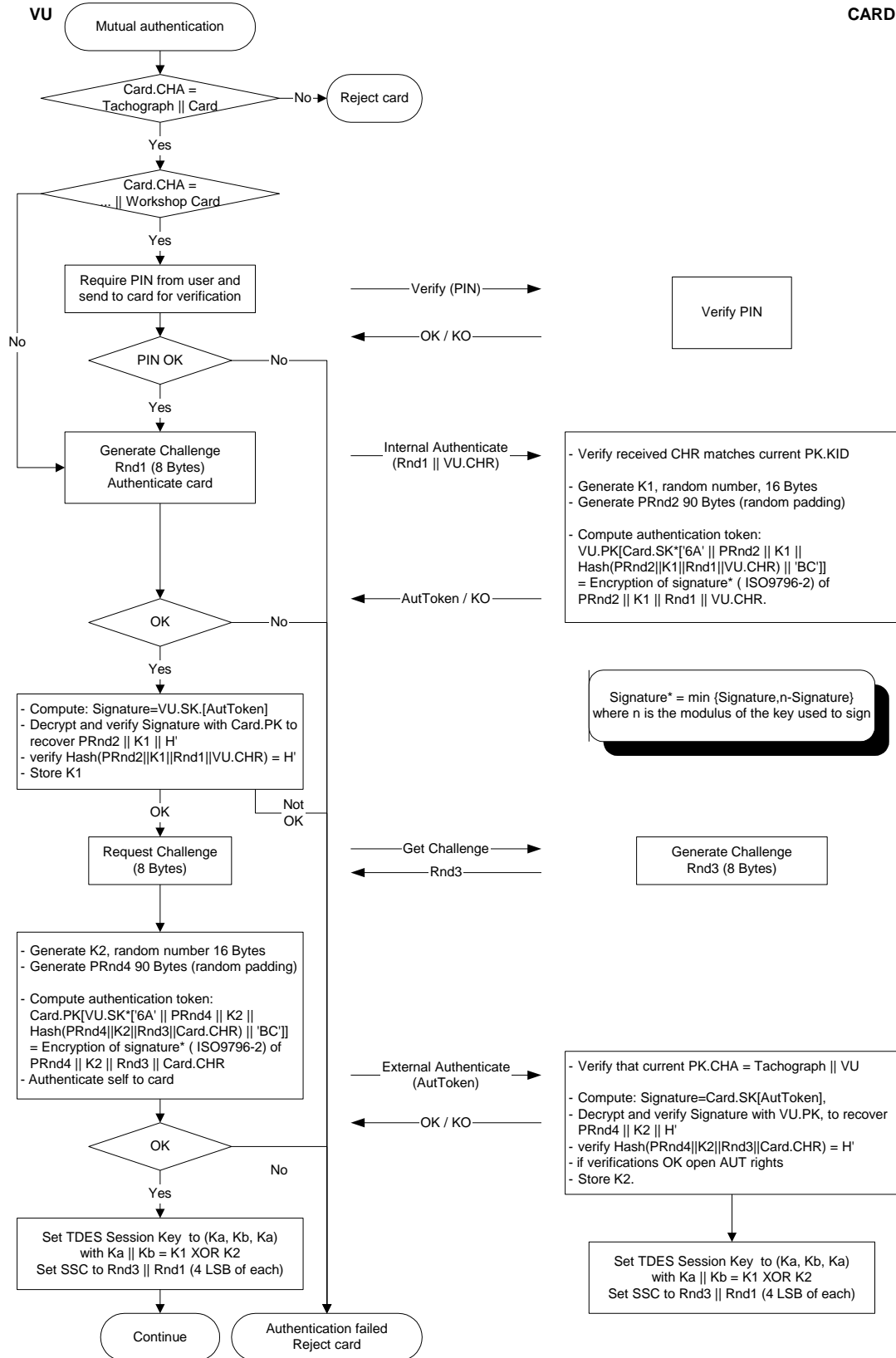
Каждая сторона должна доказать другой наличие у неё действительной пары ключей, открытый ключ которой сертифицирован сертификационным органом государства-члена, имеющим в свою очередь сертификат, выданный европейским сертификационным органом.

Доказательством служит подписание закрытым ключом случайной последовательности цифр, полученной от другой стороны, которая при проверке подписи должна восстановить из неё ту же последовательность цифр.

Данный механизм запускается со стороны 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 2)):





## 5. Механизмы обеспечения конфиденциальности, целостности и аутентификации данных при их передаче между БУ и карточками

### 5.1. Защищённый обмен сообщениями

CSM\_021 Целостность данных, передаваемых между БУ и карточками, обеспечивается благодаря криптозащите сообщений в соответствии с цитируемыми источниками [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', причём все эти объекты данных при их формировании снабжаются метками, где 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 защищённом обмене сообщениями команды и ответы имеют структуру, показанную ниже.

Используемые здесь объекты данных представляют собой часть набора ОД для защищённого обмена сообщениями, описание которого приводится в ISO/IEC 7816-4:

Метка	Мнемоника	Значение
'81'	T <sub>PV</sub>	Простое значение: данные без кодировки BER-TLV (защищаются с помощью CC)
'97'	T <sub>LE</sub>	Значение Le в незащищённой команде (защищается с помощью CC)
'99'	T <sub>SW</sub>	Информация о статусе (защищается с помощью CC)
'8E'	T <sub>CC</sub>	Криптографическая контрольная сумма
'87'	T <sub>PICG</sub>	Байт индикации заполнения    Криптограмма (Простое значение без кодировки BER-TLV)

Если незащищённая пара команды и ответа выглядит следующим образом:

Заголовок команды				Основная часть команды		
CLA	INS	P1	P2	[поле L <sub>c</sub> ]	[Поле данных]	[поле L <sub>c</sub> ]
четыре байта				Байты L, обозначаемые как V <sub>1</sub> -V <sub>L</sub>		

Основная часть ответа	Концевая метка ответа
[Поле данных] Байты данных L <sub>r</sub>	SW1 SW2 два байта

соответствующая ей защищённая пара команды и ответа имеет следующий вид:

Защищённая команда:

Заголовок команды (CH)				Основная часть команды										
CLA	INS	P1	P2	[Новое поле L <sub>c</sub> ]	[Новое поле данных]						[Новое поле L <sub>c</sub> ]			
'0C'				Длина Новое поле данных	T <sub>PV</sub>	L <sub>PV</sub>	PV	T <sub>LE</sub>	L <sub>LE</sub>	L <sub>e</sub>	T <sub>CC</sub>	L <sub>CC</sub>	CC	'00'
					'81'	L <sub>c</sub>	Поле е дан ных	'97'	'01'	L <sub>e</sub>	'8E'	'04'	CC	

Данные, которые должны быть включены в контрольную сумму = CH || PB || T<sub>PV</sub> || L<sub>PV</sub> || PV || T<sub>LE</sub> || L<sub>LE</sub> || L<sub>e</sub> || PB

PB = байты заполнения (80 .. 00) согласно стандартам ISO-IEC 7816-4 и ISO 9797 (метод 2).

Объекты данных PV и LE присутствуют лишь в случаях, когда незащищённая команда содержит соответствующие данные.

Защищённый ответ:

1. Если поле данных ответа не является пустым, но не нуждается в защите конфиденциальности:

Основная часть ответа						Концевая метка ответа	
[Новое поле данных]						Новые SW1 SW2	
T <sub>PV</sub>	L <sub>PV</sub>	PV	T <sub>CC</sub>	L <sub>CC</sub>	CC		
'81'	L <sub>r</sub>	Поле данн ых	'8E'	'04'	CC		

Данные, которые должны быть включены в контрольную сумму = T<sub>PV</sub> || L<sub>PV</sub> || PV || PB

2. Если поле данных ответа не является пустым и нуждается в защите конфиденциальности:

Основная часть ответа						Концевая метка ответа	
[Новое поле данных]						Новые SW1 SW2	
T <sub>PI CG</sub>	L <sub>PI CG</sub>	PI CG	T <sub>CC</sub>	L <sub>CC</sub>	CC		
'87'		PI    CG	'8E'	'04'	CC		

Информация, передаваемая в виде криптограммы: данные без кодировки BER-TLV и заполняющие байты.

Данные, которые должны быть включены в контрольную сумму = T<sub>PI CG</sub> || L<sub>PI CG</sub> || PI CG || PB

3. Если поле данных ответа пустое:

Основная часть ответа						Концевая метка ответа	
[Новое поле данных]						Новые SW1 SW2	
T <sub>SW</sub>	L <sub>SW</sub>	SW	T <sub>CC</sub>	L <sub>CC</sub>	CC		
'99'	'02'	Новые SW1 SW2	'8E'	'04'	CC		

Данные, которые должны быть включены в контрольную сумму = T<sub>SW</sub> || L<sub>SW</sub> || SW || PB

## 5.2. Обработка ошибок при защищённом обмене сообщениями

CSM\_026 Когда карточка тахографа обнаруживает ошибку SM при расшифровке команды, она возвращает соответствующие байты статуса, не используя SM. В соответствии со стандартом ISO/IEC 7816-4 для указания на ошибки SM предусматриваются следующие байты статуса:

'66 88': Несоответствие криптографической контрольной суммы,

- '69 87': Отсутствие предусмотренных объектов данных SM,  
 '69 88': Неверные объекты данных SM.

CSM\_027 Если карточкой тахографа возвращены байты статуса без ОД SM или с неверным ОД SM, БУ должно прервать сеанс обмена данными.

### 5.3. Алгоритм расчёта 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  $E(K_a, SSC)$ .
- Последующий этап: контрольные блоки  $y_1, \dots, y_n$  рассчитываются при помощи  $K_a$ .
- Заключительный этап: по последнему контрольному блоку  $y_n$  рассчитывается криптографическая контрольная сумма:  $E(K_a, D(K_b, y_n))$ .

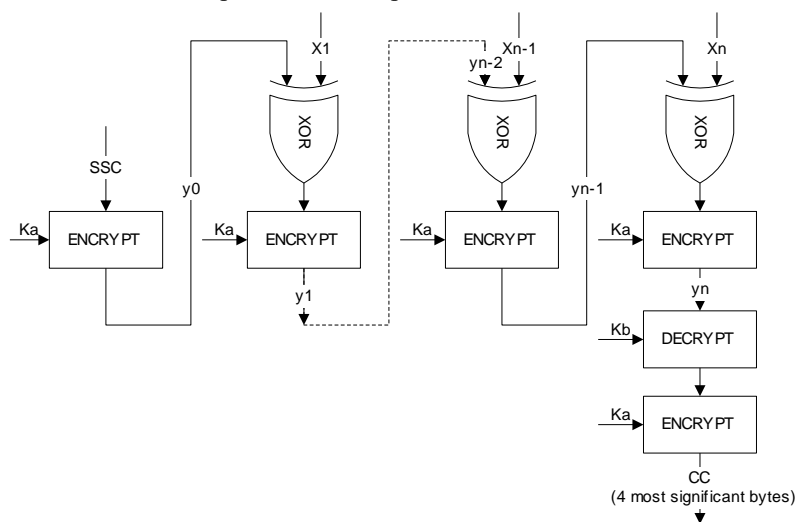
где  $E()$  означает шифрование по системе DES, а  $D()$  – расшифровку по системе DES.

Передаче подлежат четыре старших байта криптографической контрольной суммы.

CSM\_029 Счётчик исходящих сообщений (SSC) запускается во время процедуры согласования ключа:  
 Исходный SSC : Rnd3 (4 наименее значимых байта) || Rnd1 (4 наименее значимых байта).

CSM\_030 Счётчик исходящих сообщений увеличивается на 1 единицу перед каждым вычислением MAC (т.е. для первой команды значение SSC составляет исходный SSC + 1, а для первого ответа – исходный SSC + 2).

Способ вычисления retail-MAC изображен на диаграмме ниже:

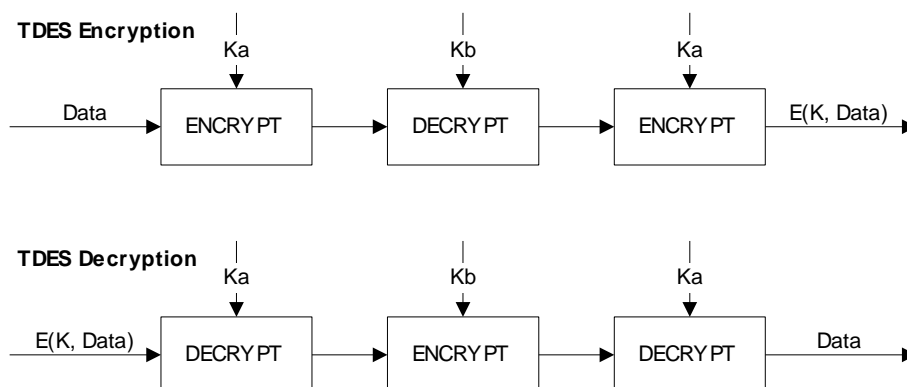




## 5.4. Алгоритм расчёта криптограмм для защиты конфиденциальности ОД

CSM\_031 Криптограммы рассчитываются с помощью алгоритма TDEA в режиме TCBC, как указано в цитируемых источниках [TDES] и [TDES-OP], причём в качестве блока начальной величины используется нуль-вектор.

Применение ключей TDES изображён на диаграмме ниже:



## 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. Данный файл должен содержать сертификаты MS<sub>i</sub>.С и EQT.С. Файл содержит цифровые подписи блоков данных в соответствии с указанными в приложении 7 (Протоколы загрузки данных).

CSM\_033 Цифровые подписи загружаемых данных создаются по схеме, предполагающей добавление информации, которая позволяет при желании производить считывание 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:

$$\text{Подпись} = \text{EQT.SK}[\text{'00' || '01' || PS || '00' || DER(SHA-1(данные))}]$$

*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.

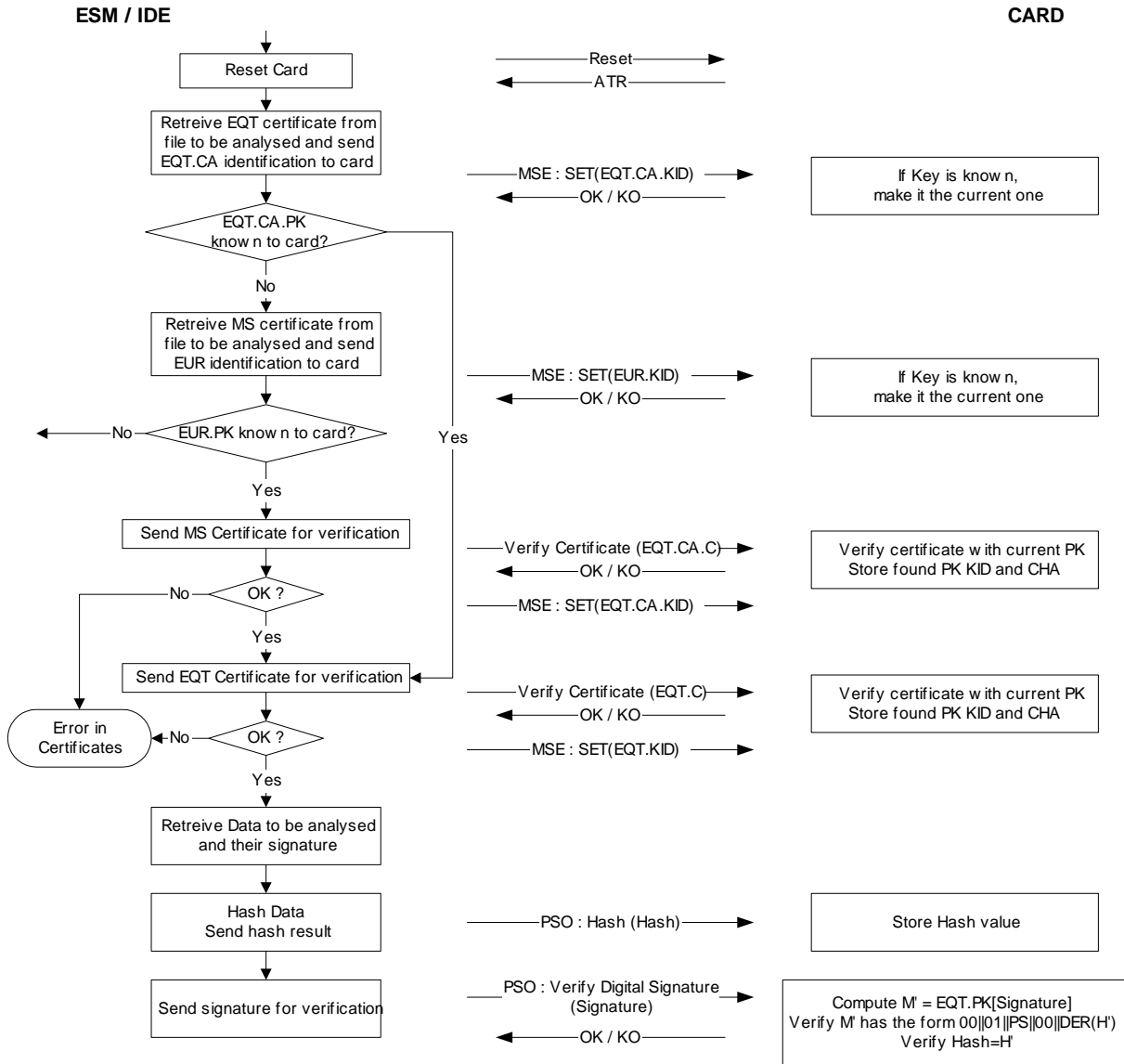
### 6.2. Проверка подписей

CSM\_035 Подписи загружаемых данных проверяются по схеме подписи с соответствующим добавлением, которая определена в цитируемом источнике [PKCS1], при помощи хеш-функции SHA-1.

Проверяющей стороне должен быть известен европейский 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 неё карточки контролёра может проверять целостность загруженных данных, сохранённых на ВН (внешнем носителе). Для расшифровки цифровых подписей используется карточка контролёра. 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 Б. СИСТЕМА ТАХОГРАФОВ ВТОРОГО ПОКОЛЕНИЯ

### 7. Введение

#### 7.1. Ссылки

В этой части настоящего приложения используются следующие источники:

AES	Национальный институт стандартов и технологий (NIST), FIPS PUB 197: Расширенный стандарт шифрования (AES), 26 ноября 2001 г.
DSS	Национальный институт стандартов и технологий (NIST), FIPS PUB 186-4: Стандарт цифровой подписи (DSS), июль 2013 г.
ISO 7816-4	ISO/IEC 7816-4, Идентификационные карточки – карточки с интегральными микросхемами. Часть 4: организация, безопасность и команды обмена. 3-е издание. 15 апреля 2013 г.
ISO 7816-4	ISO/IEC 7816-4, Идентификационные карточки – карточки с интегральными микросхемами. Часть 8: команды операций по обеспечению безопасности. 2-е издание. 1 июня 2004 г.
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 г.
ISO 9797-1	ISO/IEC 9797-1, Информационные технологии. Техники обеспечения безопасности. Коды аутентификации сообщений (MAC). Часть 1: механизмы шифрования блоками. 2-е издание, 1 марта 2011 г.
ISO 10116	ISO/IEC 10116, Информационные технологии. Техника обеспечения безопасности. Режимы работы блока шифрования $n$ -бит. 3-е издание, 1 февраля 2006 г.
ISO 16844-3	ISO/IEC 16844-3, Дорожные транспортные средства. Системы тахографов. Часть 3: интерфейс датчика движения. 1-е издание, 2004 г., включая техническую поправку 1 2006.
RFC 5480	Эллиптическая криптография. Информация об открытом ключе субъекта, март 2009 г.
RFC 5639	Эллиптическая криптография (ECC). Стандартные кривые Brainpool и генерирование кривых, 2010
RFC 5869	Функция формирования ключа извлечения и расширения на базе HMAC (HKDF), май 2010 г.
SHS	Национальный институт стандартов и технологий (NIST), FIPS PUB 180-4: стандарт безопасного хеширования, март 2012 г.
SP 800-38B	Национальный институт стандартов и технологий (NIST), специальный выпуск 800-38B: Рекомендация по режимам работы с шифрованием блоками: режим аутентификации CMAC, 2005

TR-03111 Технические рекомендации BSI TR-03111, эллиптическая криптография, версия 2.00, 28 июня 2012 г.

## 7.2. Условные обозначения и сокращения

В настоящем приложении используются следующие условные обозначения и сокращённые термины:

AES	Расширенный стандарт шифрования
CA	Сертификационный орган
CAR	Указатель сертификационного органа
CBC	Сцепление криптоблоков (режим работы)
CH	Заголовок команды
CHA	Полномочия держателя сертификата
CHR	Указатель держателя сертификата
CV	Постоянный вектор
DER	Особые правила кодирования
DO (ОД)	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	Аппаратура
IDE (СПА)	Специализированная программируемая аппаратура
K <sub>M</sub>	Ключ старшего разряда датчика движения, позволяющий осуществлять соединение бортового устройства с датчиком движения
K <sub>M-VU</sub>	Ключ, вводимый в бортовые устройства, позволяющий БУ генерировать ключ старшего разряда датчика движения, если в БУ вставлена карточка мастерской
K <sub>M-WC</sub>	Ключ, вводимый в карточки мастерской, позволяющий БУ генерировать ключ старшего разряда датчика движения, если в БУ вставлена карточка мастерской
MAC	Код аутентификации сообщений
MoS	Датчик движения
MSB	Самый значимый бит
PKI	Инфраструктура открытых ключей
RCF	Средство удалённой связи
SSC	Счётчик исходящих сообщений
SM	Защищённый обмен сообщениями
TDES	Стандарт тройного шифрования данных
TLV	Значение длины метки
VU (БУ)	Бортовое устройство
X.C	Сертификат открытого ключа пользователя X
X.CA	Сертификационный орган, выдавший сертификат пользователю X
X.CAR	Указатель сертификационного органа, указанного в сертификате пользователя X
X.CHR	Указатель держателя сертификата, указанного в сертификате пользователя X
X.PK	Открытый ключ пользователя X
X.SK	Закрытый ключ пользователя X
X.PK <sub>eph</sub>	Кратковременный открытый ключ пользователя X
X.SK <sub>eph</sub>	Кратковременный закрытый ключ пользователя X
'xx'	Шестнадцатеричное значение
	оператор конкатенации

### 7.3. Определения

Определения терминов, употребляемых в настоящем приложении, даны в разделе I дополнения 1С.

## 8. Криптографические системы и алгоритмы

### 8.1. Криптографические системы

- TCS\_180 В бортовых устройствах и карточках тахографа применяется вариант криптосистемы на основе эллиптической кривой с открытым ключом для решения следующих задач защиты:
- взаимная аутентификация бортовых устройств и карточек,
  - согласование сеансовых ключей AES между бортовыми устройствами и карточками,
  - обеспечение подлинности, целостности и неподдельности данных, загружаемых с бортовых устройств или карточек тахографа на внешние носители.
- TCS\_181 В бортовых устройствах и внешних устройствах ГНСС применяется вариант криптосистемы на основе эллиптической кривой с открытым ключом для решения следующих задач защиты:
- соединение бортового устройства и внешнего устройства ГНСС,
  - взаимная аутентификация бортового устройства и внешнего устройства ГНСС,
  - согласование сеансовых ключей AES между бортовыми устройствами и внешними устройствами ГНСС.
- TCS\_182 В бортовых устройствах и карточках тахографа применяется вариант симметричной криптосистемы на основе AES для решения следующих задач защиты:
- обеспечение подлинности и целостности данных, которыми обмениваются бортовое устройство и карточка тахографа,
  - если применимо, обеспечение конфиденциальности данных, которыми обмениваются бортовое устройство и карточка тахографа.
- TCS\_183 В бортовых устройствах и внешних устройствах ГНСС применяется вариант симметричной криптосистемы на основе AES для решения следующих задач защиты:
- обеспечение подлинности и целостности данных, которыми обмениваются бортовое устройство и внешнее устройство ГНСС.
- TCS\_184 В бортовых устройствах и датчиках движения применяется вариант симметричной криптосистемы на основе AES для решения следующих задач защиты:
- соединение бортового устройства и датчика движения,
  - взаимная аутентификация бортовых устройств и датчиков движения,
  - обеспечение конфиденциальности данных, которыми обмениваются бортовое устройство и датчик движения.
- TCS\_185 В бортовых устройствах и контрольных карточках применяется вариант симметричной криптосистемы на основе AES для решения следующих задач защиты, связанных с интерфейсом удалённой связи:
- обеспечение конфиденциальности, подлинности и целостности данных, которые бортовое устройство передаёт на контрольную карточку.

#### Примечания:

- Строго говоря, данные передаются из бортового устройства на удалённое средство контроля под руководством контролёра при помощи средства удалённой связи, которое может внутренним или внешним относительно БУ; см. приложение 14. Однако удалённое средство контроля передаёт данные на контрольную карточку для расшифровки и подтверждения подлинности. С точки зрения защиты средство удалённой связи и удалённое средство контроля полностью транспарентны.

- Карточка мастерской предлагает те же самые функции интерфейса DSRC, что и контрольная карточка. Это позволяет мастерской проверять надлежащее функционирование интерфейса удалённой связи БУ, включая характеристики безопасности. Более подробно см. в разделе 9.2.2.

## 8.2. Криптографические алгоритмы

### 8.2.1 Симметричные алгоритмы

TCS\_186 Бортовые устройства, карточки тахографов, датчики движения и внешние устройства ГНСС поддерживают алгоритм AES, определённый в источнике [AES], с длиной ключей 128, 192 и 256 бит.

### 8.2.2 Асимметричные алгоритмы и стандартизированные параметры области

TCS\_187 Бортовые устройства, карточки тахографов и внешние устройства ГНСС поддерживают эллиптическую криптографию с размером ключей 256, 384 и 512/521 бит.

TCS\_188 Бортовые устройства, карточки тахографов и внешние устройства ГНСС поддерживать алгоритм подписи ECDSA, как описано в источнике [DSS].

TCS\_189 Бортовые устройства, карточки тахографов и внешние устройства ГНСС поддерживают алгоритм согласования ключей ECKA-EG, как указано в источнике [TR 03111].

TCS\_190 Бортовые устройства, карточки тахографов и внешние устройства ГНСС поддерживают все стандартизированные параметры области, указанные ниже в Таблица 43 в отношении эллиптической криптографии.

Название	Размер (биты)	Указатель	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

Таблица 43 Стандартизированные параметры области

Примечание: идентификаторы объектов, перечисленные в последнем столбце Таблица 43, указаны в источнике [RFC 5639] по кривым Brainpool и в источнике [RFC 5480] по кривым NIST.

Пример 1: идентификатор объекта кривой BrainpoolP256r1 – {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 – {iso(1) identified-organization(3) certicom(132) curve(0) 34}.

Или в точечной нотации: 1.3.132.0.34.

### 8.2.3 Алгоритмы хеширования

TCS\_191 Бортовые устройства и карточки тахографов поддерживают алгоритмы SHA-256, SHA-384 и SHA-512, описанные в [SHS].

## 8.2.4 Последовательности шифров

Если симметричный алгоритм, несимметричный алгоритм и/или алгоритм хеширования используются вместе для формирования протокола безопасности, длина их соответствующих ключей и размеры хеш-параметров (примерно) равны. Таблица 44 отображает допустимые последовательности шифров:

ИД последовательности шифров	Размер ключа ECC (биты)	Длина ключа AES (биты)	Алгоритм хеширования	Длина MAC (в байтах)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Таблица 44 Допустимые последовательности шифров

Примечание: Размеры ключей ECC, составляющие 512 бит и 521 бит, считаются равными по силе для выполнения всех задач в рамках настоящего приложения.

## 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 защищённого обмена сообщениями между бортовыми устройствами и карточками тахографов и между бортовыми устройствами и внешними устройствами ГНСС. Данные процессы подробно освещены в главах 10 и 11 настоящего приложения.

В рамках европейской системы «умных» тахографов пары ключей ECC и соответствующие сертификаты генерируются и управляются на трёх функциональных уровнях, образующих иерархию:

- европейский уровень,
- уровень государства-члена,
- аппаратный уровень.

Во всей европейской системе «умных» тахографов открытые и закрытые ключи и сертификаты генерируются, управляются и передаются при помощи стандартизированных защищённых средств.

#### 9.1.2 Европейский уровень

На европейском уровне генерируется единая пара общеевропейских ключей ECC, обозначаемых как EUR. В неё входят закрытый ключ (EUR.SK) и открытый ключ (EUR.PK). Данная пара ключей формирует пару корневых ключей для PKI всей европейской системы «умных» тахографов. Эту задачу выполняет европейский сертификационный орган (ERCA) под руководством и при ответственности Европейской комиссии.

ERCA использует европейский закрытый ключ для подписания (самоподписывающегося) корневого сертификата европейского открытого ключа и передаёт этот европейский корневой сертификат всем государствам-членам.

ERCA использует европейский закрытый ключ для подписания сертификатов открытых ключей государств-членов по запросу. ERCA ведёт записи всех подписанных сертификатов открытых ключей государств-членов.

- TCS\_198 Как показано на Рисунок 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 создаёт новый самоподписывающийся корневой сертификат для нового европейского 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 9.2.1.2 и 9.2.2.2.
- TCS\_199 До генерирования новой пары европейских корневых ключей ERCA проводит анализ криптографической силы, необходимой для новой пары ключей, учитывая, что она должна быть защищена на протяжении следующих 34 лет. При необходимости ERCA переходит на последовательность шифров мощнее текущей, как указано в TCS\_192.
- TCS\_200 Когда ERCA генерирует новую пару европейских корневых ключей, он создаёт связующий сертификат для нового европейского открытого ключа и подписывает его старым европейским закрытым ключом. Срок действия такого сертификата составляет 17 лет. Данный процесс также показан на Рисунок 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 предлагает аппаратуре поколения X-1 средство доверия аппаратуре поколения X.
- TCS\_201 С момента вступления в силу нового сертификата корневого ключа ERCA больше не использует закрытый ключ пары корневых ключей ни для каких целей.
- TCS\_202 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 всё ещё действительны
  - Связующие сертификаты для всех поколений сертификатов EUR, кроме первого
- 9.1.3 Уровень государства-члена**
- TCS\_203 На уровне государств-членов все государства, необходимы для подписания сертификатов карточек тахографов, генерируют одну или несколько уникальных пар ключей ECC, обозначаемых как MSCA\_Card. Все государства-члены, необходимые для подписания сертификатов для бортовых устройств или внешних устройств ГНСС, также генерируют одну или несколько уникальных пар ключей ECC, обозначаемых как MSCA\_VU-EGF.
- TCS\_204 Задачу генерирования пар ключей государств-членов выполняет сертификационный орган государства-члена (MSCA). Когда MSCA генерирует пару ключей государства-члена, он передаёт открытый ключ ERCA, чтобы получить соответствующий сертификат государства-члена, подписанный ERCA.
- TCS\_205 MSCA выбирает силу пары ключей государства-члена, которая была бы равна силе пары европейских корневых ключей, используемых для подписания соответствующего сертификата государства-члена.
- TCS\_206 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.
- TCS\_207 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 тахографов.



- TCS\_208 MSCA ведёт учёт всех подписанных сертификатов БУ, внешних устройств ГНСС и карточек вместе с идентификационными данными оборудования, для которого предназначен каждый сертификат.
- TCS\_209 Срок действия сертификата MSCA\_VU-EGF составляет 17 лет и 3 месяца. Срок действия сертификата MSCA\_Card составляет 7 лет и 1 месяц.
- TCS\_210 Как показано на Рисунок 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.
- TCS\_211 С момента окончания периода применения MSCA больше не использует закрытый ключ пары ключей MSCA\_VU-EGF ни для каких целей. С момента окончания периода применения MSCA также больше ни для каких целей не использует закрытый ключ пары ключей MSCA\_Card.
- TCS\_212 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 всё ещё действительны
  - Текущий сертификат EUR, необходимый для проверки текущего сертификата MSCA
  - Все прежние сертификаты EUR, необходимые для проверки сертификатов MSCA, которые всё ещё действительны
- TCS\_213 Если MSCA должен подписывать сертификаты бортовых устройств или внешних устройств ГНСС, 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 всё ещё действительны

#### 9.1.4 Аппаратный уровень: бортовые устройства

- TCS\_214 Для каждого бортового устройства генерируются две уникальные пары ключей ECC, обозначаемые как VU\_MA и VU\_Sign. Эту задачу выполняют производители БУ. При генерировании пары ключей БУ сторона, генерирующая ключ, передаёт открытый ключ MSCA страны, в которой она проживает, чтобы получить соответствующий сертификат БУ, подписанный MSCA. Закрытый ключ использует только бортовое устройство.
- TCS\_215 У сертификатов VU\_MA и VU\_Sign определённого бортового устройства одна и та же дата срока действия сертификата.
- TCS\_216 Производитель БУ выбирает силу пары ключей БУ, которая была бы равна силе пары ключей MSCA, используемых для подписания соответствующего сертификата БУ.
- TCS\_217 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.
- TCS\_218 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 разделах 10.4 и 11.4 настоящего приложения.
- TCS\_219 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. Соответствующий открытый ключ VU\_Sign.PK используется исключительно для проверки подписей, созданных бортовым устройством.

TCS\_220 Как показано на Рисунок 1 в разделе 9.1.7, срок действия сертификата VU\_MA составляет 15 лет и 3 месяца. Срок действия сертификата VU\_Sign также составляет 15 лет и 3 месяца. The validity period of a VU\_Sign certificate shall also be 15 years and 3 months.

Примечания:

- Продлённый срок действия сертификата VU\_Sign позволяет бортовому устройству создавать действительные подписи через загружаемые данные в течение первых трёх месяцев после его истечения, как требуется в Регламенте (ЕС) № 581/2010.
- Продлённый срок действия сертификата VU\_MA нужен для аутентификации БУ относительно контрольной карточки или карточки предприятия в течение первых трёх месяцев после его истечения, чтобы можно было загрузить данные.

TCS\_221 С момент истечения срока действия соответствующего сертификата бортовое устройство не использует закрытый ключ пары ключей БУ ни для каких целей.

TCS\_222 После начала эксплуатации бортового устройства пары ключей БУ (кроме кратковременных пар ключей) и соответствующие сертификаты данного бортового устройства на месте не заменяются.

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 защищённой среде, контролируемой производителем БУ.

TCS\_223 После ввода в эксплуатацию бортовые устройства содержат следующие криптографические ключи и сертификаты:

- Закрытый ключ VU\_MA и соответствующий сертификат
- Закрытый ключ VU\_Sign и соответствующий сертификат
- Сертификат MSCA\_VU-EGF, содержащий открытый ключ MSCA\_VU-EGF.ПК для проверки сертификата VU\_MA и сертификата VU\_Sign
- Сертификат EUR, содержащий открытый ключ EUR.ПК, 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

TCS\_224 Помимо криптографических ключей и сертификатов, перечисленных в TCS\_223, в бортовых устройствах также есть ключи и сертификаты, указанные в части А настоящего приложения, позволяющие бортовому устройству вступать во взаимодействие с карточками тахографов первого поколения.

### 9.1.5 Аппаратный уровень: карточки тахографа

TCS\_225 Для каждой карточки тахографа генерируется одна уникальная пара ключей ECC, обозначаемая как Card\_MA. Для каждой карточки водителя и каждой карточки мастерской также дополнительно генерируется пара ключей ECC, обозначаемая как Card\_Sign. Эту задачу могут выполнять производители или персонализаторы карточек. При генерировании пары ключей карточки сторона, генерирующая ключ, передаёт открытый ключ MSCA страны, в которой она проживает, чтобы получить соответствующий сертификат карточки, подписанный MSCA. Закрытый ключ использует только карточка тахографа.

TCS\_226 У сертификатов Card\_MA и Card\_Sign определённой карточки водителя или мастерской одна и та же дата срока действия сертификата.

TCS\_227 Производитель или персонализатор карточки выбирает силу пары ключей карточки, которая была бы равна силе пары ключей MSCA, используемых для подписания соответствующего сертификата карточки.

- TCS\_228 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 сеансовых ключей относительно бортовых устройств, как указано в разделах 10.3 и 10.4 настоящего приложения.
- TCS\_229 Карточка водителя или мастерской использует закрытый ключ Card\_Sign.SK своей пары ключей Card\_Sign исключительно для загрузки файлов данных, как указано в главе 14 настоящего приложения. Соответствующий открытый ключ Card\_Sign.PK используется исключительно для проверки подписей, созданных карточкой.
- TCS\_230 Срок действия сертификата Card\_MA таков:
- Карточки водителя: 5 лет
  - Карточки предприятия: 2 года
  - Контрольные карточки: 2 года
  - Карточки мастерской: 1 год
- TCS\_231 Срок действия сертификата Card\_Sign таков:
- Карточки водителя: 5 лет и 1 месяц
  - Карточки мастерской: 1 год и 1 месяц
- Примечание: продлённый срок действия сертификата Card\_Sign позволяет карточке водителя создавать действительные подписи через загружаемые данные 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.
- TCS\_232 После выпуска карточки пары ключей и соответствующие сертификаты данной карточки тахографа не меняются или не возобновляются.
- TCS\_233 После выпуска карточки тахографа содержат следующие криптографические ключи и сертификаты:
- Закрытый 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, соединяющий эти два сертификата EUR, если таковые существуют
- TCS\_234 Помимо криптографических ключей и сертификатов, перечисленных в TCS\_233, на карточках тахографа также есть ключи и сертификаты, указанные в части А настоящего приложения, позволяющие таким карточкам вступать во взаимодействие с бортовыми устройствами первого поколения.

### 9.1.6 Аппаратный уровень: внешние устройства ГНСС

- TCS\_235 Для каждого внешнего устройства ГНСС генерируется одна уникальная пара ключей EGF, обозначаемая как EGF\_MA. Эту задачу выполняют производители внешних устройств ГНСС. При генерировании пары ключей EGF\_MA открытый ключ передаётся MSCA страны проживания, чтобы получить соответствующий сертификат EGF\_MA, подписанный MSCA. Закрытый ключ использует только внешнее устройство ГНСС.
- TCS\_236 Производитель EGF выбирает силу пары ключей EGF\_MA, которая была бы равна силе пары ключей MSCA, используемых для подписания соответствующего сертификата EGF\_MA.

TCS\_237 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 сеансовых ключей относительно бортовых устройств, как указано в разделах 11.4 и 11.4 настоящего приложения.

TCS\_238 Срок действия сертификата EGF\_MA составляет 15 лет.

TCS\_239 С момент истечения 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 использовать свой закрытый ключ для взаимной аутентификации относительно БУ, с которым оно уже соединено, даже после истечения срока действия соответствующего сертификата.

TCS\_240 После начала эксплуатации EGF пара ключей EGF\_MA и соответствующий сертификат данного внешнего устройства ГНСС на месте не заменяются или не возобновляются.

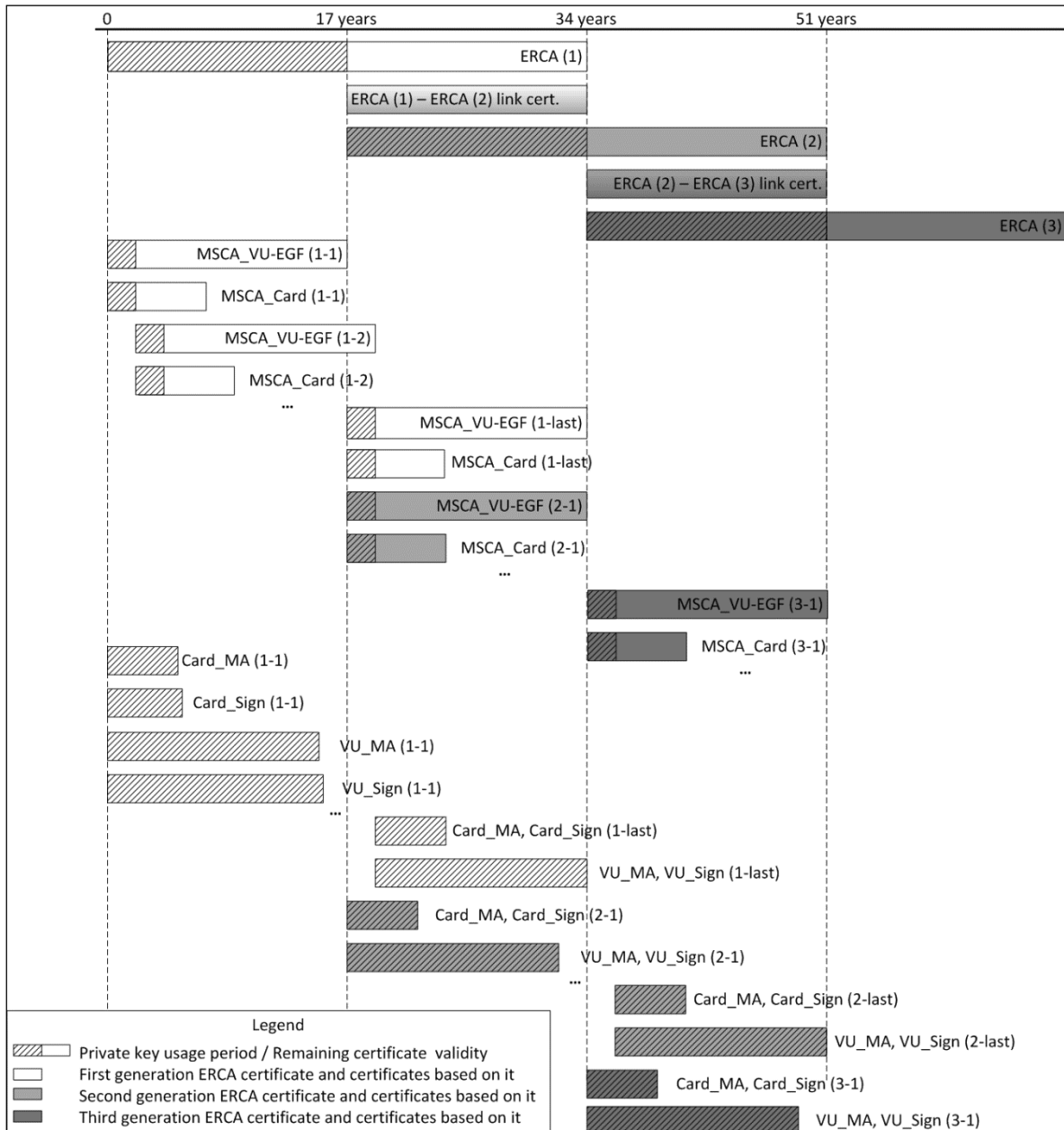
Примечание: Данное требование не исключает возможности замены статичных пар ключей EGF во время реконструкции или ремонта в защищённой среде, контролируемой производителем EGF.

TCS\_241 После ввода в эксплуатацию внешнее устройство ГНСС содержит следующие криптографические ключи и сертификаты:

- Закрытый ключ 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

### **9.1.7 Обзор: замена сертификата**

На Рисунок 1 ниже показано, как выпускаются и с течением времени используются корневые сертификаты ERCA различных поколений, связующие сертификаты ERCA, сертификаты MSCA и сертификаты оборудования (БУ и карточки):



**Рисунок 1** Выпуск и использование корневых сертификатов ERCA различных поколений, связующих сертификатов ERCA, сертификатов MSCA и сертификатов оборудования

Примечания к Рисунок 1:

1. Разные поколения корневого сертификата обозначены цифрой в скобках. Например, ERCA (1) означает корневой сертификат ERCA первого поколения; ERCA (2) – сертификат второго поколения и т.д.
2. Другие сертификаты помечаются двумя цифрами в скобках, первая из которых указывает на поколение выпуска корневого сертификата, а вторая – на поколение самого сертификата. Например, MSCA\_Card (1-1) – это первый сертификат MSCA\_Card, выпущенный в рамках ERCA (1); MSCA\_Card (2-1) – первый сертификат MSCA\_Card, выпущенный в рамках ERCA (2); MSCA\_Card (2-last) – последний сертификат MSCA\_Card, выпущенный в рамках ERCA (2);

- Card\_MA(2-1) – первый сертификат карточки для взаимной аутентификации, выпущенный в рамках ERCA (2), и т.д.
3. Сертификаты MSCA\_Card (2-1) и MSCA\_Card (1-last) выпускаются почти в тот же день, но не совсем. MSCA\_Card (2-1) – первый сертификат MSCA\_Card, выпускаемый в рамках ERCA (2), будет выпущен немного позднее, чем MSCA\_Card (1-last), последний сертификат MSCA\_Card, выпускаемый в рамках ERCA (1).
  4. Как показано на рисунке, первые сертификаты БУ и карточки, выпускаемые в рамках ERCA (2), появятся почти за два года до последних сертификатов БУ и карточки, выпускаемых в рамках ERCA (1). Это связано с тем, что сертификаты БУ и карточки выпускаются по сертификату MSCA, а не непосредственно по сертификату ERCA. Сертификат MSCA (2-1) выдаётся непосредственно после вступления в силу ERCA (2), а сертификат MSCA (1-last) выдаётся лишь незадолго до того времени, в последний момент, когда сертификат ERCA (1) ещё действителен. 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 отношении первого поколения.

## 9.2. Симметричные ключи

### 9.2.1 Ключи для обеспечения связи между БУ и датчиком движения

#### 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 между БУ и датчиком движения подробно описан в главе 12 настоящего приложения.

Для 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 Таблица 45. Все эти ключи – ключи AES, длина которых равна длине ключа старшего порядка датчиков движения, связанного с длиной (планируемой) пары европейских корневых ключей, как описано в TCS\_192.

Ключ	Символ	Кем/чем генерируется	Метод генерирования	Где хранится
Ключ старшего порядка датчика движения – часть БУ	$K_{M-VU}$	ERCA	Случайный	ERCA, MSCA, участвующие в выпуске сертификатов БУ, производители БУ, бортовые устройства
Ключ старшего порядка датчика движения – часть мастерской	$K_{M-WC}$	ERCA	Случайный	ERCA, MSCA, производители карточек, карточки мастерской
Ключ старшего порядка	$K_M$	Самостоятельно не генерируется	Вычисляется как $K_M = K_{M-VU} \text{ XOR } K_{M-WC}$	ERCA, MSCA, участвующие в выдаче ключей датчиков

датчика движения				движения (факультативно)*
Идентификационный ключ	$K_{ID}$	Самостоятельно не генерируется	Вычисляется как $K_{ID} = K_M \text{ XOR } CV$ ( $CV$ описывается в TCS_248)	ERCA, MSCA, участвующие в выдаче ключей датчиков движения (факультативно)*
Ключ соединения	$K_P$	Производитель датчика движения	Случайный	Один датчик движения
Сеансовый ключ	$K_S$	БУ (во время соединения БУ и датчика движения)	Случайный	Одно БУ и один датчик движения

Таблица 45 Ключи для обеспечения связи бортового устройства и датчика движения

\*Хранение  $K_M$  и  $K_{ID}$  факультативно, так как эти ключи можно извлечь из  $K_{M-VU}$ ,  $K_{M-WS}$  и  $CV$ .

TCS\_243 Европейский сертификационный орган (ERCA) генерирует  $K_{M-VU}$  и  $K_{M-WS}$ , два случайных и уникальных ключей AES, по которым ключ старшего порядка датчика движения  $K_M$  можно вычислить как  $K_{M-VU} \text{ XOR } K_{M-WS}$ . ERCA передаёт  $K_M$ ,  $K_{M-VU}$  и  $K_{M-WS}$  сертификационным органам государств-членов по их просьбе.

TCS\_244 Каждому ключу старшего порядка датчика движения  $K_M$  ERCA присваивает уникальный номер версии, который также используется для составления ключей  $K_{M-VU}$  и  $K_{M-WS}$  и для связанного с ними идентификационного ключа  $K_{ID}$ . ERCA сообщает MSCA о номере версии, когда отправляет им  $K_{M-VU}$  и  $K_{M-WS}$ .

Примечание: Номер версии используется для различия разных поколений этих ключей, как подробно поясняется в разделе 9.2.1.2.

TCS\_245 Сертификационный орган государства-члена передаёт  $K_{M-VU}$  вместе с номером его версии производителям бортового устройства по их просьбе. Производители БУ включают  $K_{M-VU}$  и номер его версии во все изготавливаемые БУ.

TCS\_246 Сертификационный орган государства-члена заботится о том, чтобы  $K_{M-WS}$  вместе с номером его версии был включён в каждую карточку мастерской, выдаваемую в сфере его ответственности.

Примечания:

- См. описание типа данных `SensorInstallationSecData` в приложении 2.
- Как поясняется в разделе 9.2.1.2, на одну карточку мастерской фактически может быть необходимо поместить несколько поколений  $K_{M-WS}$ .

TCS\_247 Помимо ключа AES, указанного в TCS\_246, MSCA заботится о том, чтобы ключ TDES  $K_{M-WS}$ , указанный в требовании CSM\_037 в части А настоящего приложения, был помещён на каждую карточку мастерской, выдаваемую в сфере его ответственности.

Примечания:

- Это позволяет использовать карточку мастерской второго поколения для соединения БУ первого поколения.
- На карточке мастерской второго поколения содержатся два разных приложения, одно из которых соответствует части Б настоящего приложения, а второе – части А. Последнее хранит в себе ключ TDES  $K_{M-WS}$ .

- TCS\_248 MSCA, участвующий в выпуске датчиков движения, извлекает идентификационный ключ из ключа старшего порядка датчика движения при помощи XOR и постоянного вектора CV. Значение CV:
- В случае 128-битных ключей старшего порядка датчика движения: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 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  $\pi$  = '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)

- TCS\_249 Производители датчиков движения генерируют случайный и уникальный ключ соединения  $K_P$  для каждого датчика движения и передают все ключи соединения сертификационному органу государства-члена. MSCA шифрует каждый ключ соединения отдельно с ключом старшего порядка датчика движения  $K_M$  и возвращает зашифрованный ключ производителю датчика движения. В отношении каждого зашифрованного ключа MSCA сообщает производителю датчиков движения номер версии соответствующего  $K_M$ .

Примечание: как поясняется в разделе 9.2.1.2, производитель датчиков движения фактически может быть вынужден генерировать множество уникальных ключей соединения для одного датчика движения.

- TCS\_250 Производители датчиков движения генерируют уникальный серийный номер для каждого датчика движения и передают все серийные номера сертификационному органу государства-члена. MSCA шифрует каждый серийный номер отдельно с идентификационным ключом  $K_{ID}$  и возвращает зашифрованный серийный номер производителю датчика движения. В отношении каждого зашифрованного серийного номера MSCA сообщает производителю датчиков движения номер версии соответствующего  $K_{ID}$ .

- TCS\_251 Что касается требований TCS\_249 и TCS\_250, MSCA использует алгоритм AES в режиме сцепления криптоблоков, как описано [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, описанный в [ISO 9797-1].

- TCS\_252 Производитель датчиков движения хранит зашифрованный ключ соединения и зашифрованный серийный номер на соответствующем датчике движения, вместе с соответствующими значениями в формате простого текста и номером версии  $K_M$  и  $K_{ID}$ , используемых для шифрования.

Примечание: как поясняется в разделе 9.2.1.2, производитель датчиков движения фактически может быть вынужден включить множество зашифрованных ключей соединения и множество зашифрованных серийных номеров в один датчик движения.

- TCS\_253 Помимо криптографического материала на базе AES, как описано в TCS\_252, производитель датчиков движения в каждом датчике движения может также хранить криптографический материал на базе TDES, как указано в требовании CSM\_037 в части А настоящего приложения.

Примечание: таким образом датчик движения второго поколения можно будет соединить с БУ первого поколения.

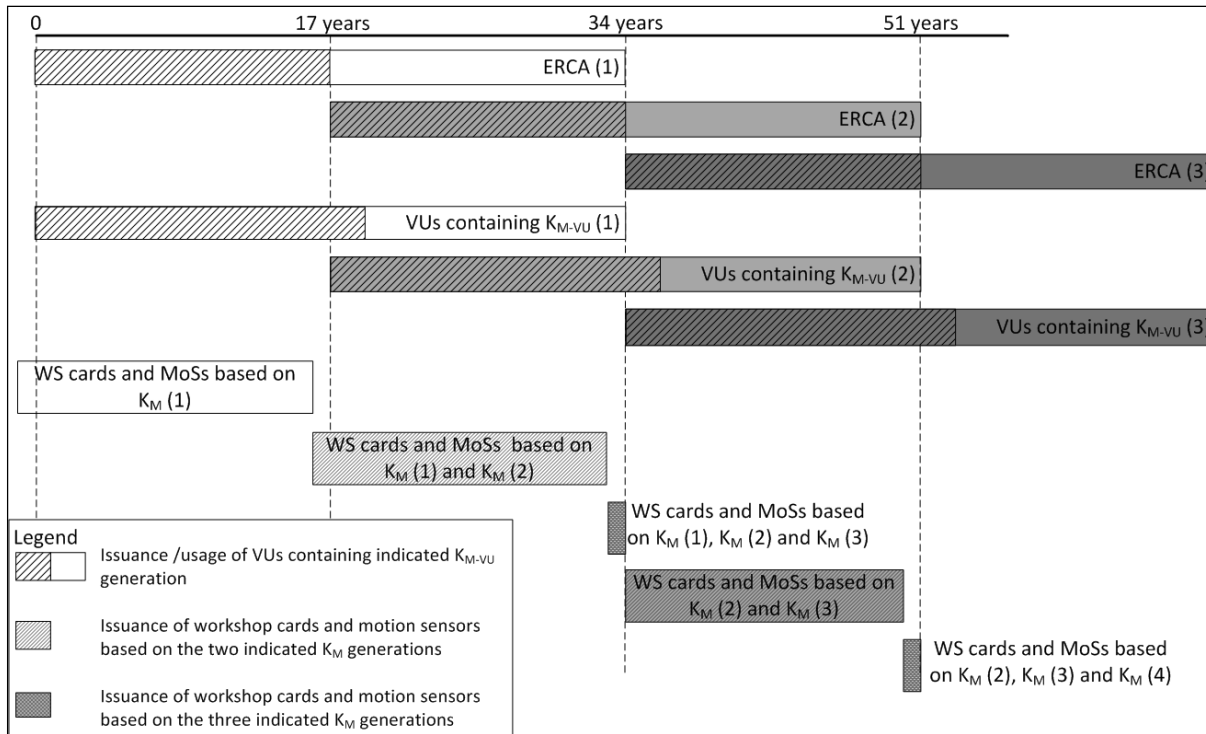
- TCS\_254 Длина сеансового ключа  $K_S$ , генерируемого БУ во время подсоединения к датчику движения, связана с длиной его  $K_{M-VU}$ , как описано в TCS\_192.



### 9.2.1.2 Замена ключа старшего порядка датчика движения в оборудовании второго поколения

TCS\_255

Каждый ключ старшего порядка датчика движения и все соответствующие ключи (см. Таблица 45) связаны с определённым поколением пары корневых ключей ERCA. Так, эти ключи заменяются каждые 17 лет. Срок действия каждого поколения ключей старшего порядка датчиков движения начинается за год до вступления в силу соответствующей пары корневых ключей ERCA и кончается, когда истекает срок действия соответствующей пары корневых ключей ERCA. Это показано на Рисунок 2.



**Рисунок 2** Выпуск и использование разных поколений ключей старшего порядка датчиков движения в бортовых устройствах, датчиках движения и на карточках мастерской

TCS\_256

По крайней мере, за один год до генерирования новой пары европейских корневых ключей, как описано в TCS\_198, ERCA генерирует новый ключ старшего порядка датчика движения  $K_M$  посредством генерирования новых  $K_{M-VU}$  и  $K_{M-WS}$ . Длина ключа старшего порядка датчика движения связана с установленным уровнем силы новой пары европейских корневых ключей, в соответствии с TCS\_192. ERCA передаёт новые  $K_M$ ,  $K_{M-VU}$  и  $K_{M-WS}$  MSCA по его просьбе вместе с номером версии.

TCS\_257

MSCA заботится о том, чтобы все действительные поколения  $K_{M-WS}$  хранились на каждой карточке мастерской, выпущенной в сфере его ответственности, вместе с номерами их версий, как показано на Рисунок 2.

Примечание: это значит, что в последний год срока действия сертификата ERCA карточки мастерской выдаются с  $K_{M-WS}$  трёх разных поколений, как показано на Рисунок 2.

TCS\_258 Что касается процесса, описанного выше в TCS\_249 и TCS\_250: MSCA шифрует каждый ключ соединения  $K_P$ , который он получает от производителя датчиков движения, отдельно для каждого действительного поколения ключа старшего порядка датчика движения  $K_M$ . MSCA также шифрует каждый серийный номер, который он получает от производителя датчиков движения, отдельно для каждого действительного поколения идентификационного ключа  $K_ID$ . Производитель датчиков движения хранит все версии зашифрованного ключа соединения и все версии зашифрованного серийного номера на соответствующем датчике движения, вместе с соответствующими значениями в формате простого текста и номером (-ами) версии  $K_M$  и  $K_ID$ , используемых для шифрования.

Примечание: это значит, что в последний год срока действия сертификата ERCA датчики движения выдаются с зашифрованными данными на основе  $K_M$  трёх разных поколений, как показано на Рисунок 2.

TCS\_259 Что касается процесса, описанного выше в TCS\_249: Поскольку длина ключа соединения  $K_P$  связана с длиной  $K_M$  (см. TCS\_242), производитель датчика движения может быть вынужден генерировать до трёх различных ключей соединения (различной длины) для одного датчика движения в случае, если у последующих поколений  $K_M$  разная длина. В подобном случае производитель передаёт MSCA каждый ключ соединения. MSCA заботится о том, чтобы каждый ключ соединения был зашифрован при правильном генерировании ключа старшего порядка датчика движения, т.е. ключа такой же длины.

Примечание: Если производитель датчика движения решает генерировать ключ соединения на базе TDES для датчика движения второго поколения (см. TCS\_253), производитель указывает MSCA, что ключ старшего порядка датчика движения на базе TDES должен использоваться для шифрования данного ключа соединения. Это связано с тем, что длина ключа TDES может быть равна длине ключа AES, так что MSCA не может ориентироваться лишь на длину ключа.

TCS\_260 Производители бортовых устройств в каждое бортовое устройство включают лишь одно поколение  $K_{M-VU}$  вместе с номером версии. Такое генерирование  $K_{M-VU}$  связано с сертификатом ERCA, на который опираются сертификаты БУ.

Примечания:

- В бортовое устройство, основанное на сертификате ERCA поколения  $X$ , вводится только  $K_{M-VU}$  поколения  $X$ , даже если оно выпускается после начала срока действия сертификата ERCA поколения  $X+1$ . Это показано на Рисунок 2.
- БУ поколения  $X$  нельзя подсоединять к датчику движения поколения  $X-1$ .
- Поскольку карточки мастерской действительны в течение года, согласно TCS\_255-TCS\_260 все карточки мастерской будут содержать новый  $K_{M-WC}$  в момент выпуска первого БУ, содержащего новый  $K_{M-VU}$ . Таким образом, такой БУ всегда сможет вычислить 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 связи DSRC

### 9.2.2.1 Общие положения

TCS\_261 Подлинность и конфиденциальность данных, передающихся из бортового устройства контрольному органу через канал удалённой связи DSRC, обеспечиваются при помощи ряда ключей AES, конкретно связанных с БУ, полученных на основе единого ключа старшего порядка DSRC  $K_{M_{DSRC}}$ .

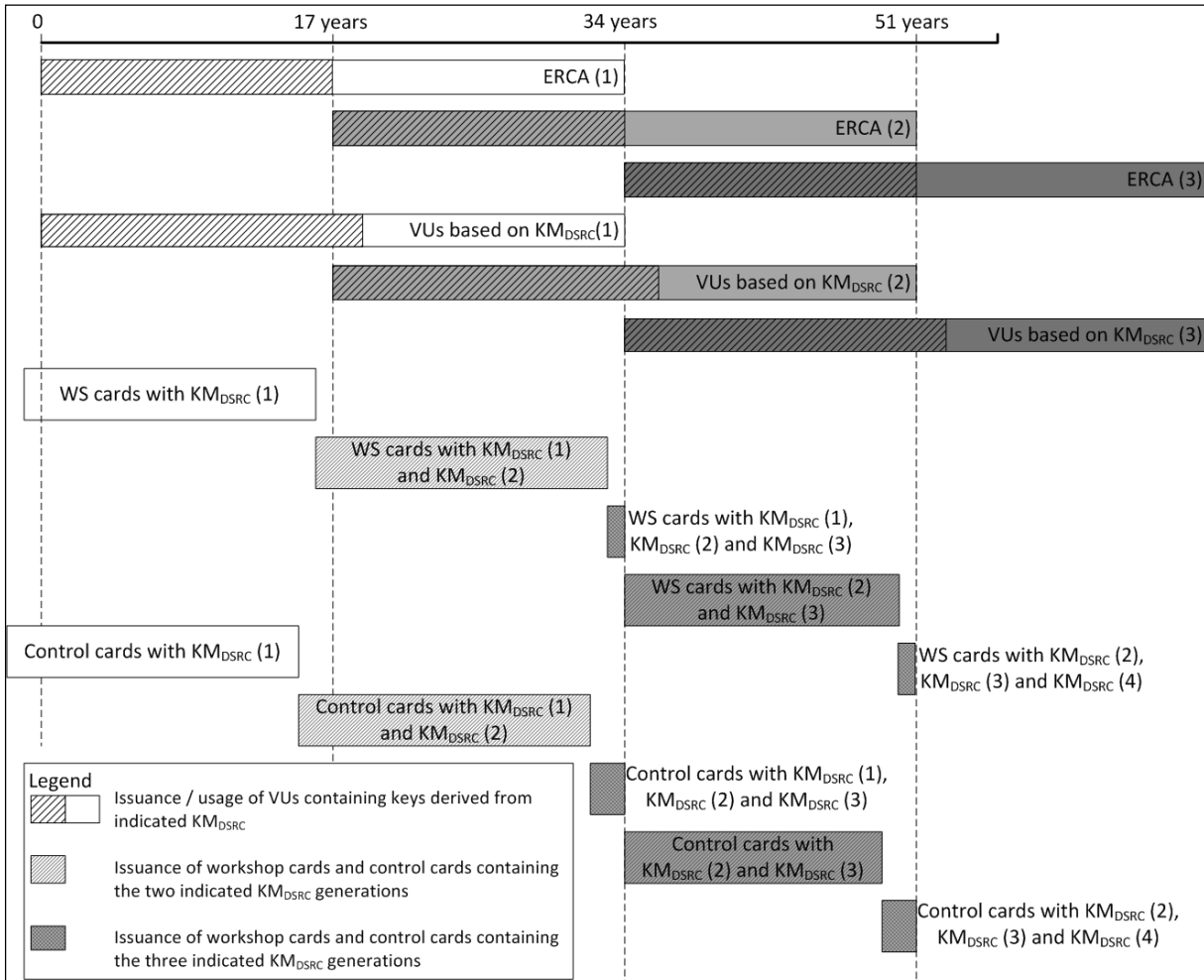
TCS\_262 Ключ старшего порядка DSRC  $K_{M_{DSRC}}$  – это ключ AES, который в защищённом виде генерирует, хранит и распространяет ERCA. Длина ключа может быть 128, 192 или 256 бит и связана с длиной пары европейских корневых ключей, как описано в TCS\_192.

- TCS\_263 ERCA передаёт ключ старшего порядка DSRC сертификационным органам государства-члена по их просьбе в защищённом виде, чтобы они могли извлечь ключи DSRC, конкретно связанные с БУ, и позаботиться о том, чтобы ключ старшего порядка DSRC был помещён на все контрольные карточки и карточки мастерской, выданные в сфере их ответственности.
- TCS\_264 Каждому ключу старшего порядка DSRC ERCA присваивает уникальный номер версии. ERCA сообщает MSCA о номере версии, когда отправляет им ключ старшего порядка DSRC.
- Примечание: Номер версии используется для различения разных поколений ключей старшего порядка DSRC, как подробно поясняется в разделе 9.2.2.2.
- TCS\_265 Для каждого бортового устройства производитель бортовых устройств создаёт уникальный серийный номер БУ и передаёт его сертификационному органу своего государства-члена с заявкой на получение набора из двух ключей DSRC, связанных с конкретным БУ. Серийный номер БУ содержит тип данных `VuSerialNumber`, а для кодирования применяются особые правила кодирования (DER) в соответствии с [ISO 8825-1].
- TCS\_266 По получении заявки на ключи DSRC, связанные с конкретным БУ, MSCA производит два ключа AES для бортового устройства, обозначаемые как `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 TCS\_192. Функция создания ключей в [RFC 5869] используется следующим образом:
- Этап 1 (извлечение):
- $PRK = \text{HMAC-Hash}(salt, IKM)$ , где  $salt$  – это пустая строка ‘’, а  $IKM$  – это  $K_{DSRC}$ .
- Этап 2 (расширение):
- $OKM = T(1)$ , где
    - $T(1) = \text{HMAC-Hash}(PRK, T(0) \parallel info \parallel '01')$  с
      - o  $T(0) =$  пустая строка (‘’)
      - o  $info =$  серийный номер БУ, как указано в TCS\_265
    - $K_{VU\_DSRC\_ENC} =$  первые  $L$  октеты  $OKM$  и  
 $K_{VU\_DSRC\_MAC} =$  последние  $L$  октеты  $OKM$ ,  
 где  $L$  – это требуемая длина  $K_{VU\_DSRC\_ENC}$  и  $K_{VU\_DSRC\_MAC}$  в октетах.
- TCS\_267 MSCA распределяет `K_VU_DSRC_ENC` и `K_VU_DSRC_MAC` в защищённом виде производителю БУ для ввода в соответствующее бортовое устройство.
- TCS\_268 При выпуске на бортовом устройстве в защищённом блоке памяти уже есть `K_VU_DSRC_ENC` и `K_VU_DSRC_MAC`, чтобы оно было в состоянии обеспечить целостность, подлинность и конфиденциальность данных, передаваемых через канал удалённой связи. Бортовое устройство также хранит номер версии ключа старшего порядка DSRC, используемого для выведения этих ключей для конкретного БУ.
- TCS\_269 При выпуске на контрольных карточках и карточках мастерской в защищённом блоке памяти уже есть  $K_{DSRC}$ , чтобы они были в состоянии обеспечить целостность и подлинность данных, передаваемых БУ через канал удалённой связи, и расшифровать эти данные. На контрольных карточках и карточках мастерской также хранится номер версии ключа старшего порядка DSRC.
- Примечание: как поясняется в разделе 9.2.2.2, на одну карточку мастерской или контрольную карточку фактически может быть необходимо поместить несколько поколений  $K_{DSRC}$ .
- TCS\_270 MSCA хранит записи обо всех составленных им ключах DSRC конкретных БУ, номере их версий и идентификационных данных БУ, для которого предназначен каждый набор ключей.

### 9.2.2.2 Замена ключа старшего порядка DSRC

TCS\_271

Каждый ключ старшего порядка DSRC связан с определённым поколением пары корневых ключей ERCA. Таким образом, ERCA заменяет ключ старшего порядка DSRC каждые 17 лет. Срок действия каждого поколения ключей старшего порядка DSRC начинается за два года до вступления в силу соответствующей пары корневых ключей ERCA и кончается, когда истекает срок действия соответствующей пары корневых ключей ERCA. Это показано на Рисунок 3.



**Рисунок 3 Выпуск и использование разных поколений ключей старшего порядка DSRC в бортовых устройствах, на карточках мастерской и на контрольных карточках**

TCS\_272

По крайней мере, за два года до генерирования новой пары европейских корневых ключей, как описано в TCS\_198, ERCA генерирует новый ключ старшего порядка DSRC. Длина ключа DSRC связана с установленным уровнем силы новой пары европейских корневых ключей, в соответствии с TCS\_192. ERCA передаёт новые ключ старшего порядка DSRC MSCA по его просьбе вместе с номером версии.

TCS\_273

MSCA заботится о том, чтобы все действительные поколения  $KM_{DSRC}$  хранились на каждой контрольной карточке, выпущенной в сфере его ответственности, вместе с номерами их версий, как показано на Рисунок 3.

Примечание: это значит, что в последние два года срока действия сертификата ERCA карточки мастерской выдаются с  $KM_{DSRC}$  трёх разных поколений, как показано на Рисунок 3.

TCS\_274 MSCA заботится о том, чтобы все поколения  $KM_{DSRC}$ , действительные хотя бы в течение года и всё ещё действительные, хранились на каждой карточке мастерской, выпущенной в сфере его ответственности, вместе с номерами их версий, как показано на Рисунок 3.

Примечание: это значит, что в последний год срока действия сертификата ERCA карточки мастерской выдаются с  $KM_{DSRC}$  трёх разных поколений, как показано на Рисунок 3.

TCS\_275 Производители бортовых устройств в каждое бортовое устройство включают лишь один набор ключей DSRC, связанных с конкретным БУ, вместе с номером версии. Такой набор ключей выводится на основе поколения  $KM_{DSRC}$ , связанного с сертификатом ERCA, на основании которого выдаются сертификаты БУ.

Примечания:

- Это значит, что в бортовое устройство, основанное на сертификате ERCA поколения  $X$ , вводится только  $K\_VU_{DSRC\_ENC}$  и  $K\_VU_{DSRC\_MAC}$  поколения  $X$ , даже если БУ выпускается после начала срока действия сертификата ERCA поколения  $X+1$ . Это показано на Рисунок 3.
- Поскольку карточки мастерской действительны в течение года, а контрольные карточки – двух лет, согласно TCS\_273-TCS\_275 все карточки мастерской и контрольные карточки будут содержать новый ключ старшего порядка DSRC в момент выпуска первого БУ, содержащего конкретно с ним связанные ключи, основанные на том ключе старшего порядка.

## 9.3. Сертификаты

### 9.3.1 Общие положения

TCS\_276 Все сертификаты европейской системы «умных» тахографов являются самодокументирующимися сертификатами, поддающимися проверке по карточке (CV), в соответствии с [ISO 7816-4] и [ISO 7816-8].

TCS\_277 Для кодирования структур данных ASN.1 и (связанных с конкретным приложением) объектов данных в сертификатах применяются особые правила кодирования (DER) в соответствии с [ISO 8825-1].

Примечание: 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 65535 октетов. Используется минимальное число октетов.
- Значение: Значение кодируется в виде нуля или более октетов.

### 9.3.2 Содержание сертификатов

Структура всех сертификатов такова, как показано в описании сертификата в Таблица 46.

Поле	ИД поля	Метка	Длина (байты)	Тип данных ASN.1 (см. приложение 1)
Сертификат ECC	C	'7F 21'	var	
Сертификационный орган ECC	B	'7F 4E'	var	
Идентификатор описания сертификата	CPI	'5F 29'	'01'	INTEGER (0..255)
Указатель сертифицирующего органа	CAR	'42'	'08'	KeyIdentifier
Полномочия держателя сертификата	CHA	'5F 4C'	'07'	CertificateHolderAuthorisation
Открытый ключ	PK	'7F 49'	var	
Параметры области	DP	'06'	var	OBJECT IDENTIFIER
Открытая точка	PP	'86'	var	OCTET STRING
Указатель держателя сертификата	CHR	'5F 20'	'08'	KeyIdentifier
Дата вступления сертификата в силу	CEfD	'5F 25'	'04'	TimeReal
Дата истечения срока действия сертификата	CExD	'5F 24'	'04'	TimeReal
Подпись сертификата ECC	S	'5F 37'	var	OCTET STRING

Таблица 46 Описание сертификата, версия 1

Примечание: ИД поля применяется в последующих разделах настоящего приложения, чтобы указать на отдельные поля сертификата, например, X.CAR – это указатель сертифицирующего органа, отмеченного в сертификате пользователя X.

#### 9.3.2.1 Идентификатор описания сертификата

В сертификатах идентификатор описания сертификата используется для указания на описание сертификата, взятое за основу. Версия 1, как указано в Таблица 46, обозначается значением '00'.

#### 9.3.2.2 Указатель сертифицирующего органа

Указатель сертифицирующего органа используется для обозначения открытого ключа, который должен применяться для проверки подписи сертификата. Таким образом, указатель сертифицирующего органа в сертификате соответствующего сертификационного органа равен указателю держателя сертификата.

Корневой сертификат ERCA самоподписывающийся, т.е. указатель сертифицирующего органа и указатель держателя сертификата в сертификате равны.

Что касается связующего сертификата ERCA, указатель держателя сертификата равен CHR нового корневого сертификата ERCA. Указатель сертифицирующего органа в связующем сертификате равен CHR прежнего корневого сертификата ERCA.

### 9.3.2.3 Полномочия держателя сертификата

TCS\_283 Полномочия держателя сертификата используются для определения типа сертификата. Они состоят из шести наиболее значимых байтов ИД приложения тахографа в конкатенации с типом оборудования, для которого предназначен сертификат.

### 9.3.2.4 Открытый ключ

Открытый ключ включает в себя два элемента данных: стандартизированные параметры области, используемые с открытым ключом в сертификате, и значение открытой точки.

TCS\_284 Элемент данных параметров области содержит один из идентификаторов объектов, указанных в Таблица 43, чтобы указать на набор стандартизированных параметров области.

TCS\_285 Элемент данных открытой точки содержит в себе открытую точку. Открытые точки эллиптической кривой конвертируются в октетные строки, как указано в [TR-03111]. Используется несжатый формат кодирования. При восстановлении точки эллиптической кривой из кодированного формата всегда проводятся проверки, описанные в [TR-03111].

### 9.3.2.5 Указатель держателя сертификата

TCS\_286 Указатель держателя сертификата – это идентификатор открытого ключа, представленного в сертификате. Он используется для указания этого открытого ключа на других сертификатах.

TCS\_287 В случае сертификатов карточек и сертификатов внешних устройств ГНСС указатель держателя сертификата содержит тип данных `ExtendedSerialNumber`, указанный в приложении 1.

TCS\_288 В отношении бортовых устройств производитель, подавая заявку на сертификат, необязательно знает серийный номер БУ производителя, для которого предназначен сертификат и связанный с ним закрытый ключ. Если номер производителю известен, указатель держателя сертификата содержит тип данных `ExtendedSerialNumber`, указанный в приложении 1. Если номер производителю известен, указатель держателя сертификата содержит тип данных `CertificateRequestID`, указанный в приложении 1.

TCS\_289 В случае сертификатов ERCA и MSCA указатель держателя сертификата содержит тип данных `CertificationAuthorityKID`, указанный в приложении 1.

### 9.3.2.6 Дата вступления сертификата в силу

TCS\_290 Дата вступления сертификата в силу указывает на дату и время начала периода действительности сертификата. Это дата поколения сертификата.

### 9.3.2.7 Дата истечения срока действия сертификата

TCS\_291 Дата истечения срока действия сертификата указывает на дату и время конца периода действительности сертификата.

### 9.3.2.8 Подпись сертификата

TCS\_292 Подпись на сертификате создаётся через закодированную основную часть сертификата, включая метку и длину основной части сертификата. Алгоритм подписи – ECDSA, как указано в [DSS], с использованием алгоритма хеширования, связанного с размером ключа подписывающего органа, как указано в TCS\_192. Формат подписи простой, как указано в [TR-03111].

### 9.3.3 Заявки на сертификаты

- TCS\_293 При подаче заявки на сертификат заявитель передаёт своему сертификационному органу следующие данные:
- Идентификатор описания соответствующего сертификата
  - Указатель сертифицирующего органа, в который планируется обратиться за подписью сертификата.
  - Открытый ключ, подлежащий подписи
- TCS\_294 Помимо данных в TCS\_293, MSCA передаёт следующие данные в заявке на сертификат ERCA, что позволяет ERCA сформировать указатель держателя сертификата для нового сертификата MSCA:
- Цифровой код государства сертификационного органа (тип данных `NationNumeric`, определённый в приложении 1)
  - Буквенно-цифровой код государства сертификационного органа (тип данных `NationAlpha`, определённый в приложении 1)
  - 1-байтовый серийный номер, позволяющий проводить различие между различными ключами сертификационного органа в случае изменения ключей
  - Двухбайтовое поле, содержащее конкретную дополнительную информацию о сертификационном органе
- TCS\_295 Помимо данных в TCS\_293, производитель оборудования передаёт следующие данные в заявке на сертификат MSCA, что позволяет MSCA сформировать указатель держателя сертификата для нового сертификата оборудования:
- Идентификатор типа оборудования конкретного производителя
  - Если известен (см. TCS\_296), серийный номер оборудования, уникальный для данного производителя, типа оборудования и месяц изготовления. В противном случае, уникальный идентификатор заявки на сертификат.
  - Месяц и год изготовления оборудования или заявки на сертификат.
- Производитель заботится о том, чтобы эта дата была правильной и чтобы выданный MSCA сертификат был введён в оборудование, для которого он предназначен.
- TCS\_296 В отношении БУ производитель, подавая заявку на сертификат, необязательно знает серийный номер БУ производителя, для которого предназначен сертификат и связанный с ним закрытый ключ. Если серийный номер известен, производитель БУ передаёт его MSCA. Если он неизвестен, производитель присваивает уникальный идентификатор каждой заявке на сертификат и передаёт этот серийный номер заявки MSCA. Выданный впоследствии сертификат будет содержать серийный номер заявки на сертификат. После ввода сертификата в соответствующее БУ производитель передаёт MSCA связь между серийным номером заявки на сертификат и идентификационными данными БУ.



## 10. Взаимная аутентификация БУ и карточки и защищённый обмен сообщениями

### 10.1. Общие положения

На высоком уровне защищённая связь между бортовым устройством и карточкой тахографа осуществляется следующими этапами:

- Во-первых, каждая сторона доказывает другой наличие у неё действительного сертификата открытого ключа, подписанного сертификационным органом государства-члена. Сертификат открытого ключа MSCA в свою очередь должен быть подписан европейским сертификационным органом. Данный этап называется проверкой цепочки сертификата и подробно рассматривается в разделе 10.2
- Во-вторых, бортовое устройство доказывает карточке наличие у него закрытого ключа, соответствующего открытому ключу в представленном сертификате. Это происходит путём подписания случайного числа, отправленного карточкой. Карточка проверяет подпись случайного числа. Если проверка выполнена успешно, происходит аутентификация БУ. Данный этап называется аутентификацией БУ и подробно рассматривается в разделе 10.3.
- В-третьих, обе стороны самостоятельно вычисляют два сеансовых ключа AES при помощи алгоритма согласования асимметричного ключа. При помощи одного из этих сеансовых ключей карточка создаёт код аутентификации сообщения (MAC), связанный с некоторыми данными, переданными из БУ. БУ проверяет MAC. Если проверка выполнена успешно, происходит аутентификация карточки. Данный этап называется аутентификацией карточки и подробно рассматривается в разделе 10.4.
- В-четвёртых, БУ и карточка используют согласованные сеансовые ключи для обеспечения конфиденциальности, целостности и подлинности всех передаваемых сообщений. Данный этап называется защищённым обменом сообщениями и подробно рассматривается в разделе 10.5.

Механизм, описанный в TCS\_297, запускается бортовым устройством всякий раз, когда в одно из его считывающих устройств вводится карточка.

### 10.2. Взаимная проверка цепочки сертификата

#### 10.2.1 Проверка цепочки сертификата карточки, проводимая БУ

Для проверки цепочки сертификата карточки тахографа бортовые устройства используют протокол, изображённый на Рисунок 4.

Примечания к Рисунок 4:

- Сертификаты карточки и открытые ключи, указанные на рисунке, предназначены для взаимной аутентификации. В разделе 9.1.5 они обозначаются как Card\_MA.
- Сертификаты Card.CA и открытые ключи, указанные на рисунке, предназначены для подписания сертификатов карточек, и это отмечено в CAR сертификата карточки. В разделе 9.1.3 они обозначаются как MSCA\_Card.
- Сертификат Card.CA.EUR, указанный на рисунке – это европейский корневой сертификат, отмеченный в CAR сертификата Card.CA.
- Сертификат Card.Link, указанный на рисунке, – это связующий сертификат карточки, если он имеется. Как указано в разделе 9.1.2, это связующий сертификат для новой пары европейских корневых ключей, созданной ERCA и подписанной прежним европейским закрытым ключом.
- Сертификат Card.Link.EUR – это европейский корневой сертификат, отмеченный в CAR сертификата Card.Link.

TCS\_300 Как показано на Рисунок 4, проверка цепочки сертификата карточки начинается с ввода карточки. Бортовое устройство считывает указатель владельца карточки (`cardExtendedSerialNumber`) из EF ICC. БУ проверяет, известна ли ему карточка, т.е. была ли в прошлом проведена успешная проверка цепочки сертификата карточки, которая была сохранена на будущее. Если да и если сертификат карточки всё ещё действителен, процесс продолжается, и проводится проверка цепочки сертификата БУ. В противном случае БУ последовательно считывает с карточки сертификат MSCA\_Card, используемый для проверки сертификата карточки Card.CA. Сертификат EUR, используемого для проверки сертификата MSCA\_Card и, возможно, связующего сертификата, пока не будет найден известный ему сертификат или сертификат, который он может проверить. Если такой сертификат найден, БУ использует его для проверки базовых сертификатов карточки, которые он считал с карточки. Если проверка прошла успешно, процесс продолжается, и проводится проверка цепочки сертификата БУ. Если нет, БУ игнорирует карточку.

Примечание: Есть три способа, по которым БУ узнаёт 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, и этот сертификат уже содержался в БУ при его выпуске (см. CSM\_81);
- сертификат Card.CA.EUR выдан позднее собственного сертификата EUR БУ, и БУ в прошлом получил связующий сертификат с другой карточки тахографа, проверил его и сохранил на будущее.

TCS\_301 Как показано на Рисунок 4, как только БУ проверит подлинность и действительность ранее неизвестного сертификата, он может сохранить этот сертификат на будущее, чтобы не надо было снова проверять подлинность этого сертификата, если он будет опять представлен БУ. Вместо хранения всего сертификата БУ может принять решение хранить только содержание основной части сертификата, как указано в разделе 9.3.2.

TCS\_302 БУ проверяет временную действительность любого сертификата, считываемого с карточки или хранящегося в его памяти, и отклоняет просроченные сертификаты. Для проверки временной действительности представленного карточкой сертификата БУ использует внутренние часы.

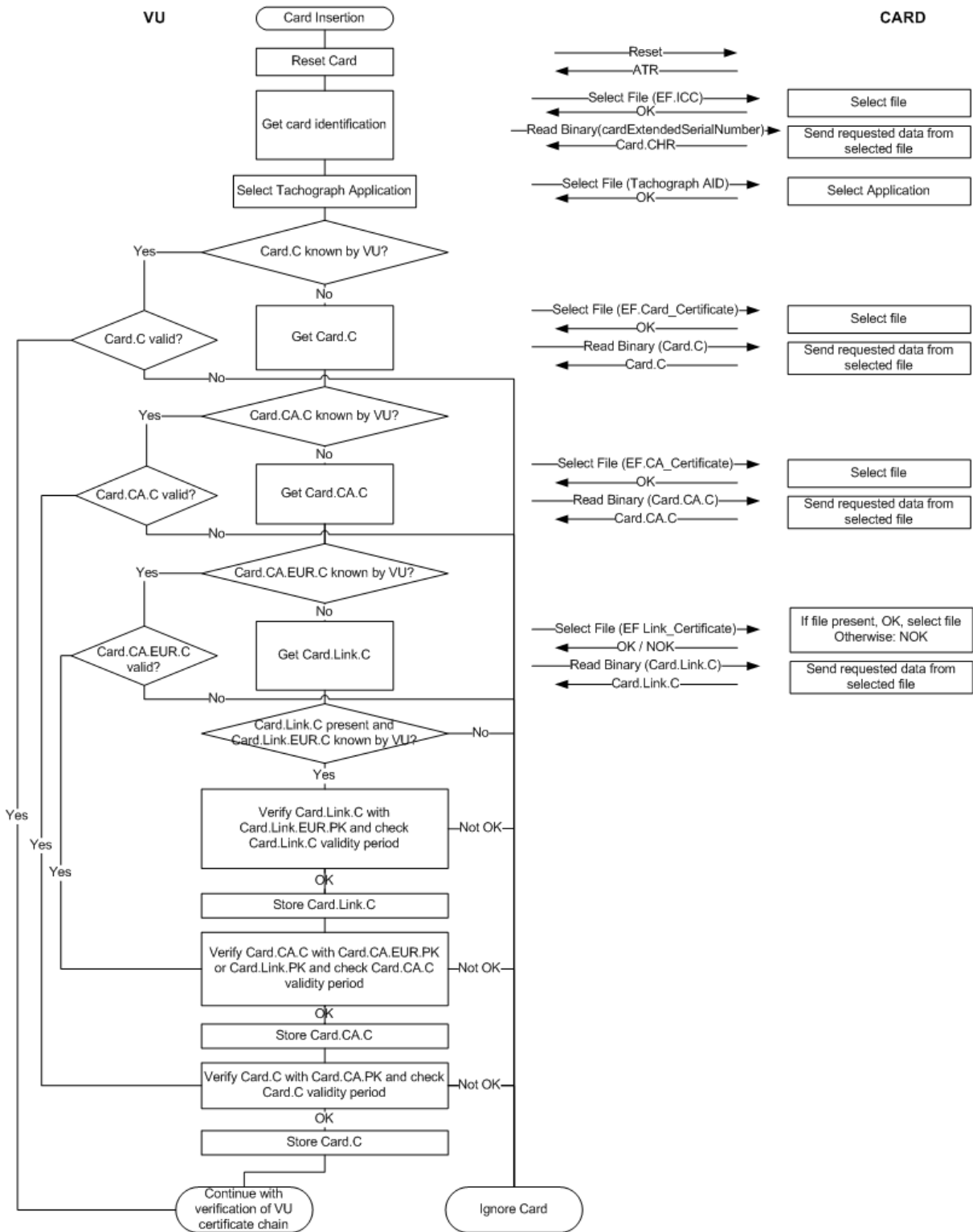
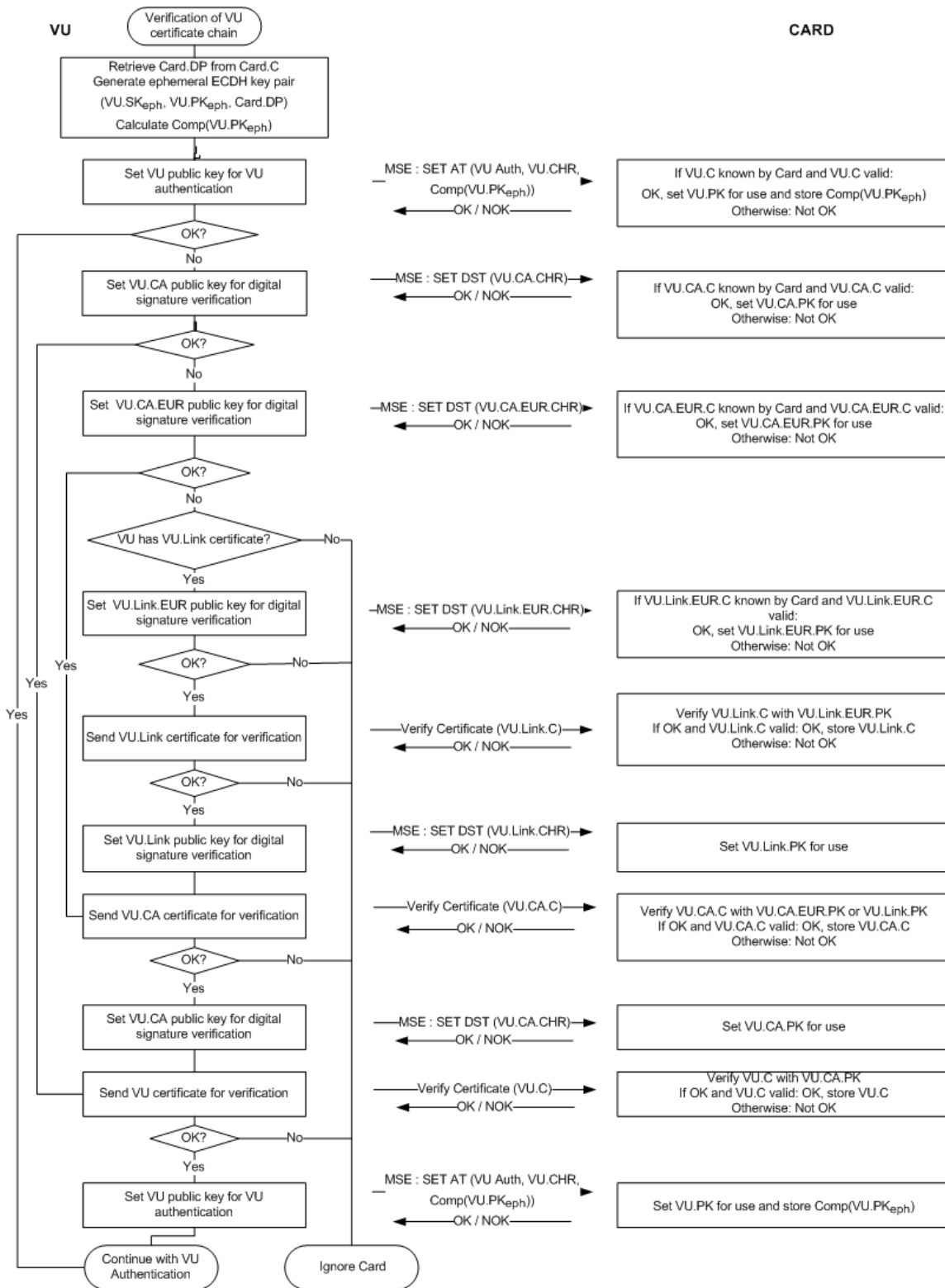


Рисунок 4 Протокол проверки цепочки сертификата карточки, проводимой ВУ

### 10.2.2 Проверка цепочки сертификата ВУ, проводимая карточкой

Для проверки цепочки сертификата ВУ карточки тахографа используют протокол, изображённый на Рисунке 5.



**Рисунок 5** Протокол проверки цепочки сертификата БУ, проводимой карточкой

## Примечания к Рисунок 5:

- Сертификаты БУ и открытые ключи, указанные на рисунке, предназначены для взаимной аутентификации. В разделе 9.1.4 они обозначаются как VU\_MA.
- Сертификаты VU.CA и открытые ключи, указанные на рисунке, предназначены для подписания сертификатов БУ и внешних устройств ГНСС. В разделе 9.1.3 они обозначаются как MSCA\_VU-EGF.
- Сертификат VU.CA.EUR, указанный на рисунке – это европейский корневой сертификат, отмеченный в CAR сертификата VU.CA.
- Сертификат VU.Link, указанный на рисунке, – это связующий сертификат БУ, если он имеется. Как указано в разделе 9.1.2, это связующий сертификат для новой пары европейских корневых ключей, созданной ERCA и подписанной прежним европейским закрытым ключом.
- Сертификат VU.Link.EUR – это европейский корневой сертификат, отмеченный в CAR сертификата VU.Link.

TCS\_304 Как показано на Рисунок 5, проверка цепочки сертификата бортового устройства начинается с того, что бортовое устройство пытается установить свой собственный открытый ключ для использования на карточке тахографа. Если эта попытка удалась, это значит, что карточка успешно проверяла цепочку сертификата БУ ранее и сохранила сертификат БУ на будущее. В таком случае сертификат БУ можно использовать, и процесс продолжается с проведением аутентификации БУ. Если сертификат БУ карточке неизвестен, БУ последовательно представляет сертификат VU.CA для проверки его 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 найден, карточка использует его для проверки базовых сертификатов БУ, которые были ей представлены. Если получилось, БУ наконец устанавливает свой собственный открытый ключ для использования на карточке тахографа. Если нет, БУ игнорирует карточку.

Примечание: Есть три способа, по которым карточка узнаёт 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 при её выпуске (см. CSM\_91);
- сертификат VU.CA.EUR выдан позднее собственного сертификата EUR карточки, и карточка в прошлом получила связующий сертификат из другого бортового устройства, проверила его и сохранила на будущее.

TCS\_305 БУ использует MSE: Set AT, чтобы установить свой собственный открытый ключ для использования на карточке тахографа. Как указано в приложении 2, эта команда содержит указание криптографического механизма, который используется с установленным ключом. Этот механизм – аутентификация БУ с применением алгоритма ECDSA в сочетании с алгоритмом хеширования, связанным с размером ключа пары ключей VU\_MA БУ, как указано в TCS\_192.

TCS\_306 Команда MSE: Set AT также содержит указание на кратковременную пару ключей, которую БУ использует во время согласования сеансовых ключей (см. раздел 10.4). Таким образом, перед передачей команды MSE: Set AT БУ генерирует кратковременную пару ключей ECC. Для генерирования кратковременной пары ключей БУ использует стандартизированные параметры области, указанные в сертификате карточки. Кратковременная пара ключей обозначается как  $(VU.SK_{eph}, VU.PK_{eph}, Card.DP)$ . БУ принимает координату  $x$  кратковременной открытой точки ECDH как идентификационные данные ключа; это называется сжатым выражением открытого ключа и обозначается как  $Comp(VU.PK_{eph})$ .

TCS\_307 Если команда MSE: Set AT выполнена успешно, карточка устанавливает указанный VU.PK для 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, карточка сохраняет только последнюю полученную команду  $Comp(VU.PK_{eph})$ .

TCS\_308 Карточка проверяет временную действительность любого сертификата, представляемого БУ или указанного БУ и при этом хранящегося в памяти карточки, и отклоняет просроченные сертификаты.

TCS\_309 Для проверки временной действительности представленного БУ сертификата, каждая карточка тахографа внутри сохраняет некоторые данные, представляющие текущий момент времени. БУ эти данные напрямую не обновляет. При выпуске текущее время карточки устанавливается как равно фактической дате сертификата Card\_MA карточки. Карточка обновляет своё текущее время, если фактическая дата подлинного действительного источника времени, представленная БУ, более поздняя, чем текущее время карточки. В подобном случае карточка устанавливает своё 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 сертификат (-ы) карточки.

Примечание: последнее требование значит, что карточка способна распознавать CAR сертификата БУ, т.е. сертификата MSCA\_VU-EGF. Он будет отличаться от CAR её собственного сертификата, т.е. сертификата MSCA\_Card.

TCS\_310 Как показано на Рисунок 5, как только карточка проверит подлинность и действительность ранее неизвестного сертификата, она может сохранить этот сертификат на будущее, чтобы не надо было снова проверять подлинность этого сертификата, если он будет опять представлен карточке. Вместо хранения всего сертификата карточка может принять решение хранить только содержание основной части сертификата, как указано в разделе 9.3.2.

### **10.3. Аутентификация БУ**

TCS\_311 Бортовые устройства и карточки используют протокол аутентификации БУ, представленный на Рисунок 6 для аутентификации БУ относительно карточки. Аутентификация БУ позволяет карточке тахографа достоверно проверить подлинность БУ. Для этого БУ использует закрытый ключ для подписания запроса, сгенерированного карточкой.

TCS\_312 Помимо запроса карточки, БУ включает в подпись указатель владельца карточки, взятый из сертификата карточки.

Примечание: Таким образом обеспечивается, что карточка, относительно которой происходит аутентификация БУ, является той же самой карточкой, цепочку сертификата которой БУ уже проверял.

TCS\_313 БУ также включает в подпись идентификатор кратковременного открытого ключа  $Comp(VU.PK_{eph})$ , который БУ использует для установки защищённого обмена сообщениями во время процесса аутентификации микросхемы, указанного в разделе 10.4.

Примечание: Тем самым обеспечивается, чтобы БУ, с которым карточка установила связь во время сеанса защищённого обмена сообщениями, был тот же самый БУ, который был аутентифицирован карточкой.

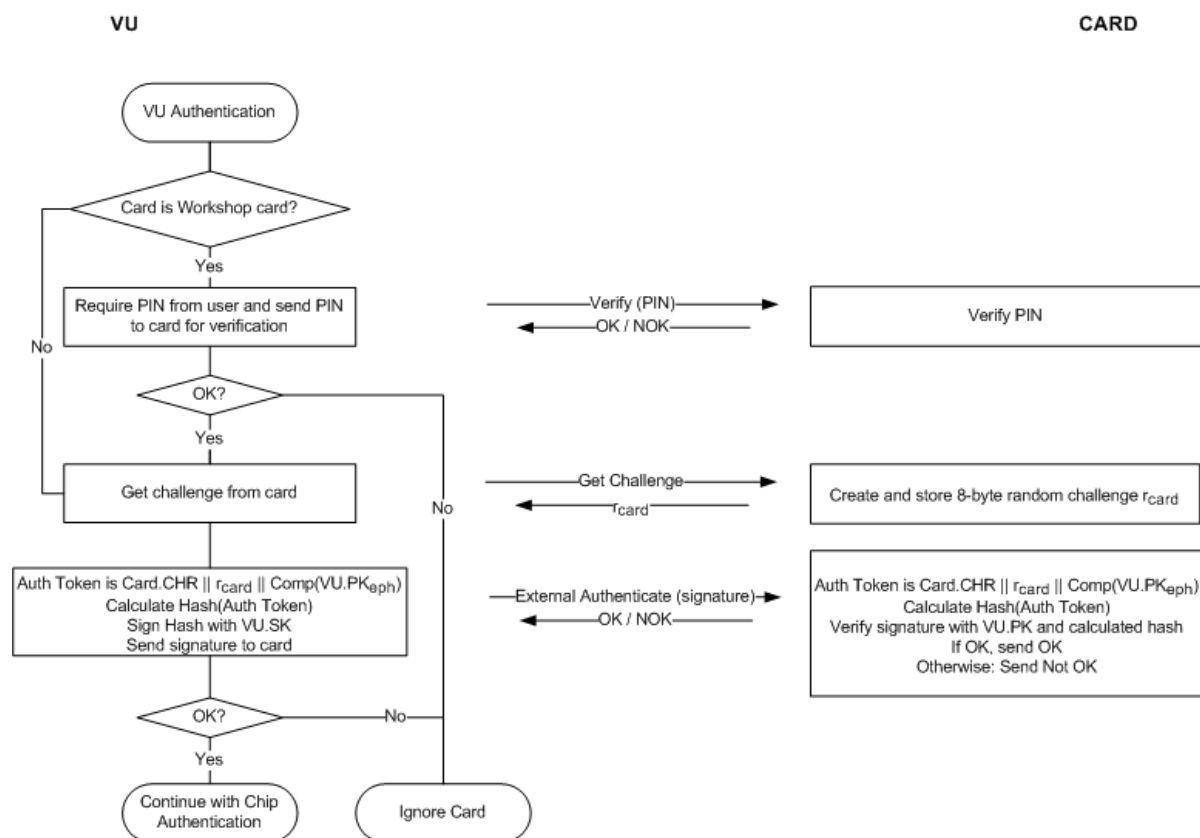


Рисунок 6 Протокол аутентификации БУ

TCS\_314 Если во время аутентификации БУ передаёт несколько команд GET CHALLENGE, карточка каждый раз возвращает новый 8-байтовый случайный запрос, а сохраняет только последний из них.

TCS\_315 Алгоритм подписи, который БУ использует для аутентификации БУ, – ECDSA, как указано в [DSS], с использованием алгоритма хеширования, связанного с размером ключа пары ключей VU\_MA БУ, как указано в TCS\_192. Формат подписи простой, как указано в [TR-03111]. БУ передаёт полученную подпись на карточку.

TCS\_316 По получении подписи БУ в команде EXTERNAL AUTHENTICATE карточка

- Вычисляет маркер аутентификации путём конкатенации Card.CHR, запроса карточки  $r_{card}$  и идентификатора кратковременного открытого ключа БУ  $Comp(VU.PK_{eph})$ ,
- Вычисляет хеш-функцию, связанную с маркером аутентификации, с применением алгоритма хеширования, связанного с размером ключа пары ключей VU\_MA БУ, как указано в TCS\_192,
- Проверяет подпись БУ с применением алгоритма ECDSA в сочетании с VU.PK и вычисленной хеш-функцией.

#### 10.4. Аутентификация микросхемы и согласование сеансовых ключей

TCS\_317 Бортовые устройства и карточки используют протокол аутентификации микросхемы, представленный на  
 TCS\_318 **Рисунок 7** для аутентификации карточки относительно БУ. Аутентификация микросхемы позволяет бортовому устройству достоверно проверить подлинность карточки.

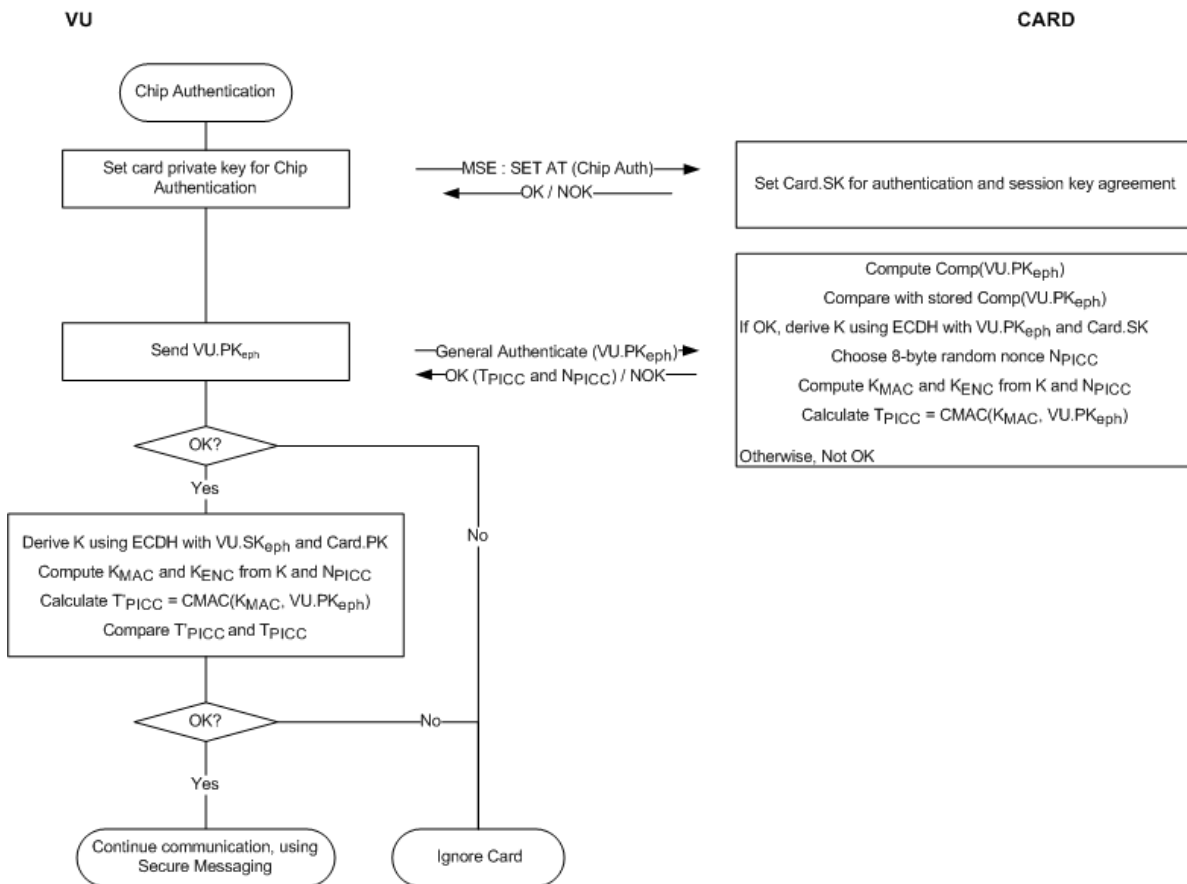


Рисунок 7 Аутентификация микросхемы и согласование сеансовых ключей

БУ и карточка предпринимают следующие действия:

1. Бортовое устройство инициирует процесс аутентификации микросхемы, передавая команду MSE: Set AT с указанием аутентификации микросхемы с применением алгоритма ECDSA, в результате чего получается длина сеансового ключа AES, связанная с размером ключа пары ключей Card\_MA карточки, как указано в TCS\_192. БУ определяет размер ключа пары ключей карточки по сертификату карточки.
2. БУ передаёт открытую точку  $VU.PK_{eph}$  своей кратковременной пары ключей на карточку. Как поясняется в TCS\_306, БУ сгенерировал эту кратковременную пару ключей до проверки цепочки сертификата БУ. БУ передало идентификатор кратковременного открытого ключа  $Comp(VU.PK_{eph})$  на карточку, и карточка его сохранила.
3. Карточка вычисляет  $Comp(VU.PK_{eph})$  по  $VU.PK_{eph}$  и сравнивает полученное значение с сохранённым значением  $Comp(VU.PK_{eph})$ .
4. Используя алгоритм ECDH в сочетании со статичным закрытым ключом карточки и кратковременным открытым ключом БУ, карточка вычисляет тайный K.
5. Карточка выбирает случайный временный 8-байтовый код  $N_{PICC}$  и использует его для получения двух сеансовых ключей AES  $K_{MAC}$  и  $K_{ENC}$  из K. См. TCS\_322.
6. Используя  $K_{MAC}$ , карточка вычисляет маркер аутентификации по идентификатору кратковременного открытого ключа БУ:  $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$ . Карточка передаёт  $N_{PICC}$  и  $T_{PICC}$  в бортовое устройство.
7. Используя алгоритм ECDH в сочетании со статичным открытым ключом карточки и кратковременным закрытым ключом БУ, БУ вычисляет тот же самый тайный K, что и карточка на этапе 4.



8. БУ получает сеансовые ключи  $K_{MAC}$  и  $K_{ENC}$  из  $K$  и  $N_{PICC}$ ; см. TCS\_322.
9. БУ проверяет маркер аутентификации  $T_{PICC}$ .

- TCS\_320 На указанном выше этапе 3 карточка вычисляет  $Comp(VU.PKeph)$  как координату  $x$  открытой точки в  $VU.PKeph$ .
- TCS\_321 На указанных выше этапах 4 и 7 карточка и бортовое устройство используют алгоритм ЕСКА-EG, как описано в [TR-03111].
- TCS\_322 На указанных выше этапах 5 и 8 карточка и бортовое устройство используют функцию составления ключей для сеансовых ключей AES, как описано в [TR-03111], с учётом следующих уточнений и изменений:
- Значение счётчика – '00 00 00 01' для  $K_{ENC}$  и '00 00 00 02' для  $K_{MAC}$ .
  - Используется факультативное временное значение  $r$ , равное  $N_{PICC}$ .
  - 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.
- TCS\_323 На указанных выше этапах 6 и 9 карточка и бортовое устройство используют алгоритм AES в режиме СМАС, как описано в [SP 800-38B]. Длина  $T_{PICC}$  связана с длиной сеансовых ключей AES, как описано в TCS\_192.

## 10.5. Защищённый обмен сообщениями

### 10.5.1 Общие положения

- TCS\_324 Все команды и ответы, которыми обмениваются бортовое устройство и карточка тахографа после успешной аутентификации микросхемы и до конца сеанса, защищены механизмом защищённого обмена сообщениями.
- TCS\_325 За исключением случаев считывания из файла с условием доступа SM-R-ENC-MAC-G2 (см. приложение 2, раздел 4), защищённый обмен сообщениями используется только в режиме аутентификации. В этом режиме ко всем командам и ответам добавляется криптографическая контрольная сумма (MAC), чтобы обеспечить подлинность и целостность сообщения.
- TCS\_326 При считывании данных из файла с условием доступа SM-R-ENC-MAC-G2 защищённый обмен сообщениями используется в режиме шифрования с последующей аутентификацией, т.е. данные ответа сначала шифруются, чтобы обеспечить конфиденциальность сообщения, а затем вычисляется MAC, связанная с отформатированными зашифрованными данными, для обеспечения подлинности и целостности.
- TCS\_327 Защищённый обмен сообщениями использует AES, как описано в [AES], с сеансовыми ключами  $K_{MAC}$  и  $K_{ENC}$ , согласованными в процессе аутентификации микросхемы.
- TCS\_328 В качестве счётчика исходящих сообщений (SSC) для предотвращения повторных атак используется неподписанное целое число. Размер SSC равен размеру блока AES, т.е. 128 битам. SSC представлен в формате изначальных MSB. Счётчик исходящих сообщений выставляется на ноль (т.е. '00 00 00 00 00 00 00 00 00 00 00 00 00 00'), когда начинается защищённый обмен сообщениями. SSC увеличивается всякий раз перед генерированием команды или ответа APDU, т.к. поскольку стартовое значение SSC в сеансе SM равно 0, в первой команде значение SSC будет 1. Значение SSC в первом ответе будет 2.
- TCS\_329 Для шифрования сообщения используется  $K_{ENC}$  с AES в режиме сцепления криптоблоков (CBC), как описано в [ISO 10116], с параметром чередования  $m = 1$  и вектором инициализации  $SV = E(K_{ENC}, SSC)$ , т.е. текущее значение счётчика исходящих сообщений, зашифрованного при помощи  $K_{ENC}$ .

TCS\_330 Для аутентификации сообщений используется  $K_{MAC}$  с AES в режиме CMAC, как описано в [SP 800-38B]. Длина MAC связана с длиной сеансовых ключей AES, как описано в TCS\_192. Счётчик исходящих сообщений включается в MAC путём его добавления перед аутентификацией датаграммы.

## 10.5.2 Структура защищённого сообщения

TCS\_331 Защищённый обмен сообщениями использует только объекты данных защищённого обмена сообщениями (см. [ISO 7816-4]), перечисленные в Таблица 47. В любом сообщении эти объекты данных используются в очерёдности, указанной в данной таблице

Название объекта данных	Метка	Присутствие обязательно (M), условно (C) или запрещено (F)	
		Команды	Ответы
Простое значение, не закодированное в BER-TLV	'81'	C	C
Простое значение, закодированное в BER-TLV, но не включающее в себя объекты данных SM	'B3'	C	C
Показатель заполняющего содержания с последующей пиктограммой, простое значение, не закодированное в BER-TLV	'87'	C	C
Защищённое значение Le	'97'	C	F
Статус обработки	'99'	F	M
Криптографическая контрольная сумма	'8E'	M	M

Таблица 47 Объекты данных защищённого обмена сообщениями

Примечание: Как указано в приложении 2, карточки тахографа могут поддерживать команды READ BINARY и UPDATE BINARY с нечётным байтом INS ('B1' resp. 'D7'). Эти варианты команд необходимы для считывания и обновления файлов, содержащих более чем 32768 байтов или более. В случае использования такого варианта вместо объекта с меткой '81' используется объект данных с меткой 'B3'. Более подробно см. приложение 2.

TCS\_332 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 65535 октетов. Используется минимальное число октетов.
- Значение: Значение кодируется в виде нуля или более октетов.

TCS\_333 APDU, защищённые механизмом защищённого обмена сообщениями, создаются следующим образом:

- Заголовок команды включается в вычисление MAC, так что значение '0C' используется для классового байта CLA.
- Как указано в приложении 2, все байты INS чётные, с возможным исключением нечётных байтов INS для команд READ BINARY и UPDATE BINARY.
- Фактическое значение Lc будет изменено на Lc' после применения механизма защищённого обмена сообщениями.
- Поле данных состоит из объектов данных SM.
- В защищённой команде APDU новый байт Le устанавливается на '00'. При необходимости объект данных '97' включается в поле данных, чтобы передать исходное значение Le.

TCS\_334 Любой объект данных, подлежащий шифрованию, заполняется в соответствии с [ISO 7816-4] при помощи показателя заполнения '01'. Для вычисления MAC каждый объект данных в APDU также отдельно заполняется в соответствии с [ISO 7816-4].

Примечание: Заполнение в механизме защищённого обмена сообщениями всегда происходит на уровне защищённого обмена сообщениями, а не через алгоритмы СМАС или СВС.

### Резюме и примеры

У команды APDU с применяемым механизмом защищённого обмена сообщениями будет следующая структура, в зависимости от соответствующей незащищённой команды (DO – объект данных):

Пример 1: CLA INS P1 P2 || Lc' || DO '8E' || Le  
 Пример 2: CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le  
 Пример 3 (чётный байт INS): CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le  
 Пример 3 (нечётный байт INS): CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le  
 Пример 4 (чётный байт INS): CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le  
 Пример 4 (нечётный 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].

У ответа APDU с применяемым механизмом защищённого обмена сообщениями будет следующая структура, в зависимости от соответствующего незащищённого ответа:

Пример 1 или 3: DO '99' || DO '8E' || SW1SW2  
 Пример 2 или 4 (чётный байт INS) с шифрованием: DO '81' || DO '99' || DO '8E' || SW1SW2  
 Пример 2 или 4 (чётный байт INS) без шифрования: DO '87' || DO '99' || DO '8E' || SW1SW2  
 Пример 2 или 4 (нечётный байт INS) без шифрования: DO 'B3' || DO '99' || DO '8E' || SW1SW2

Примечание: Пример 2 или 4 (нечётный байт INS) с шифрованием никогда не используется при связи между БУ и карточкой.

Далее приводятся три примера трансформаций APDU для команд с чётным кодом INS. Рисунок 8 показывает аутентифицированную команду APDU в примере 4, Рисунок 9 показывает аутентифицированный ответ APDU в примере 2/4, и Рисунок 10 показывает зашифрованный и аутентифицированный ответ APDU в примерах 2/4.

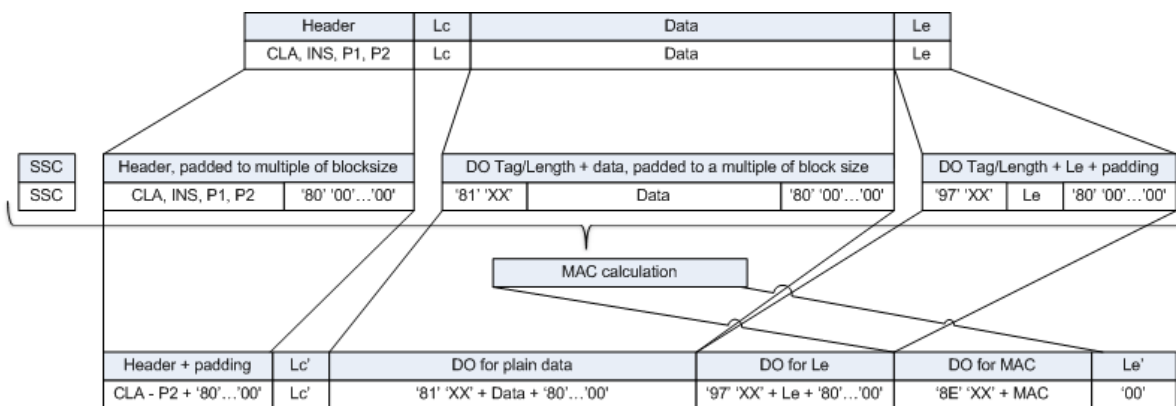


Рисунок 8 Трансформация аутентифицированной команды APDU в примере 4

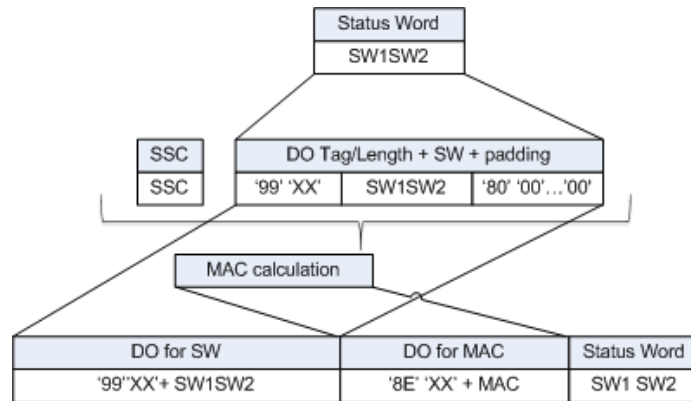


Рисунок 9 Трансформация аутентифицированного ответа APDU в примерах 1/3

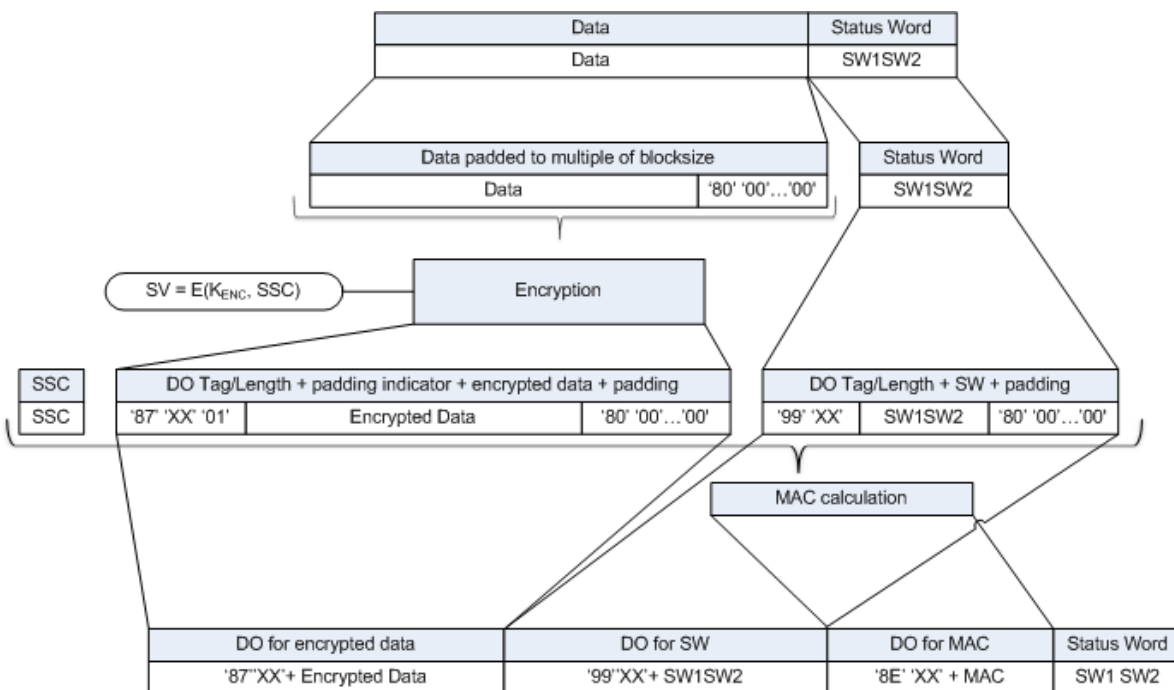


Рисунок 10 Трансформация зашифрованного и аутентифицированного ответа APDU в примерах 2/4

### 10.5.3 Отмена сеанса защищённого обмена сообщениями

Бортовое устройство прерывает текущий сеанс защищённого обмена сообщениями, только если возникает одно из следующих условий:

TCS\_335

- оно получает простой ответ APDU,
- оно обнаруживает ошибку защищённого обмена сообщениями в ответе APDU:
  - o Отсутствие ожидаемого объекта данных защищённого обмена сообщениями, неверная последовательность объектов данных или присутствие неизвестного объекта данных.
  - o Объект данных защищённого обмена сообщениями неверный, например, неверное значение MAC, неверная структура TLV или показатель заполнения с меткой '87' не равен '01'.
- карточка передаёт байт статуса, указывающий на то, что обнаружена ошибка SM (см. TCS\_337),
- достигнуто предельное число команд и соответствующих ответов в рамках текущего сеанса. В отношении данного БУ такой предел устанавливает производитель, учитывающий требования безопасности к используемому аппаратному обеспечению, с максимальным значением 240 команд и ответов SM за сеанс.

TCS\_336 Карточка тахографа прерывает текущий сеанс защищённого обмена сообщениями, только если возникает одно из следующих условий:

- она получает простую команду APDU,
- она обнаруживает ошибку защищённого обмена сообщениями в команде APDU:
  - o Отсутствие ожидаемого объекта данных защищённого обмена сообщениями, неверная последовательность объектов данных или присутствие неизвестного объекта данных.
  - o Объект данных защищённого обмена сообщениями неверный, например, неверное значение MAC или неверная структура TLV.
- прекращено питание или она перезагрузилась,
- БУ выбирает приложение на карточке,
- БУ начинает процесс аутентификации БУ,
- достигнуто предельное число команд и соответствующих ответов в рамках текущего сеанса. В отношении данной карточки такой предел устанавливает производитель, учитывающий требования безопасности к используемому аппаратному обеспечению, с максимальным значением 240 команд и ответов SM за сеанс.

TCS\_337 Касательно ошибки обработки SM на карточке тахографа:

- Если в команде APDU отсутствуют некоторые ожидаемые объекты данных защищённого обмена сообщениями, неверный порядок объектов данных или присутствуют неизвестные объекты данных, карточка тахографа отвечает байтами статуса '69 87'.
- Если в команде APDU неверный объект данных защищённого обмена сообщениями, карточка тахографа отвечает байтами статуса '69 88'.

В таком случае байты статуса возвращаются без использования SM.

TCS\_338 Если сеанс защищённого обмена сообщениями между БУ и карточкой тахографа прерван, БУ и карточка тахографа

- в безопасной манере уничтожают сохранённые сеансовые ключи
- немедленно запускают новый сеанс защищённого обмена сообщениями, как описано в разделах 10.2-10.5.

TCS\_339 Если по какой-либо причине БУ решает перезапустить взаимную аутентификацию в отношении введённой карточки, процесс снова начинается с проверки цепочки сертификата карточки, как описано в разделе 10.2, и продолжается, как описано в разделах 10.2-10.5.

## **11. Соединение, взаимная аутентификация и защищённый обмен сообщениями между БУ и внешним устройством ГНСС**

### **11.1. Общие положения**

- TCS\_340 Устройство ГНСС, которое БУ использует для установления местоположения, может быть внутренним (т.е. встроенным в корпус БУ и не съёмным), или это может быть внешний модуль. В первом случае нет необходимости стандартизировать внутреннюю связь между устройством ГНСС и БУ, и требования настоящей главы не применяются. В последнем случае связь между БУ и внешним устройством ГНСС стандартизируется и защищается, как описано в настоящей главе.
- TCS\_341 Защищённая связь между бортовым устройством и внешним устройством ГНСС происходит так же, как защищённая связь между бортовым устройством и карточкой тахографа, где внешнее устройство ГНСС (EGF) играет роль карточки. EGF удовлетворяет всем требованиям главы 10 к карточкам тахографа с учётом отклонений, пояснений и дополнений, представленных в настоящей главе. В частности, взаимная проверка цепочки сертификата, аутентификация БУ и аутентификация микросхемы проводятся так, как описано в разделах 11.3 и 11.4.
- TCS\_342 Связь между бортовым устройством и EGF отличается от связи между бортовым устройством и карточкой тем, что бортовое устройство и EGF должны быть однажды соединены в мастерской, чтобы впоследствии в режиме нормальной эксплуатации они могли обмениваться данными ГНСС. Процесс соединения описан в разделе 11.2.
- TCS\_343 Для обеспечения 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**

- TCS\_344 Бортовое устройство и EGF транспортного средства соединяются в мастерской. В режиме нормальной эксплуатации связь могут держать только соединённые между собой бортовое устройство и EGF.
- TCS\_345 Соединение бортового устройства и EGF возможно только в том случае, если бортовое устройство находится в режиме калибровки. Соединение инициирует бортовое устройство.
- TCS\_346 Мастерская может в любой момент пересоединить бортовое устройство с другим или тем же самым EGF. В время повторного соединения БУ в безопасной манере уничтожает сохранившийся в памяти сертификат EGF\_MA и сохраняет сертификат EGF\_MA EGF, с которым оно соединяется.
- TCS\_347 Мастерская может в любой момент пересоединить внешнее устройство ГНСС с другим или тем же самым БУ. В время повторного соединения EGF в безопасной манере уничтожает сохранившийся в памяти сертификат VU\_MA и сохраняет сертификат VU\_MA БУ, с которым оно соединяется.

### **11.3. Взаимная проверка цепочки сертификата**

#### **11.3.1 Общие положения**

- TCS\_348 Взаимная проверка цепочки сертификата между БУ и EGF проводится только во время соединения БУ и EGF в мастерской. Во время нормальной эксплуатации соединённых БУ и EGF проверка сертификатов не проводится. Вместо этого БУ и EGF доверяют сертификатам, которые они сохранили во время соединения, после проверки временной действительности таких сертификатов. Для защиты связи БУ и EGF во время нормальной эксплуатации БУ и EGF не доверяют никаким другим сертификатам.

#### **11.3.2 Во время соединения БУ и EGF**

- TCS\_349 Во время соединения с EGF для проверки цепочки сертификата внешнего устройства ГНСС бортовое устройство использует протокол, отображённый на Рисунок 4 (раздел 10.2.1).

Связанные с этим примечания по Рисунок 4:

- Контроль связи не входит в область применения настоящего приложения. Однако EGF не является «умной» карточкой, и потому БУ, скорее всего, не передаст команду Reset для запуска связи и не получит ATR.
- Сертификаты карточки и открытые ключи, указанные на рисунке, интерпретируются как сертификаты и открытые ключи EGF для взаимной аутентификации. В разделе 9.1.6 они обозначаются как EGF\_MA.
- Сертификаты Card.CA и открытые ключи, указанные на рисунке, интерпретируются как сертификаты и открытые ключи MSCA для подписания сертификатов EGF. В разделе 9.1.3 они обозначаются как MSCA\_VU-EGF.
- Сертификат Card.CA.EUR, указанный на рисунке, интерпретируется как европейский корневой сертификат, отмеченный 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 корневых ключей, созданной ERCA и подписанной прежним европейским закрытым ключом.
- Сертификат Card.Link.EUR – это европейский корневой сертификат, отмеченный в CAR сертификата Card.Link.
- Вместо `cardExtendedSerialNumber` БУ считывает `sensorGNSSserialNumber` из EF ICC.
- Вместо выбора AID тахографа БУ выбирает AID EGF.
- ‘Ignore Card’ интерпретируется как ‘Ignore EGF’.

TCS\_350 После проверки сертификата EGF\_MA бортовое устройство хранит этот сертификат для использования во время нормальной эксплуатации; см. раздел 11.3.3.

TCS\_351 Во время соединения с БУ для проверки цепочки сертификата БУ внешнее устройство ГНСС использует протокол, отображённый на Рисунок 5 (раздел 10.2.2).

Связанные с этим примечания по Рисунок 5:

- БУ генерирует новую кратковременную пару ключей с параметрами области в сертификате EGF.
- Сертификаты БУ и открытые ключи, указанные на рисунке, предназначены для взаимной аутентификации. В разделе 9.1.4 они обозначаются как VU\_MA.
- Сертификаты VU.CA и открытые ключи, указанные на рисунке, предназначены для подписания сертификатов БУ и внешних устройств ГНСС. В разделе 9.1.3 они обозначаются как MSCA\_VU-EGF.
- Сертификат VU.CA.EUR, указанный на рисунке – это европейский корневой сертификат, отмеченный в CAR сертификата VU.CA.
- Сертификат VU.Link, указанный на рисунке, – это связующий сертификат БУ, если он имеется. Как указано в разделе 9.1.2, это связующий сертификат для новой пары европейских корневых ключей, созданной ERCA и подписанной прежним европейским закрытым ключом.
- Сертификат VU.Link.EUR – это европейский корневой сертификат, отмеченный в CAR сертификата VU.Link.

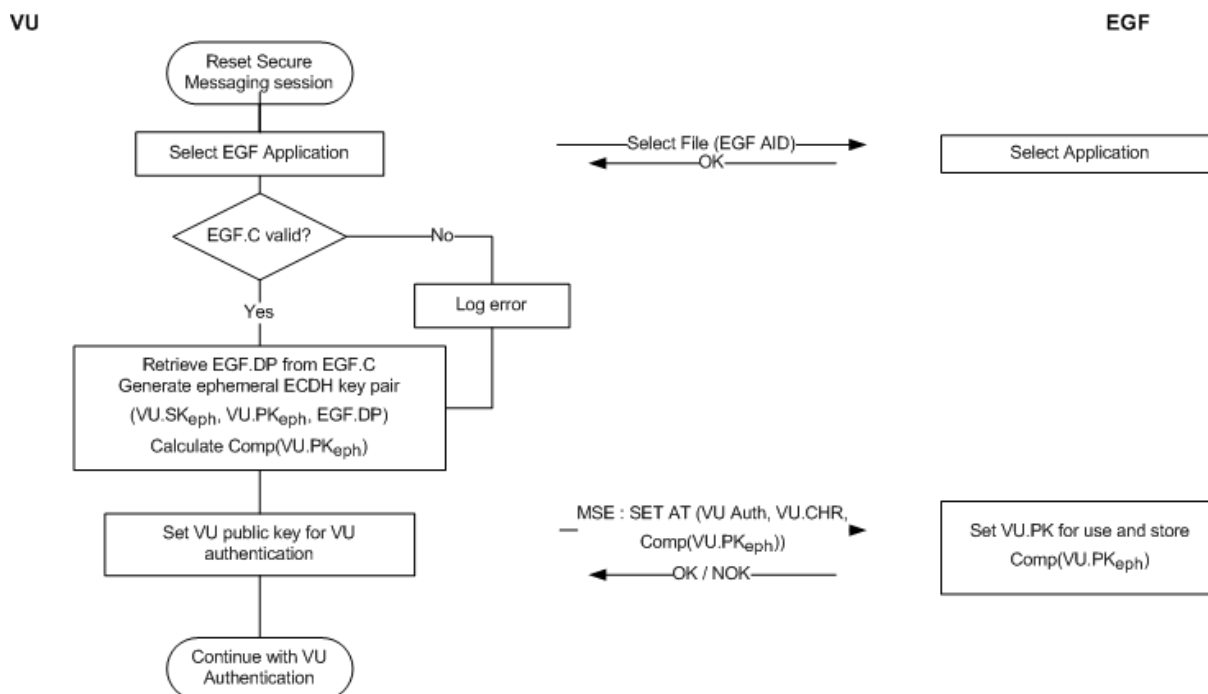
TCS\_352 Отклоняясь от требования TCS\_309, EGF использует время ГНСС для проверки временной действительности любого представленного сертификата.

TCS\_353 После проверки сертификата VU\_MA внешнее устройство ГНСС хранит этот сертификат для использования во время нормальной эксплуатации; см. раздел 11.3.3.

### 11.3.3 Во время нормальной эксплуатации

TCS\_354 Во время нормальной эксплуатации бортовое устройство и EGF используют протокол, описанный на Рисунок 11, для проверки временной действительности хранящихся сертификатов EGF\_MA и VU\_MA и определения открытого ключа VU\_MA для последующей аутентификации БУ. Во время нормальной эксплуатации никакой дальнейшей взаимной проверки цепочек сертификатов не проводится.

Следует отметить, что Рисунок 11 в целом состоит из первых этапов, отражённых на Рисунок 4 и Рисунок 5. Опять-таки следует иметь в виду, что EGF не является «умной» карточкой, и потому БУ, скорее всего, не передаст команду Reset для запуска связи и не получит ATR. В любом случае это не входит в область применения настоящего приложения.



**Рисунок 11** Взаимная проверка временной действительности сертификата во время нормальной эксплуатации БУ и EGF

TCS\_355 Как показано на Рисунок 11, бортовое устройство регистрирует ошибку, если сертификат EGF\_MA более недействителен. Однако взаимная аутентификация, согласование ключей и дальнейшая связь через механизм защищённого обмена сообщениями должны происходить, как обычно.

#### **11.4. Аутентификация БУ, аутентификация микросхемы и согласование сеансовых ключей**

TCS\_356 Аутентификация БУ, аутентификация микросхемы и согласование сеансовых ключей между БУ и EGF происходят во время соединения и во всех случаях, когда в условиях нормальной эксплуатации восстанавливается сеанс защищённого обмена сообщениями. БУ и EGF выполняют процессы, описанные в разделах 10.3 и 10.4. Выполняются все требования указанных разделов.

#### **11.5. Защищённый обмен сообщениями**

TCS\_357 Все команды и ответы, которыми обмениваются бортовое устройство и внешнее устройство ГНСС после успешной аутентификации микросхемы и до конца сеанса, защищены механизмом защищённого обмена сообщениями в режиме только аутентификации. Выполняются все требования раздела 10.5.

TCS\_358 Если сеанс защищённого обмена сообщениями между БУ и EGF прерван, БУ немедленно запускает новый сеанс защищённого 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

Бортовое устройство и датчик движения устанавливают связь при помощи протокола интерфейса, указанного в [ISO 16844-3], в рамках процесса соединения и в условиях нормальной эксплуатации, с учётом 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 присутствию на карточках мастерской до трёх ключей AES  $K_{M-wc}$  (последовательных поколений ключей), связанных с датчиком движения. Также и в датчиках движения может быть до трёх различных вариантов зашифрованных данных на базе AES (последовательных поколений ключа старшего порядка датчика движения  $K_M$ ). В бортовом устройстве есть только один ключ, связанный с датчиком движения,  $K_{M-vu}$ .

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, и БУ подсоединяется к датчику движения.
2. БУ считывает все имеющиеся ключи  $K_{M-wc}$  с карточки мастерской, проверяет номера их версий и выбирает один, соответствующий номеру версии ключа  $K_{M-vu}$  БУ. Если соответствующего ключа  $K_{M-wc}$  на карточке мастерской нет, БУ прерывает процесс соединения и показывает владельцу карточки мастерской соответствующее сообщение об ошибке.
3. БУ вычисляет ключ старшего порядка датчика движения  $K_M$  по  $K_{M-vu}$  и  $K_{M-wc}$ , а идентификационный ключ  $K_{ID}$  по  $K_M$ , как указано в разделе 9.2.1.
4. БУ передаёт указание начать процесс соединения на датчик движения, как описано в [ISO 16844-3], и шифрует серийный номер, который он получил от датчика движения, при помощи идентификационного ключа  $K_{ID}$ . БУ передаёт зашифрованный серийный номер обратно в датчик движения.
5. Датчик движения совмещает зашифрованный серийный номер последовательно с каждым зашифрованным серийным номером, который в нём хранится. Если соответствие найдено, происходит аутентификация БУ. Датчик движения отмечает поколение  $K_{ID}$ , используемого БУ, и возвращает соответствующую зашифрованную версию своего ключа соединения, т.е. Шифр, созданный при помощи того же поколения  $K_M$ .
6. БУ расшифровывает ключ соединения при помощи  $K_M$ , генерирует сеансовый ключ  $K_S$ , шифрует его при помощи ключа соединения и передаёт результат в 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 передаёт результат в датчик движения. Датчик движения расшифровывает информацию о соединении.
8. Датчик движения шифрует полученную информацию о соединении при помощи полученного  $K_S$  и возвращает её БУ. БУ проверяет, является ли информация о соединении той же информацией, которую БУ направил датчику движения на предыдущем этапе. Если да, это доказывает, что датчик движения использовал тот же  $K_S$ , что и БУ, и, соответственно, на этапе 5 передал свой ключ соединения, зашифрованный при помощи правильного поколения  $K_M$ . Так происходит аутентификация датчика движения.

Следует отметить, что этапы 2 и 5 отличаются от стандартного процесса в [ISO 16844-3]; остальные этапы стандартные.

Пример: Предположим, что соединение происходит в первый год действия сертификата ERCA (3); см. Рисунок 2 в разделе 9.2.1.2. Более того,

- Предположим, что датчик движения был выпущен в последний год срока действия сертификата ERCA (1). Таким образом, он будет содержать следующие ключи и данные:
  - $N_s[1]$ : свой серийный номер, зашифрованный при помощи первого поколения  $K_{ID}$ ,
  - $N_s[2]$ : свой серийный номер, зашифрованный при помощи второго поколения  $K_{ID}$ ,
  - $N_s[3]$ : свой серийный номер, зашифрованный при помощи третьего поколения  $K_{ID}$ ,
  - $K_P[1]$ : свой ключ соединения первого поколения<sup>12</sup>, зашифрованный при помощи первого поколения  $K_M$ ,
  - $K_P[2]$ : свой ключ соединения второго поколения, зашифрованный при помощи второго поколения  $K_M$ ,
  - $K_P[3]$ : свой ключ соединения третьего поколения, зашифрованный при помощи третьего поколения  $K_M$ ,
- Предположим, что карточка мастерской был выпущена в первый год срока действия сертификата ERCA (3). Таким образом, на ней будет содержаться второе и третье поколения ключа  $K_{M-WC}$ .
- Предположим, что БУ – это БУ второго поколения, в котором содержится второе поколение  $K_{M-VU}$ .

В этом случае на этапах 2-5 произойдёт следующее:

- Этап 2: БУ считывает второе и третье поколения  $K_{M-WC}$  с карточки мастерской и проверяет номера их версий.
- Этап 3: БУ комбинирует  $K_{M-WC}$  второго поколения со своим  $K_{M-VU}$ , чтобы 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 данные с  $N_s[2]$  и находит соответствие. Он делает вывод, что БУ представляет собой БУ второго поколения и передаёт обратно  $K_P[2]$ .

---

<sup>12</sup> Следует отметить, что ключи соединения первого, второго и третьего поколений фактически могут быть одним и тем же ключом, или это могут быть три разных ключа различной длины, как поясняется в TCS\_259.

### 12.3. Соединение и связь между БУ и датчиком движения с использованием AES

TCS\_361

Как указано в Таблица 45 в разделе 9.2.1, все ключи, участвующие 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 бит.

Поскольку размер блока AES составляет 16 байтов, длина зашифрованного сообщения должна быть кратной 16 байтам, по сравнению с 8 байтами TDES. Кроме того, некоторые из этих сообщений будут использоваться для передачи ключей AES, длина которых может быть 128, 192 или 256 бит. Таким образом, число байтов данных в одной инструкции в таблице 5 [ISO 16844-3] меняется, как показано в Таблица 48:

Инструкция	Запрос/ответ	Описание данных	Число байтов простого текста в соответствии с [ISO 16844-3]	Число байтов простого текста с использованием ключей AES	Число байтов зашифрованных данных с использованием ключей AES 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	16 / 32	16 / 32	16 / 32
41	запрос	Серийный номер MoS	8	8	16	16	16
41	ответ	Ключ соединения	16	16 / 24 / 32	16	32	32
42	запрос	Сеансовый ключ	16	16 / 24 / 32	16	32	32
43	запрос	Информация о соединении	24	24	32	32	32
50	ответ	Информация о соединении	24	24	32	32	32
70	запрос	Данные аутентификации	8	8	16	16	16
80	ответ	Значение счётчика MoS + данные аут.	8	8	16	16	16

Таблица 48 Число байтов простого текста и зашифрованных данных в одной инструкции в соответствии с [ISO 16844-3]

TCS\_362

Информация о соединении, передаваемая в инструкциях 43 (запрос БУ) и 50 (ответ MoS), собирается, как указано в разделе 7.6.10 [ISO 16844-3], за исключением того, что алгоритм AES используется вместо алгоритма TDES в схеме шифрования данных соединения, приводя таким образом к двум шифрованным вариантам AES и заполнению, отмеченному в TCS\_363, 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.

TCS\_363

Если длина простого текста (с использованием ключей AES) не кратна 16 байтам, применяется метод заполнения, представленный в [ISO 9797-1].

Примечание: в [ISO 16844-3] число байтов текстовых данных всегда кратно 8, так что при использовании TDES заполнение не является необходимым. Определение данных и сообщений в [ISO 16844-3] в данной части настоящего приложения не изменяется, что обуславливает необходимость применения заполнения.

TCS\_364

В инструкции 11 и в случае, когда необходимо зашифровать более одного блока данных, применяется режим сцепления криптоблоков, представленный в [ISO 10116], с параметром чередования  $m = 1$ . Используется IV

- Относительно инструкции 11: 8-байтовый блок аутентификации, указанный в разделе 7.6.3.3 [ISO 16844-3], заполненный при помощи метода заполнения 2, описанного в [ISO 9797-1]; также см. разделы 7.6.5 и 7.6.6 [ISO 16844-3].
- В случае всех других инструкций, в которых передаётся больше 16 байтов данных, как указано в Таблица 48: '00' {16}, т.е. шестнадцать байтов с двоичным значением, равным 0.

Примечание: Как показано в разделах 7.6.5 и 7.6.6 [ISO 16844-3], когда MoS шифрует файлы данных для их включения в инструкцию 11, блок аутентификации

- Используется как вектор инициализации для шифрования файлов данных в режиме CBC
- И зашифровывается и включается как первый блок в данные, передаваемые в БУ

## 12.4. Соединение БУ и датчика движения с использованием аппаратуры разных поколений

TCS\_365

Как поясняется в разделе 9.2.1, в датчике движения второго поколения может содержаться шифрование данных соединения на базе TDES (в соответствии с частью А настоящего приложения), что позволяет датчику движения соединяться с БУ первого поколения. В таком случае БУ первого поколения и датчик движения второго поколения соединяются, как описано в части А настоящего приложения и в [ISO 16844-3]. В процессе соединения может использоваться карточка мастерской первого или второго поколения.

Примечания:

- БУ второго поколения невозможно соединить с датчиком движения первого поколения.
- Карточку мастерской первого поколения невозможно использовать для соединения БУ второго поколения с датчиком движения.

## 13. Защита удалённой связи через DSRC

### 13.1. Общие положения

Как указано в приложении 14, БУ регулярно генерирует данные удалённого контроля тахографа (RTM) и передаёт их в (внутреннее или внешнее) устройство удалённой связи (RCF). Устройство удалённой связи отвечает за передачу таких данных через интерфейс DSRC, описанный в приложении 14, средству удалённого контроля. В приложении 1 указано, что данные RTM представляют собой конкатенацию:

- **Зашифрованных данных тахографа** зашифрованных текстовых данных тахографа
- **Данных безопасности DSRC** описано ниже

Текстовый формат данных тахографа представлен в приложении 1 и более подробно описан в приложении 14. В разделе описана структура данных безопасности DSRC; официальная спецификация содержится в приложении 1.

TCS\_366

Текстовые данные `tachographPayload`, передаваемые БУ на средство удалённой связи (если RCF является внешним по отношению БУ) или из БУ на средство удалённого контроля через интерфейс DSRC (если RCF является внешним по отношению к БУ), защищаются в режиме шифрования с последующей аутентификацией, т.е. данные тахографа сначала шифруются, чтобы обеспечить конфиденциальность сообщения, а затем для обеспечения подлинности и целостности данных вычисляется MAC.

- TCS\_367 Данные безопасности DSRC состоят из конкатенации следующих элементов данных в следующем порядке; см. также Рисунок 12:
- **Текущие дата и время** текущие дата и время БУ (тип данных TimeReal)
  - **Счётчик** 3-байтовый счётчик, см. TCS\_368
  - **Серийный номер БУ** серийный номер БУ (тип данных VuSerialNumber)
  - **Номер версии ключа старшего порядка DSRC** 1-байтовый номер версии ключа старшего порядка DSRC, на основе которого составляются ключи DSRC, связанные с БУ, см. раздел 9.2.2.
  - **MAC** значение MAC, вычисляемое по всем прежним байтам в данных RTM.

- TCS\_368 3-байтовый счётчик в данных безопасности DSRC представлен в формате изначальных MSB. В первый раз когда БУ вычисляет набор данных RTM после начала их производства, значение счётчика устанавливается на 0. Каждый раз перед вычислением следующего набора данных RTM БУ увеличивает значение данных счётчика на 1.

### 13.2. Шифрование данных тахографа и генерирование MAC

- TCS\_369 С учётом элемента текстовых данных с типом данных TachographPayload, как описано в приложении 14, БУ шифрует эти данные, как показано на Рисунок 12: ключ DSRC БУ для шифрования  $K_{VU_{DSRC\_ENC}}$  (см. раздел 9.2.2) используется с AES в режиме сцепления криптоблоков (CBC), как описано в [ISO 10116], с параметром чередования  $m = 1$ . Вектор инициализации равен  $IV = \text{текущие дата и время} \parallel '00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00' \parallel \text{счётчик}$ , где *текущие дата и время* и *счётчик* описаны в TCS\_367. Данные, подлежащие шифрованию, заполняются по методу 2, представленному в [ISO 9797-1].
- TCS\_370 БУ вычисляет MAC в данных безопасности DSRC, как показано на Рисунок 12: MAC вычисляется по всем прежним байтам в данных RTM, до номера версии ключа старшего порядка DSRC включительно, включая также метки и длины объектов данных. БУ использует свой ключ DSRC для аутентификации  $K_{VU_{DSRC\_MAC}}$  (см. раздел 9.2.2) при помощи алгоритма AES в режиме CMAC, как указано в [SP 800-38B]. Длина MAC связана с длиной ключей DSRC, связанных с БУ, как описано в TCS\_192.

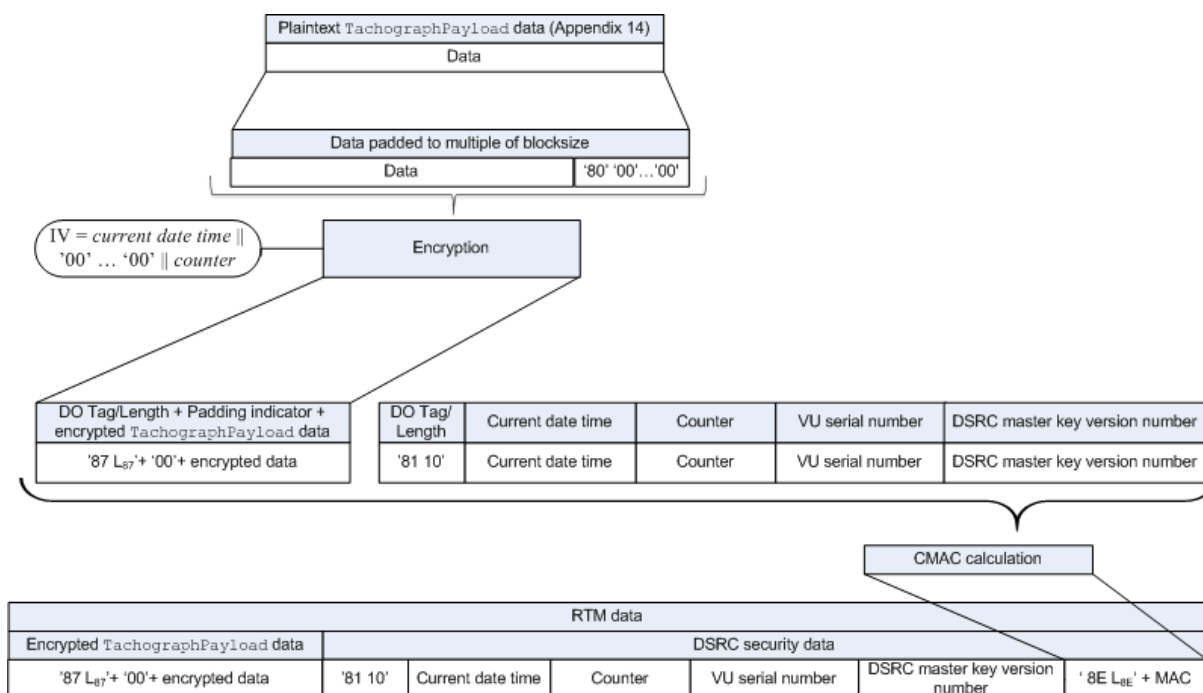


Рисунок 12 Шифрование данных тахографа и генерирование MAC

### 13.3. Проверка и расшифровка данных тахографа

Когда средство удалённого контроля получает из БУ данные RTM, оно передаёт все данные RTM на контрольную карточку в поле данных команды PROCESS DSRC MESSAGE, как описано в приложении 2. Затем:

1. Контрольная карточка проверяет номер версии ключа старшего порядка DSRC в данных безопасности DSRC. Если контрольной карточке указан ключ старшего порядка DSRC неизвестен, она возвращает ошибку, указанную в приложении 2, и прекращает процесс.
2. Контрольная карточка использует указанный ключ старшего порядка DSRC в сочетании с серийным номером БУ в данных безопасности DSRC, чтобы получить ключи DSRC, связанные с БУ, K\_VU<sub>DSRC\_ENC</sub> и K\_VU<sub>DSRC\_MAC</sub>, как указано в TCS\_266.
3. Контрольная карточка использует K\_VU<sub>DSRC\_MAC</sub> для проверки MAC в данных безопасности DSRC, как указано в TCS\_370. Если значение MAC неверно, контрольная карточка возвращает ошибку, указанную в приложении 2, и прекращает процесс.
4. Контрольная карточка использует K\_VU<sub>DSRC\_ENC</sub> для расшифровки зашифрованных данных тахографа, как указано в TCS\_369. Контрольная карточка убирает заполнение и возвращает расшифрованные данные тахографа средству удалённого контроля.

Для предотвращения повторных атак средство удалённого контроля проверяет свежесть данных RTM, проверяя, чтобы *текущие дата и время* в данных безопасности DSRC слишком существенно не отклонялись от текущего времени средства удалённого контроля.

Примечания:

- Для этого средству удалённого контроля нужен точный и надёжный источник времени.
- Поскольку согласно приложению 14 БУ должно вычислять новый набор данных RTM каждые 60 секунд и часы БУ могут отклоняться от реального времени на 1 минуту, нижний предел свежести данных RTM составляет 2 минуты. Фактическая требуемая свежесть также зависит от точности часов средства удалённого контроля.

TCS\_373 Когда мастерская проверяет правильное функционирование DSRC БУ, она передаёт все данные RTM, полученные из БУ, на карточку мастерской в поле данных команды PROCESS DSRC MESSAGE, как описано в приложении 2. Карточка мастерской выполняет все проверки и действия, указанные в TCS\_371.

#### 14. Подписание загружаемых данных и проверка подписей

##### 14.1. Общие положения

TCS\_374 Данные, полученные из БУ или с карточки за один сеанс загрузки, сохраняются специализированной программируемой аппаратурой (СПА) в виде одного физического файла данных. Данные могут храниться на внешнем носителе. Файл содержит цифровые подписи блоков данных в соответствии с указанными в приложении 7. Файл также содержит следующие сертификаты (см. раздел 9.1):

- При загрузке из БУ:
  - o VU\_Sign certificate
  - o Сертификат MSCA\_VU-EGF, содержащий открытый ключ для проверки сертификата VU\_Sign
- При загрузке с карточки:
  - o Сертификат Card\_Sign
  - o Сертификат MSCA\_Card, содержащий открытый ключ для проверки сертификата Card\_Sign

TCS\_375 СПА также располагает следующими средствами.

- Если для проверки подписи используется контрольная карточка, как описано на Рисунок 13: Связующий сертификат, объединяющий последний сертификат EUR с сертификатом EUR, период действительности которого непосредственно ему предшествует, если таковые существуют.
- Если проверяется сама подпись: все действительные европейские корневые сертификаты.

Примечание: метод, используемый СПА для извлечения этих сертификатов, в настоящем приложении не указывается.

##### 14.2. Генерирование подписей

TCS\_376 Алгоритм подписания для создания цифровых подписей загружаемых данных – ECDSA, как указано в [DSS], с использованием алгоритма хеширования, связанного с размером ключа БУ или карточки, как указано в TCS\_192. Формат подписи простой, как указано в [TR-03111].

##### 14.3. Проверка подписей

TCS\_377 СПА может проверять подпись загружаемых данных самостоятельно или использовать для этого контрольную карточку. Если используется контрольная карточка, проверка подписи происходит так, как описано на Рисунок 13. Если СПА проводит проверку подписи самостоятельно, проверяются подлинность и действительность всех сертификатов в цепочке сертификатов в файле данных, а также подпись данных по схеме подписи, представленной в [DSS].

Примечания к Рисунок 13:

- Аппаратура, с помощью которой были подписаны подлежащие анализу данные, обозначена буквами EQT.
- Сертификаты EQT и открытые ключи, указанные на рисунке, предназначены для подписания сертификатов VU\_Sign или Card\_Sign.
- Сертификаты EQT.CA и открытые ключи, указанные на рисунке, предназначены для подписания сертификатов БУ или карточек соответственно.
- Сертификат EQT.CA.EUR, указанный на рисунке – это европейский корневой сертификат, отмеченный в CAR сертификата EQT.CA.
- Сертификат EQT.Link, указанный на рисунке, – это связующий сертификат EQT, если он имеется. Как указано в разделе 9.1.2, это связующий сертификат для новой пары европейских корневых ключей, созданной ERCA и подписанной прежним европейским закрытым ключом.

- Сертификат EQT.Link.EUR – это европейский корневой сертификат, отмеченный в CAR сертификата EQT.Link.

TCS\_378 Для вычисления хеша М, передаваемого контрольной карточке в команде PSO:Hash, СПА использует алгоритм хеширования, связанного с размером ключа БУ или карточки, с которых загружаются данные, как указано в TCS\_192.

TCS\_379 Для проверки подписи EQT контрольная карточка применяет схему подписи, представленную в [DSS].

Примечание: В настоящем документе не указываются конкретные действия, которые следует предпринимать, если подпись файла загружаемых данных невозможно проверить или если проверка была неудачной.



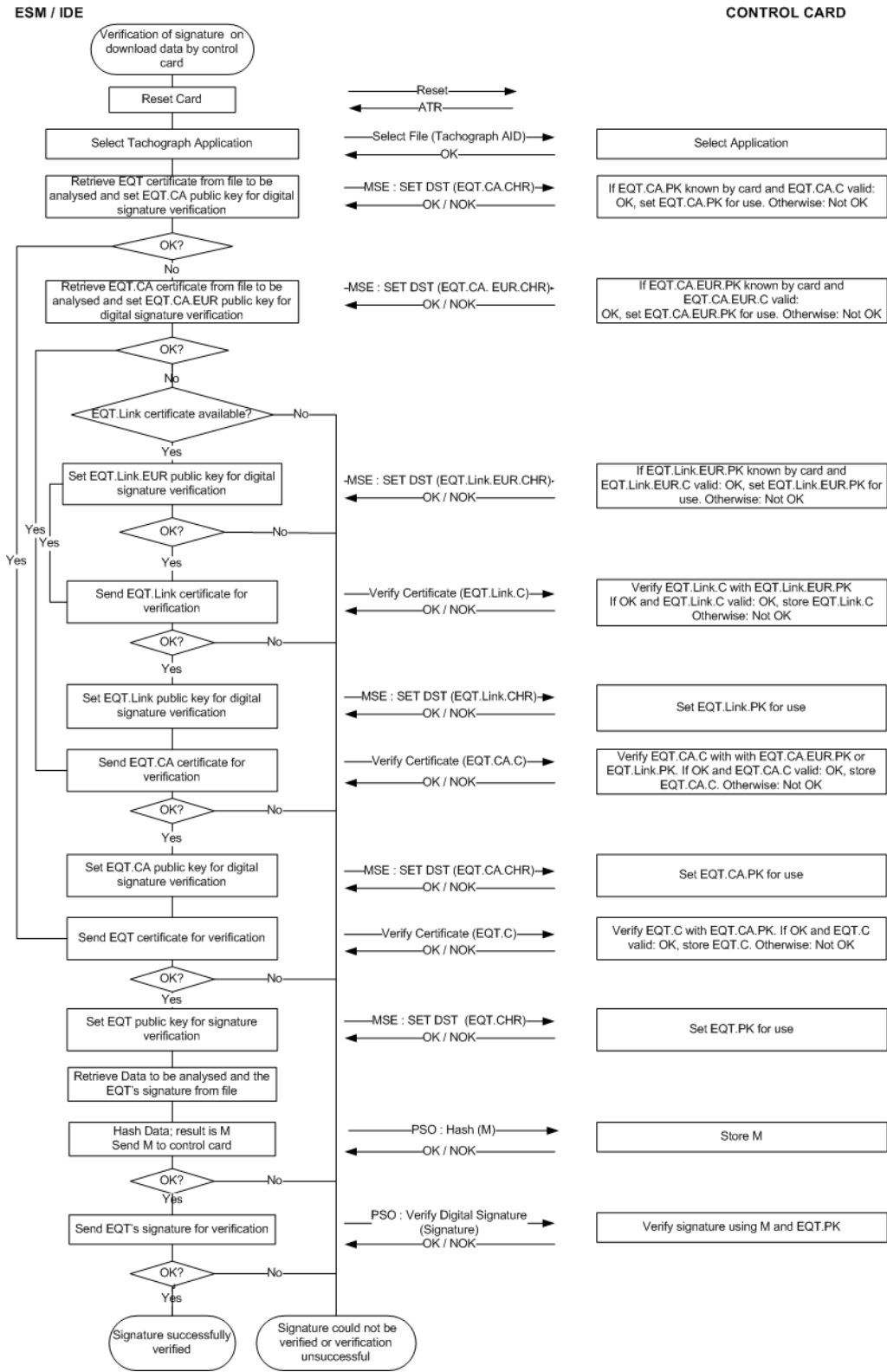


Рисунок 13 Протокол проверки подписи файла загружаемых данных

## Приложение 12. Определение местоположения при помощи глобальной навигационной спутниковой системы (ГНСС)

### СОДЕРЖАНИЕ

<b>ПРИЛОЖЕНИЕ 12. ОПРЕДЕЛЕНИЕ МЕСТОПОЛОЖЕНИЯ ПРИ ПОМОЩИ ГЛОБАЛЬНОЙ НАВИГАЦИОННОЙ СПУТНИКОВОЙ СИСТЕМЫ (ГНСС) .....</b>	<b>438</b>
<b>1. ВВЕДЕНИЕ .....</b>	<b>439</b>
<b>1.1. Область применения.....</b>	<b>439</b>
<b>1.2. Сокращения и обозначения.....</b>	<b>440</b>
<b>2. СПЕЦИФИКАЦИЯ ПРИЁМНИКА ГНСС .....</b>	<b>440</b>
<b>3. ПРЕДЛОЖЕНИЯ NMEA .....</b>	<b>440</b>
<b>4. БОРТОВОЕ УСТРОЙСТВО С ВНЕШНИМ УСТРОЙСТВОМ ГНСС .....</b>	<b>442</b>
<b>4.1. Конфигурация.....</b>	<b>442</b>
4.1.1 Основные компоненты и интерфейсы .....	442
4.1.2 Состояние внешнего устройства ГНСС в конце процесса производства .....	443
<b>4.2. Связь между внешним устройством ГНСС и бортовым устройством .....</b>	<b>443</b>
4.2.1 Протокол передачи данных.....	443
4.2.2 Защищённая передача данных ГНСС .....	445
4.2.3 Структура команды Read Record.....	446
<b>4.3. Соединение, взаимная аутентификация и согласование сеансовых ключей между внешним устройством ГНСС и бортовым устройством .....</b>	<b>447</b>
<b>4.4. Обработка ошибок .....</b>	<b>447</b>
4.4.1 Ошибка связи с внешним устройством ГНСС .....	448
4.4.2 Нарушение физической целостности внешнего устройства ГНСС .....	448
4.4.3 Отсутствие информации о местоположении из приёмника ГНСС .....	448
4.4.4 Истёкший срок действия сертификата внешнего устройства ГНСС .....	448
<b>5. БОРТОВОЕ УСТРОЙСТВО БЕЗ ВНЕШНЕГО УСТРОЙСТВА ГНСС .....</b>	<b>449</b>
<b>5.1. Конфигурация.....</b>	<b>449</b>
<b>5.2. Обработка ошибок .....</b>	<b>449</b>
5.2.1 Отсутствие информации о местоположении из приёмника ГНСС .....	449
<b>6. НЕСТЫКОВКА ВО ВРЕМЕНИ ГНСС.....</b>	<b>449</b>
<b>7. ПРОТИВОРЕЧИВЫЕ ДАННЫЕ О ДВИЖЕНИИ ТРАНСПОРТНОГО СРЕДСТВА .....</b>	<b>449</b>

## 1. Введение

Настоящее приложение устанавливает технические требования к данным ГНСС, используемым бортовым устройством, включая протоколы, которые должны быть реализованы для обеспечения защищённой и правильной передачи данных информации о местоположении.

Основные статьи Регламента (ЕС) № 165/2014, на которые опираются данные требования: статья 8 «Регистрация местоположения транспортного средства в определённых точках в течение дневного периода работы», статья 10 «Интерфейс с интеллектуальными транспортными системами» и статья 11 «Подробные положения об «умных» тахографах».

### 1.1. Область применения

GNS\_1

Бортовое устройство собирает данные о местоположении хотя бы из одной ГНСС с целью выполнения требований статьи 8.

Бортовое устройство может быть или не быть оснащено внешним устройством ГНСС, как показано на Рисунок 14:

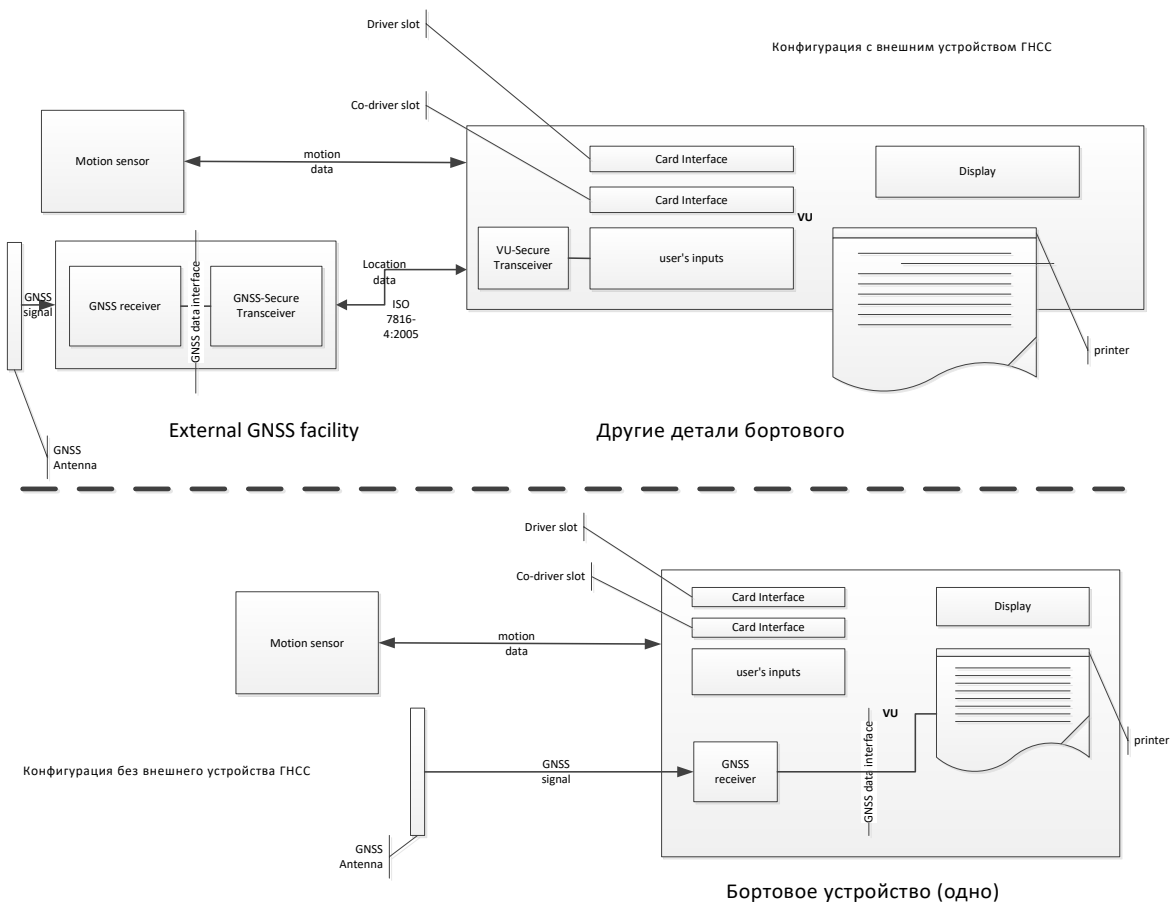


Рисунок 14. Различные конфигурации приёмника ГНСС.

## 1.2. Сокращения и обозначения

В настоящем приложении используются следующие сокращения:

DOP Показатель снижения точности  
 EGF Элементарный файл устройства ГНСС  
 EGNOS Европейская геостационарная служба навигационного покрытия  
 GNSS Глобальная навигационная спутниковая система  
 GSA GPS DOP и активные спутники  
 HDOP Горизонтальный показатель снижения точности  
 ICD Документ по контролю интерфейса  
 NMEA Национальная ассоциация морской электроники  
 PDOP Показатель снижения точности определения положения в пространстве  
 RMC Рекомендуемый конкретный минимальный уровень  
 SIS Сигнал в пространстве  
 VDOP Вертикальный показатель снижения точности  
 VU (БУ) Бортовое устройство

## 2. Спецификация приёмника ГНСС

Вне зависимости от конфигурации «умного» тахографа с внешним устройством ГНСС или без него, предоставление точной и надёжной информации о местоположении является ключевым элементом эффективной эксплуатации «умных» 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 Совета<sup>13</sup>. 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 Производители обеспечивают совместимость приёмников ГНСС в «умных» тахографах с услугами определения местоположения, предоставляемыми системами «Галилей» и EGNOS. Производители также могут дополнительно выбирать совместимость с другими спутниковыми навигационными системами.

GNS\_3 Приёмник ГНСС способен поддерживать аутентификацию при помощи открытой услуги «Галилей», если система «Галилей» предоставляет такую услугу и если она поддерживается производителями приёмников ГНСС. Однако в отношении «умных» тахографов, поставляемых на рынок до удовлетворения прежних условий и не способных поддерживать аутентификацию при помощи открытой услуги «Галилей», переоснащение проводить не придётся.

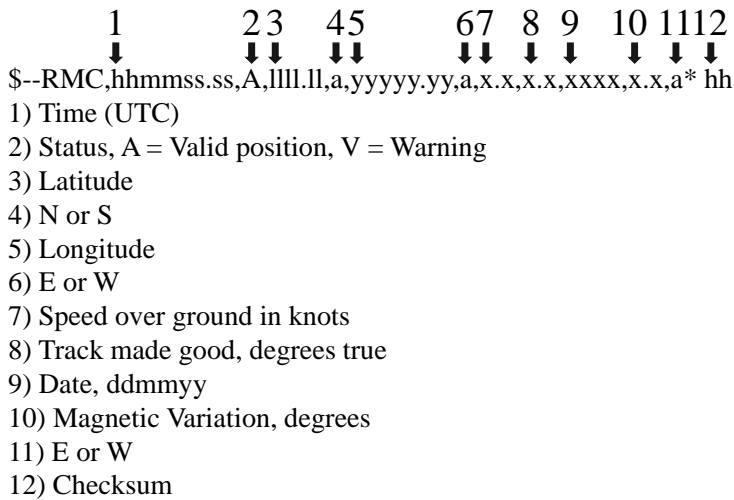
## 3. Предложения NMEA

Данный раздел описывает фразы NMEA, используемые для функционирования «умного» тахографа. Данный раздел актуален для обеих конфигураций «умного» тахографа: с внешним устройством ГНСС или без него.

GNS\_4 Данные о местоположении опираются на рекомендуемый конкретный минимальный уровень (RMC) данных ГНСС в фразе NMEA, в которых содержится информация о местоположении (широта, долгота), время в формате UTC (hhmmss.ss) и скорость относительно грунта в узлах плюс дополнительные значения.

Формат фразы RMC выглядит так (по стандарту NMEA V4.1):

<sup>13</sup> Регламент (ЕС) № 1285/2013 Европейского парламента и Совета от 11 декабря 2013 г. о внедрении и эксплуатации европейских спутниковых навигационных систем, отменяющий Регламент Совета (ЕС) № 876/2002 и Регламент (ЕС) № 683/2008 Европейского парламента и Совета (ОЖ L 347, 20.12.2013, стр. 1).



**Рисунок 15. Структура фразы RMC**

Статус указывает, имеется ли сигнал ГНСС. Пока значение статуса не установлено на А, получаемые данные (например, время или широта/долгота) не могут использоваться для регистрации местоположения транспортного средства в БУ.

Разрешение местоположения представлено в формате описанной выше фразы RMC. Первая часть полей 3 и 5 (первые два числа) используется для отражения градусов. Остальная часть используется для выражения минут с тремя десятичными знаками. Таким образом, разрешение составляет 1/1000 минуты или 1/60000 градуса (поскольку одна минута – это 1/60 градуса).

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 1 для типа геокоординат.

БУ может использовать команду GPS DOP и активных спутников (GSA) для определения и регистрации наличия и точности сигнала. В частности, для указания на уровень точности записанных данных о местоположении используется HDOP (см. 4.2.2). БУ хранит значение горизонтального показателя снижения точности (HDOP), вычисляемого как минимум значений HDOP, собранных со всех имеющихся ГНСС.

ИД ГНСС указывает на GPS, Glonass, Galileo, Beidou или спутниковые системы функционального дополнения (SBAS).

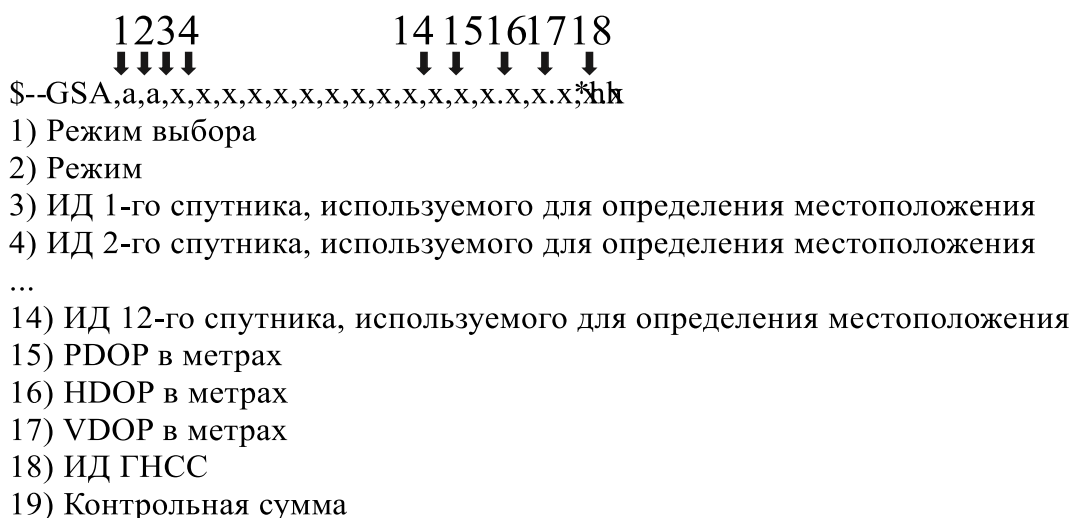


Рисунок 16. Структура фразы GSA

Если режим (2) указывает, что местоположение не определено (режим = 1) или что местоположение определено в 2D (режим = 2) или 3D (режим = 3).

GNS\_6 Предложение GSA хранится под номером записи '06'.

GNS\_7 Максимальный размер фраз NMEA (например, RMC, GSA или других), который можно использовать для определения размера команды записи, составляет 85 байтов (см. Таблица 49).

#### 4. Бортовое устройство с внешним устройством ГНСС

##### 4.1. Конфигурация

###### 4.1.1 Основные компоненты и интерфейсы

В данной конфигурации приёмник ГНСС представляет собой часть внешнего устройства ГНСС.

GNS\_8 Внешнее устройство ГНСС должно обеспечиваться питанием через специальный интерфейс с транспортным средством.

GNS\_9 Внешнее устройство ГНСС состоит из следующих компонентов (см. Рисунок 17):

- а) Коммерческий приёмник ГНСС, поставляющий данные о местоположении через интерфейс данных ГНСС. Например, интерфейс данных ГНСС может соответствовать стандарту NMEA V4.10, когда приёмник ГНСС работает как рация и передаёт фразы NMEA на безопасный трансивер ГНСС с частотой 1 Гц для predetermined фраз NMEA, в которые должны быть включены хотя бы фразы RMC и GSA. Реализация интерфейса данных ГНСС зависит от выбора производителей внешнего устройства ГНСС.
- б) Блок трансивера (безопасный трансивер ГНСС), способный поддерживать стандарт ISO/IEC 7816-4:2013 (см. 4.2.1) для связи с бортовым устройством и поддержки интерфейса данных ГНСС с приёмником ГНСС. Блок оснащён памятью для хранения идентификационных данных приёмника ГНСС и внешним устройством ГНСС.

- c) Системный шкаф с функцией обнаружения взлома, вмещающий и приёмник ГНСС, и безопасный трансивер ГНСС. Функция обнаружения взлома реализует меры обеспечения безопасности, требуемые в соответствии с характеристиками защиты «умного» тахографа.
- d) Антенна ГНСС, установленная на транспортном средстве и соединённая с приёмником ГНСС через системный шкаф.

GNS\_10 Внешнее устройство ГНСС снабжено, по крайней мере, 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 безопасный трансивер БУ представляет собой другой конец защищённой связи с безопасным трансивером ГНСС и должен поддерживать ISO/IEC 7816-4:2013 для связи с внешним устройством ГНСС.

GNS\_12 Для физического уровня связи с внешним устройством ГНСС бортовое устройство поддерживает ISO/IEC 7816-12:2005 или другой стандарт, способный поддерживать ISO/IEC 7816-4:2013. (см. 4.2.1).

#### **4.1.2 Состояние внешнего устройства ГНСС в конце процесса производства**

GNS\_13 На момент выпуска с завода внешнее устройство ГНСС хранит следующие значения 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 передачи данных**

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.

- GNS\_15 Протокол передачи данных опирается на стандарт ISO/IEC 7816-4:2013, причём безопасный трансивер БУ играет роль ведущего, а безопасный трансивер ГНСС – роль ведомого. Физическая связь между внешним устройством ГНСС и бортовым устройством опирается на ISO/IEC 7816-12:2005 или другой стандарт, способный поддерживать 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 (и \*-4:2013, и \*-12:2005) между внешним устройством ГНСС и БУ устанавливается как T = 1.
- GNS\_18 Что касается функций 1) сбора и рассылки данных ГНСС и 2) сбора данных конфигурации внешнего устройства ГНСС и 3) протокола управления, безопасный трансивер ГНСС имитирует «умную» карточку с архитектурой файловой системы, включающей в себя главный файл (MF), справочный файл (DF) с идентификатором приложения, указанным в приложении 1, глава 6.2 (' FF 44 54 45 47 4D') и с 3 EF, содержащими сертификаты и одним элементарным файлом (EF.EGF) с идентификатором файла, равным '2F2F', как описано в Таблица 49.
- GNS\_19 Безопасный трансивер ГНСС хранит данные, поступающие из приёмника ГНСС, и конфигурацию в EF.EGF. Это линейный файл с записями переменной длины, идентификатор которого в шестнадцатеричном формате равен '2F2F'.
- GNS\_20 Безопасный трансивер ГНСС использует блок памяти для хранения данных, способный проводить не менее 20 миллионов циклов записи/считывания. Помимо данного аспекта, внутренний дизайн и внедрение безопасного трансивера ГНСС остаются на усмотрение производителей.
- Структура числа записей и данных представлена в Таблица 49. Следует отметить, что есть четыре фразы GSA для четырёх спутниковых систем и спутниковой системы функционального дополнения (SBAS).
- GNS\_21 Структура файла представлена в Таблица 49. Условия доступа (ALW, NEV, SM-MAC) см. в приложении 2, глава 3.5.

Таблица 49. Структура файла

Файл	ИД файла	Условия доступа		
		Read	Update	Зашифровано
MF	3F00			
EF.ICC	0002	ALW	NEV (БУ)	Нет
DF устройства ГНСС	0501	ALW	NEV	Нет
EF EGF MACertificate	C100	ALW	NEV	Нет
EF CA Certificate	C108	ALW	NEV	Нет
EF Link Certificate	C109	ALW	NEV	Нет
EF.EGF	2F2F	SM-MAC	NEV (БУ)	Нет

Файл/Элемент данных	Число записей	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				
Фраза RMC NMEA	'01'	85	85	
1-я фраза GSA NMEA	'02'	85	85	
2-я фраза GSA NMEA	'03'	85	85	
3-я фраза GSA NMEA	'04'	85	85	
4-я фраза GSA NMEA	'05'	85	85	
5-я фраза GSA NMEA	'06'	85	85	
Расширенный серийный номер внешнего устройства ГНСС, указанный в приложении 1 как SensorGNSSSerialNumber.	'07'	8	8	
Идентификатор операционной системы ГНСС Безопасный трансивер, указанный в приложении 1 как SensorOSIdentifier.	'08'	2	2	
Номер утверждения типа внешнего устройства ГНСС, указанный в приложении как SensorExternalGNSSApproval Number.	'09'	16	16	
Идентификатор компонента защиты внешнего устройства ГНСС, указанный в приложении 1 как SensorExternalGNSSIdentifier	'10'	8	8	
RFU – зарезервировано для будущего пользования	От '11' до 'FD'			

#### 4.2.2 Защищённая передача данных ГНСС

GNS\_22 Защищённая передача данных ГНСС о местоположении возможна только на следующих условиях:

1. Процесс соединения завершён, как описано в приложении 11. Общие механизмы защиты

2. Периодическая взаимная аутентификация и согласование сеансовых ключей между БУ и внешним устройством ГНСС, также описанные в приложении 11. Общие механизмы защиты реализуются с указанной частотой.

GNS\_23 Каждые T секунд, где T – это значение, меньше или равное 10, если не происходит соединение или взаимная аутентификация и согласование сеансовых ключей, БУ из внешнего устройства ГНСС запрашивает информацию о местоположении в соответствии со следующей последовательностью:

1. БУ запрашивает данные о местоположении из внешнего устройства ГНСС вместе с данными о показателе снижения точности (из фразы GSA NMEA). Безопасный трансивер БУ использует команду SELECT и READ RECORD(S) согласно ISO/IEC 7816-4:2013 в рамках защищённого обмена сообщениями в режиме только аутентификации, как описано в приложении 11, раздел 11.5, с идентификатором файла “2F2F” и значением RECORD, равным “01”, для фразы RMC NMEA и ‘02’, ‘03’, ‘04’, ‘05’, ‘06’ для фразы GSA NMEA.
2. Полученные данные о последнем местоположении хранятся в EF с идентификатором ‘2F2F’ и записями, описанными в Таблица 49, в безопасном трансивере ГНСС, учитывая, что безопасный трансивер ГНСС получает данные NMEA с частотой не менее 1 Гц из приёмника ГНСС через интерфейс данных ГНСС.
3. Безопасный трансивер ГНСС передаёт ответ в безопасный трансивер БУ при помощи сообщения ответа APDU через защищённый обмен сообщениями в режиме только аутентификации, как описано в приложении 11, раздел 11.5.
4. Безопасный трансивер БУ проверяет подлинность 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 фразы RMC NMEA. Фраза RMC NMEA включает в себя информацию, если местоположение действительно. Если местоположение недействительно, данные о нём остаются недоступными и не могут использоваться для регистрации местоположения транспортного средства. Если местоположение действительно, процессор БУ также извлекает значения HDOP из фраз GSA NMEA и вычисляет среднее значение по имеющимся спутниковым системам (т.е. когда местоположение зафиксировано).
6. Процессор БУ хранит полученную и обработанную информацию, такую как широта, долгота, время и скорость, в БУ в формате, указанном в словаре данных в приложении 1 как геокоординаты, вместе со значением HDOP, вычисляемым как минимальное значение HDOP из всех значений, собранных с помощью имеющихся ГНСС.

### 4.2.3 Структура команды Read Record

В настоящем разделе подробно описана структура команды Read Record. Также обеспечивается защищённый обмен сообщениями (в режиме только аутентификации), как описано в приложении 11 «Общие механизмы безопасности».

GNS\_24 Команда поддерживает защищённый обмен сообщениями в режиме только аутентификации, см. приложение 11.

GNS\_25 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'0Ch'	Требуется защищённый обмен сообщениями.
INS	1	'B2h'	Read Record
P1	1	'XXh'	Число записей ('00' указывает на текущую запись)
P2	1	'04h'	Считывание записи с номером записи, указанным в P1
Le	1	'XXh'	Ожидаемая длина данных. Число байтов, подлежащих извлечению.

GNS\_26 Запись, указанная в P1, становится текущей записью.

Байт	Длина	Значение	Описание
#1-#X	X	'XX..XXh'	Прочитанные данные
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, безопасный трансивер ГНСС выдаёт '9000'.
- Если текущий файл не имеет доступа к записям, безопасный трансивер ГНСС выдаёт '6981'.
- Если команда используется с P1 = '00', но текущего EF нет, безопасный трансивер ГНСС выдаёт '6986' (команда не разрешена).
- Если запись не найдена, безопасный трансивер ГНСС выдаёт '6A 83'.
- Если внешнее устройство ГНСС обнаружило взлом, оно выдаёт характеристику статуса '66 90'.

GNS\_27 Безопасный трансивер ГНСС поддерживает следующие команды тахографа второго поколения, указанные в приложении 2:

Команда	Ссылка
Select	Приложение 2, глава 3.5.1
Read Binary	Приложение 2, глава 3.5.2
Get Challenge	Приложение 2, глава 3.5.4
PSO: Verify Certificate	Приложение 2, глава 3.5.7
External Authenticate	Приложение 2, глава 3.5.9
General Authenticate	Приложение 2, глава 3.5.10
MSE:SET	Приложение 2, 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 11. Общие механизмы защиты, глава 11.

### **4.4. Обработка ошибок**

В настоящем разделе описывается, как внешним устройством ГНСС обрабатываются возможные условия ошибок и как они записываются в БУ.

#### 4.4.1 Ошибка связи с внешним устройством ГНСС

GNS\_28 Если БУ не может связаться с соединённым с ним внешним устройством ГНСС в течение более чем 20 минут подряд, БУ генерирует и регистрирует событие типа EventFaultType со значением enum '53'Н *Ошибка связи с внешним устройством ГНСС* и указанием времени относительно текущего. Событие генерируется, только если выполнены два следующих условия: а) «умный» тахограф не находится в режиме калибровки и б) транспортное средство движется. В данном контексте ошибка связи инициируется, когда безопасный трансивер БУ не получает ответного сообщения на сообщение запроса, как описано в 4.2.

#### 4.4.2 Нарушение физической целостности внешнего устройства ГНСС

GNS\_29 Если внешнее устройство ГНСС взломано, безопасный трансивер ГНСС стирает всю свою память, включая криптографические материалы. Как описано в GNS\_25 и GNS\_26, БУ обнаруживает взлом, если статус ответа '6690'. Затем БУ генерирует событие типа EventFaultType enum '55'Н *Обнаружение взлома ГНСС*.

#### 4.4.3 Отсутствие информации о местоположении из приёмника ГНСС

GNS\_30 Если безопасный трансивер ГНСС не получает данные из приёмника ГНСС в течение более чем 3 часов подряд, безопасный трансивер ГНСС генерирует ответное сообщение на команду READ RECORD с номером RECORD, равным '01', и 12-байтовым полем данных, установленным как 0xFF. По получении ответного сообщения с таким значением поля данных БУ генерирует и регистрирует событие типа EventFaultType enum '52'Н *Ошибка внешнего устройства ГНСС* 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 Истёкший срок действия сертификата внешнего устройства ГНСС

GNS\_31 Если БУ обнаруживает, что сертификат EGF, используемый для взаимной аутентификации, уже не действителен, БУ генерирует и регистрирует ошибку записывающего оборудования typeEventFaultType enum '56'Н *Истёкший срок действия сертификата внешнего устройства ГНСС* с указанием времени, равным текущему значению времени. БУ всё ещё использует полученные данные ГНСС о местоположении.

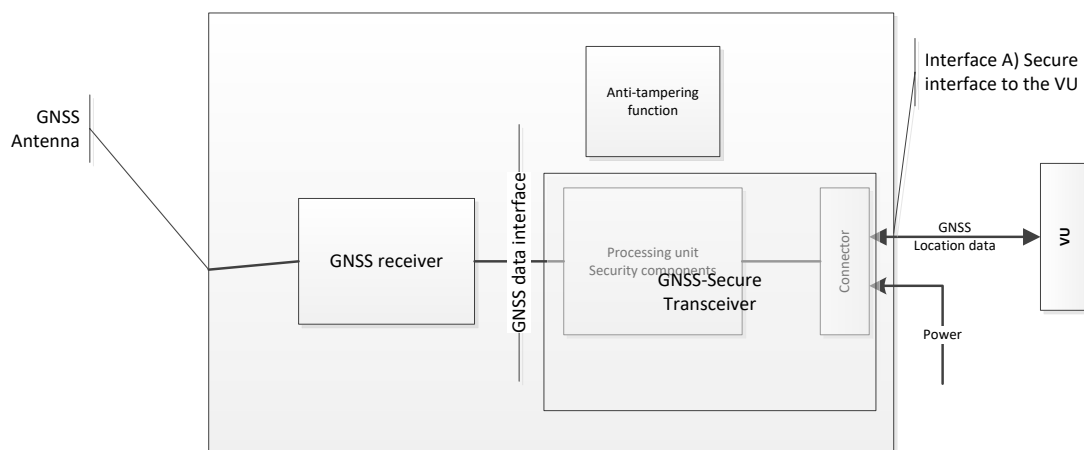


Рисунок 17. Схема внешнего устройства ГНСС

## 5. Бортовое устройство без внешнего устройства ГНСС

### 5.1. Конфигурация

В данной конфигурации приёмник ГНСС находится внутри бортового устройства, как описано на Рисунок 14.

GNS\_32 Приёмник ГНСС работает как рация и передаёт фразы NMEA в процессор БУ, который принимает их с частотой 1/10 или больше Гц в случае predetermined набора фраз NMEA, в который входят хотя бы фразы RMC и GSA.

GNS\_33 К БУ подсоединена внешняя антенна ГНСС, установленная на транспортном средстве, или внутренняя антенна ГНСС.

### 5.2. Обработка ошибок

#### 5.2.1 Отсутствие информации о местоположении из приёмника ГНСС

GNS\_34 Если БУ не получает данные из приёмника ГНСС в течение более 3 часов подряд, оно генерирует и регистрирует событие типа EventFaultType enum '51'Н *Ошибка внутреннего приёмника ГНСС* 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.

## 6. Нестыковка во времени ГНСС

Если БУ обнаруживает несоответствие более чем на 1 минуту между временем функции измерения времени бортового устройства и временем приёмника 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 приёмник ГНСС не обнаруживает действительного сигнала ГНСС в течение последних 30 дней. Однако если информация о местоположении из приёмника ГНСС появляется снова, производится автоматическая корректировка времени.

## 7. Противоречивые данные о движении транспортного средства

GNS\_35 БУ инициирует и регистрирует событие противоречивых данных о движении транспортного средства (см. Требование 84 в настоящем приложении) с указанием времени, равного текущему значению времени, в случае если информация движения, вычисляемая по датчику движения, противоречит информации движения, вычисляемой по внутреннему приёмнику ГНСС или внешнему устройству ГНСС. Для обнаружения таких противоречий используется медианное значение разностей скоростей между указанными источниками, как описано 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 медианного значения.
- медианное значение вычисляется как среднее 80% остальных значений после устранения самых высоких абсолютных значений.

Событие, связанное с противоречивыми данными о движении транспортного средства, инициируется, если медианное значение превышает 10 км/ч в течение пяти минут движения транспортного средства подряд. Для более надёжного обнаружения манипуляций с тахографом возможно факультативное применение других независимых источников обнаружения движения транспортного средства. (Примечание: медианное значение за последние 5 минут применяется для смягчения риска, связанного с посторонними и мгновенными значениями). Данное событие не инициируется при соблюдении следующих условий: а) во время переправы на пароме/поезде, б) если информации о местоположении из приёмника ГНСС нет и в) в режиме калибровки.

## RU

## Приложение 13. Интерфейс ИТС

## СОДЕРЖАНИЕ

<b>1.</b>	<b>ВВЕДЕНИЕ .....</b>	<b>452</b>
<b>2.</b>	<b>ОБЛАСТЬ ПРИМЕНЕНИЯ.....</b>	<b>452</b>
<b>2.1.</b>	<b>Сокращения, определения и обозначения.....</b>	<b>452</b>
<b>3.</b>	<b>ССЫЛКИ НА РЕГЛАМЕНТЫ И СТАНДАРТЫ.....</b>	<b>453</b>
<b>4.</b>	<b>ПРИНЦИПЫ РАБОТЫ ИНТЕРФЕЙСА .....</b>	<b>454</b>
<b>4.1.</b>	<b>Обязательные условия передачи данных через интерфейс ИТС .....</b>	<b>454</b>
4.1.1	Данные, передаваемые через интерфейс ИТС .....	454
4.1.2	Содержание данных.....	454
4.1.3	Приложения ИТС.....	454
<b>4.2.</b>	<b>Коммуникационные технологии .....</b>	<b>454</b>
<b>4.3.</b>	<b>Авторизация при помощи ПИН-кода.....</b>	<b>455</b>
<b>4.4.</b>	<b>Формат сообщения .....</b>	<b>456</b>
<b>4.5.</b>	<b>Согласие водителя.....</b>	<b>461</b>
<b>4.6.</b>	<b>Извлечение стандартных данных .....</b>	<b>462</b>
<b>4.7.</b>	<b>Извлечение личных данных.....</b>	<b>462</b>
<b>4.8.</b>	<b>Извлечение данных о событиях и неисправностях .....</b>	<b>462</b>

## 1. Введение

В настоящем приложении представлен дизайн и процедуры реализации интерфейса с интеллектуальными транспортными системами (ИТС) в соответствии с требованиями статьи 10 Регламента (ЕС) № 165/2014 (*регламент*).

В *регламенте* уточняется, что тахографы транспортных средств могут быть оснащены стандартизированными интерфейсами, позволяющими использовать данные, записанные или произведённые 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;
- в) внешнее устройство, соединённое с интерфейсом, имеет доступ к личным данным, включая данные геопозиционирования, только при условии получения поддающегося проверке согласия водителя, с которым связаны эти данные.

## 2. Область применения

Область применения настоящего приложения – 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 настоящем приложении обсуждается следующее:

- *Данные*, доступные 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* или является функцией дизайна изделия).
- Форма подачи собранных данных в приложение на внешнем устройстве.
- Положения по безопасности данных, помимо обеспечиваемой Bluetooth® (например, шифрования), относительно содержания *данных* (это обсуждается в других частях *регламента* [приложение 10 «Общие механизмы безопасности»]).
- Протоколы Bluetooth®, используемые интерфейсом ИТС.

### 2.1. Сокращения, определения и обозначения

В настоящем приложении используются следующие сокращения и определения:



<b>Передача данных</b>	обмен информацией/данными между основным устройством (т.е. тахографом) и внешним устройством через интерфейс ИТС при помощи Bluetooth®.
<b>Данные</b>	Наборы данных в соответствии с определением в приложении 1.
<b>Регламент</b>	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 в дорожном транспорте и вносящий поправки в Регламент (ЕС) № 561/2006 Европейского парламента и Совета о гармонизации определённого социального законодательства, связанного с дорожным транспортом
<b>BR</b>	Базовая скорость
<b>EDR</b>	Ускоренная передача данных
<b>GNSS</b>	Глобальная навигационная спутниковая система
<b>IRK</b>	Ключ разрешения при опознавании
<b>ITS</b>	Интеллектуальная транспортная система
<b>LE</b>	Энергия низкого уровня
<b>PIN</b>	Персональный идентификационный номер
<b>PUC</b>	Персональный разблокировочный код
<b>SID</b>	Идентификатор функции
<b>SPP</b>	Профиль последовательного порта
<b>SSP</b>	Защищённое простое соединение
<b>TRTP</b>	Параметр запроса передачи данных
<b>TREP</b>	Ответный параметр передачи данных
<b>VU (БУ)</b>	Бортовое устройство

### 3. Ссылки на регламенты и стандарты

Спецификация, представленная в настоящем приложении, относится ко всем следующим регламентам и стандартам или их частям или опирается на них. В положениях настоящего приложения указываются конкретные стандарты или конкретные их условия. В случае противоречия преимущественную силу имеют положения настоящего приложения.

Регламенты и стандарты, на которые даются ссылки в настоящем приложении:

- 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 в дорожном транспорте и вносящий поправки в Регламент (ЕС) № 561/2006 Европейского парламента и Совета о гармонизации определённого социального законодательства, связанного с дорожным транспортом.
- Регламент (ЕС) № 561/2006 Европейского парламента и Совета от 15 марта 2006 г. о гармонизации определённого 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 : Дорожные транспортные средства. Системы тахографов. Часть 7: параметры
- Bluetooth®. Профиль последовательного. V1.2
- Bluetooth®. Основная версия 4.2

- Протокол NMEA 0183 V4.1

#### **4. Принципы работы интерфейса**

### **4.1. Обязательные условия передачи данных через интерфейс ИТС**

БУ отвечает за обновление и поддержку данных, хранящихся в БУ, без участия интерфейса ИТС. Средства, которыми это достигается, являются внутренними средствами БУ, описанными в других частях регламента и не указанными в настоящем приложении.

#### **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, или, если такой спецификации нет, являются функцией дизайна изделия и в настоящем приложении не обсуждаются.

#### **4.1.2 Содержание данных**

Содержание *данных* соответствует представленному в приложении 1 настоящего приложения.

#### **4.1.3 Приложения ИТС**

Приложения ИТС используются данные, предоставляемые через интерфейс ИТС, например, для оптимизации управления действиями водителя при условии соблюдения регламента, обнаружения возможных неисправностей тахографа или использования данных ГНСС. Спецификация приложений в настоящее приложение не входит.

### **4.2. Коммуникационные технологии**

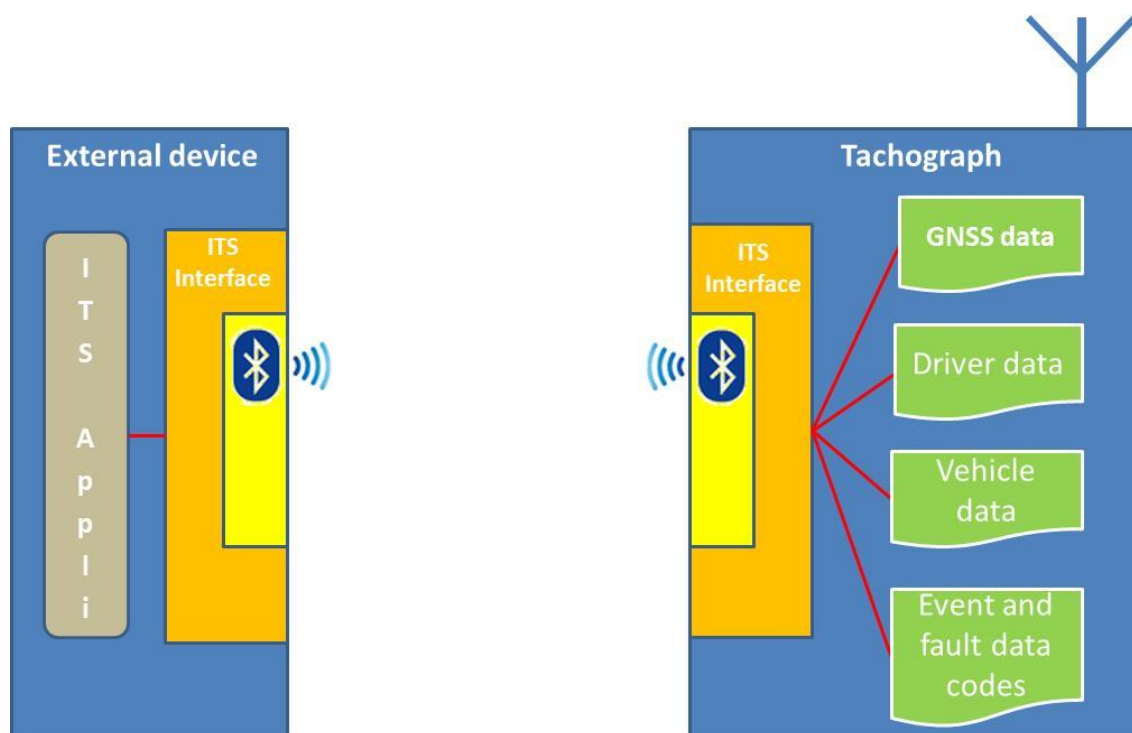
Обмен *данными* через интерфейс ИТС происходит при помощи интерфейса Bluetooth®, совместимость которого обеспечивается через версию 4.2 или новее. Bluetooth® действует на нелицензированной промышленной, научной и медицинской волне (ISM) от 2,4 до 2,485 ГГц. Bluetooth® 4.2 обеспечивает усиленные механизмы конфиденциальности и защиты и увеличивает скорость и надёжность 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 \(https://www.bluetooth.org/en-us/specification/adopted-specifications?\\_ga=1.215147412.2083380574.1435305676\)](https://www.bluetooth.com/specifications?_ga=1.215147412.2083380574.1435305676).

*Передача данных* происходит с оборудованием связи после завершения процесса соединения 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 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 вступать в связь при

дальнейших соединениях в будущем. После завершения данного этапа устанавливается доверие внешнему устройству, и 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 «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. Авторизация при помощи ПИН-кода

Из соображений безопасности БУ предусматривает систему авторизации по ПИН-коду, отдельную 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 предоставить верный 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 провалилась, устройство временно вносится в чёрный список. Пока оно находится в чёрном списке, любые новые попытки устройства отклоняются. Если попытка ввода верного ПИН-кода снова проваливается 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. Рисунок 1 в приложении 2 представляет собой диаграмму последовательности действий при попытке ввода ПИН-кода.

Число неудачных попыток подряд	Продолжительность запрета
3	30 секунд
6	5 минут
9	1 час
12	24 часа
15	Навсегда

**Таблица 50. Продолжительность запрета в зависимости от числа неудачных попыток ввода верного ПИН-кода подряд**

Если попытка ввода ПИН-кода провалилась пятнадцать раз подряд (5 x 3), устройство ИТС вносится в чёрный список навсегда. Этот запрет на него снимается только при вводе верного кода PUC.

Код PUC состоит из 8 цифр; его предоставляет производитель вместе с БУ. Если попытка ввода верного кода PUC провалилась десять раз подряд, устройство ИТС необратимо вносится в чёрный список.

Хотя производитель 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, внесённые в белый список, сохраняются до тех пор, пока их вручную не удалит пользователь (например, через интерфейс пользователя и машины БУ или другие средства). Таким образом утерянные или украденные 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 предоставить верный ПИН-код.

Формат сообщений между интерфейсом БУ и БУ оставлен на усмотрение производителя. Однако производитель должен позаботиться о том, 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. Рисунок 2 в приложении 2 представляет собой диаграмму последовательности действий для проведения указанной процедуры. Любое устройство, внесённое в чёрный список, получает автоматический отказ, а устройство, не внесённое ни в чёрный, 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 трёхкомпонентной структурой: Заголовок, состоящий из байта адреса приёмника (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.

Заголовок			Поле данных					Контрольная сумма
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 байта			Макс. 255 байтов					1 байт

**Таблица 51. Общий формат сообщения.**

#### Заголовок

TGT и SRC: ИД устройств приёма (TGT) и источника (SRC) сообщения. ИД интерфейса БУ по умолчанию "EE". Его изменить нельзя. Для первого сообщения сеанса связи устройство ИТС по умолчанию использует ИД "A0". Затем интерфейс БУ присваивает уникальный идентификатор устройству ИТС и передаёт его ему для дальнейшего обмена сообщениями во время сеанса.

Байт LEN учитывает только часть "DATA" в поле данных (см. таблицу 2), а первые 4 байта остаются неясными.

Интерфейс БУ подтверждает подлинность отправителя сообщения, проводя перекрёстную 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 счётчика.

Если данные, которые необходимо передать, слишком длинные и не помещаются в одно сообщение, они разбиваются на несколько подсообщений. Каждое подсообщение имеет одинаковый заголовок и SID, но содержит 2-байтовый счётчик, счётчик текущего сообщения (CC) и счётчик максимального числа сообщений (CM), 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 её.

Если CC и CM не используются, им присваивается значение 0xFF.

Например, такое сообщение

ЗАГОЛОВОК	SID	TRTP	CC	CM	ДАнные	CS
3 байта	Более 255 байтов					1 байт

Передаётся в таком виде:

ЗАГОЛОВОК	SID	TRTP	01	n	ДАнные	CS
3 байта	255 байта					1 байт

ЗАГОЛОВОК	SID	TRTP	02	n	ДАнные	CS
3 байта	255 байта					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 CS и CM не отображаются; см. полный формат выше.

Сообщение	Заголовок			Данные			Контрольная сумма
	TGT	SRC	LEN	SID	TRTP	ДАнные	
<i>RequestPIN</i>	<i>ITSID</i>	EE	00	01	FF		
<i>SendITSID</i>	<i>ITSID</i>	EE	01	02	FF	<i>ITSID</i>	
<i>SendPIN</i>	EE	<i>ITSID</i>	04	03	FF	4*INTEGER (0..9)	
<i>PairingResult</i>	<i>ITSID</i>	EE	01	04	FF	BOOLEAN (T/F)	
<i>SendPUC</i>	EE	<i>ITSID</i>	08	05	FF	8*INTEGER (0..9)	
<i>BanLiftingResult</i>	<i>ITSID</i>	EE	01	06	FF	BOOLEAN (T/F)	
<i>RequestRejected</i>	<i>ITSID</i>	EE	08	07	FF	Время	
<i>RequestData</i>							
standardTachData	EE	<i>ITSID</i>	01	08	01		
personalTachData	EE	<i>ITSID</i>	01	08	02		
gnssData	EE	<i>ITSID</i>	01	08	03		
standardEventData	EE	<i>ITSID</i>	01	08	04		
personalEventData	EE	<i>ITSID</i>	01	08	05		
standardFaultData	EE	<i>ITSID</i>	01	08	06		

manufacturerData	EE	ITSID	01	08	07		
ResquestAccepted	ITSID	EE	Len	09	TREP	Данные	
DataUnavailable							
Данных нет	ITSID	EE	02	0A	TREP	10	
Личные данные не передаются	ITSID	EE	02	0A	TREP	11	
NegativeAnswer							
Общее отклонение запроса	ITSID	EE	02	0B	SID Req	10	
Функция 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 очередн.	ITSID	EE	02	0B	SID Req	22	
Нештатный запрос	ITSID	EE	02	0B	SID Req	31	
Ожидается ответ	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	

Таблица 52. Подробное содержание сообщения

*RequestPIN (SID 01)*

Сообщение выдаёт интерфейс БУ, если устройство ИТС, не включённое в чёрный или белый списки, направляет запрос о передаче данных.

*SendITSID (SID 02)*

Данное сообщение выдаёт 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 выдаёт устройство ИТС, чтобы быть внесённым в белый список интерфейса БУ. Содержание данного сообщения – 4 ЦЕЛЫХ ЧИСЛА от 0 до 9.

*PairingResult (SID 04)*

Данное сообщение выдаёт интерфейс БУ, чтобы 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 выдаёт устройство ИТС, чтобы быть удалённым из чёрного списка интерфейса БУ. Содержание данного сообщения – 8 ЦЕЛЫХ ЧИСЕЛ от 0 до 9.

*BanLiftingResult (SID 06)*

Данное сообщение выдаёт интерфейс БУ, чтобы сообщить устройству ИТС, что переданный код PUC верный. Содержание данного сообщения – BOOLEAN со значением “True”, если код PUC верный, и “False” в противном случае.

*RequestRejected (SID 07)*

Данное сообщение выдаётся интерфейсом БУ как ответ на любое сообщение устройства ИТС из чёрного списка, кроме “SendPUC”. Сообщение содержит оставшееся время, в течение которого устройство ИТС остаётся в чёрном списке, в соответствии с форматом последовательности “Time”, как указано в приложении 3.

*RequestData (SID 08)*

Данное сообщение о доступе к данным выдаётся устройством ИТС. Тип требуемых данных указывается однобайтовым параметром запроса передачи (TRTP). Возможна передача нескольких типов данных:

- standardTachData (TRTP 01): Данные, которые можно получить с тахографа, классифицируемые как неличные.
- personalTachData (TRTP 02): Данные, которые можно получить с тахографа, классифицируемые как личные.
- gnssData (TRTP 03): Данные ГНСС, всегда личные.
- standardEventData (TRTP 04): Данные регистрируемых событий, классифицируемые как неличные.
- personalEventData (TRTP 05): Данные регистрируемых событий, классифицируемые как личные.
- standardFaultData (TRTP 06): Регистрируемые неисправности, классифицируемые как неличные.
- manufacturerData (TRTP 07): данные, предоставляемые производителем.

Более подробную информацию о содержании каждого типа данных см. в приложении 3 настоящего приложения.

Более подробную информацию о формате и содержании данных ГНСС см. в приложении 12.

Более подробную информацию о коде данных событий и неисправностей см. в дополнениях IB и IC.

*ResquestAccepted (SID 09)*

Данное сообщение выдаётся интерфейсом БУ, если принято сообщение устройства ИТС “RequestData”. Данное сообщение содержит 1-байтовое значение TREP, представляющее собой байт TRTP соответствующего сообщения RequestData, и все данные запрошенного типа.



*DataUnavailable* (SID 0A)

Данное сообщение выдаётся интерфейсом БУ, если по какой-либо причине запрашиваемых данных нет, чтобы их можно было передать устройству ИТС, включённому в белый список. Сообщение содержит 1-байтовое значение TREP, 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. Могут использоваться 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*).
- Функция 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 очередн. (код: 22)  
Требуемая функция не активирована либо неверная очередность запросов.
- Нештатный запрос (код: 33)  
Значение параметра запроса (поле данных) недействительно.
- Ожидается ответ (код: 78)  
Запрошенная операция не может быть завершена своевременно; БУ не готов к приёму 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 если водитель дал своё согласие, что его личные данные из тахографа могут покинуть сеть транспортного средства и быть переданы приложениям третьих сторон.

Согласие водителя предоставляется при первом вводе определённой карточки водителя или мастерской, в настоящее время неизвестной для бортового устройства, владельцу карточки предлагается выразить

своё согласие на вывод личных данных, связанных с тахографом, через факультативный интерфейс ИТС. (см. также приложение IC, пункт 3.6.2).

Статус согласия (дано/не дано) записывается в блоке памяти тахографа.

Если водитель не один, с интерфейсом ИТС происходит обмен личными данными только тех водителей, которые дали своё согласие. Например, если есть два водителя транспортного средства, и только первый водитель дал согласие на обмен его личными данными, данные второго водителя не передаются.

#### **4.6. Извлечение стандартных данных**

Рисунок 3 приложения 2 представляет 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**

Рисунок 4 в приложении 2 представляет собой диаграмму последовательности действий обработки запроса на личные данные. Как уже указывалось, интерфейс БУ передаёт личные данные, только если водитель дал явное согласие на это (см. также 4.5). В противном случае запрос должен быть автоматически отклонён.

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

ПЕРЕЧЕНЬ ДАННЫХ, ДОСТУПНЫХ ЧЕРЕЗ ИНТЕРФЕЙС ИТС

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

**2°) ПОСТОЯННЫЕ ДАННЫЕ ГНСС, ДОСТУПНЫЕ ПРИ УСЛОВИИ СОГЛАСИЯ ВОДИТЕЛЯ**

См. приложение 12. ГНСС

**3°) КОДЫ СОБЫТИЙ, ДОСТУПНЫХ БЕЗ СОГЛАСИЯ ВОДИТЕЛЯ**

Событие	Правила хранения	Данные по каждому событию, подлежащие регистрации
Ввод недействительной карточки	- 10 последних событий.	- дата и время события, - тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, в отношении которой произошло событие. - число аналогичных событий за указанный день
Несовместимость карточек	- 10 последних событий.	- дата и время начала события, - дата и время завершения события, - тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение обеих карточек, в отношении которых возникла несовместимость.
Неправильное завершение последнего сеанса использования карточки	- 10 последних событий.	- дата и время ввода карточки, - тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение, - дата последнего сеанса использования, записанная на карточке: - дата и время ввода карточки, - VRN, государство-член регистрации и поколение БУ.
Прекращение электропитания (2)	- самое продолжительное событие за каждые последние 10 дней данного случая, - 5 самых продолжительных событий за последние 365 дней.	- дата и время начала события, - дата и время завершения события, - тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события, - число аналогичных событий за указанный день.

Ошибка связи со средством удалённой связи	<ul style="list-style-type: none"> <li>- самое продолжительное событие за каждые последние 10 дней данного случая,</li> <li>- 5 самых продолжительных событий за последние 365 дней.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- число аналогичных событий за указанный день.</li> </ul>
Отсутствие информации о местоположении из приёмника ГНСС	<ul style="list-style-type: none"> <li>- самое продолжительное событие за каждые последние 10 дней данного случая,</li> <li>- 5 самых продолжительных событий за последние 365 дней.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- число аналогичных событий за указанный день.</li> </ul>
Ошибочные данные о движении	<ul style="list-style-type: none"> <li>- самое продолжительное событие за каждые последние 10 дней данного случая,</li> <li>- 5 самых продолжительных событий за последние 365 дней.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- число аналогичных событий за указанный день.</li> </ul>
Противоречивые данные о движении транспортного средства	<ul style="list-style-type: none"> <li>- самое продолжительное событие за каждые последние 10 дней данного случая,</li> <li>- 5 самых продолжительных событий за последние 365 дней.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- число аналогичных событий за указанный день.</li> </ul>
Попытка нарушения системы защиты	<ul style="list-style-type: none"> <li>- 10 последних событий по типу события.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события (если актуально),</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- тип события.</li> </ul>

Противоречивые данные о времени	<ul style="list-style-type: none"> <li>- самое продолжительное событие за каждые последние 10 дней данного случая,</li> <li>- 5 самых продолжительных событий за последние 365 дней.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время в записывающем оборудовании</li> <li>- дата и время ГНСС,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- число аналогичных событий за указанный день.</li> </ul>
---------------------------------	---	--

#### **4°) КОДЫ СОБЫТИЙ, ДОСТУПНЫХ ПРИ УСЛОВИИ СОГЛАСИЯ ВОДИТЕЛЯ**

<b>Событие</b>	<b>Правила хранения</b>	<b>Данные по каждому событию, подлежащие регистрации</b>
Управление без соответствующей карточки	<ul style="list-style-type: none"> <li>- самое продолжительное событие за каждые последние 10 дней данного случая,</li> <li>- 5 самых продолжительных событий за последние 365 дней.</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце события,</li> <li>- число аналогичных событий за указанный день.</li> </ul>
Ввод карточки во время управления	<ul style="list-style-type: none"> <li>- последнее событие за каждые последние 10 дней данного случая,</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время события,</li> <li>- тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение,</li> <li>- число аналогичных событий за указанный день</li> </ul>
Превышение скорости (1)	<ul style="list-style-type: none"> <li>- самое серьёзное событие за каждые последние 10 дней данного случая (т.е. самая высокая средняя скорость),</li> <li>- 5 самых серьёзных событий за последние 365 дней.</li> <li>- первое событие, наступившее после последней калибровки</li> </ul>	<ul style="list-style-type: none"> <li>- дата и время начала события,</li> <li>- дата и время завершения события,</li> <li>- максимальная скорость, измеренная во время события,</li> <li>- средняя арифметическая скорость, измеренная во время события,</li> <li>- тип и номер карточки, выдавшее её государство-член и поколение карточки водителя (если применимо),</li> <li>- число аналогичных событий за указанный день.</li> </ul>

**5°) КОДЫ ДАННЫХ О НЕИСПРАВНОСТЯХ, ДОСТУПНЫХ БЕЗ СОГЛАСИЯ ВОДИТЕЛЯ**

<b>Неисправность</b>	<b>Правила хранения</b>	<b>Данные по каждой неисправности, подлежащие регистрации</b>
Неисправность карточки	- 10 последних неисправностей карточки водителя.	- дата и время начала неисправности, - дата и время окончания неисправности, - тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение.
Неисправность записывающего оборудования	- 10 последних неисправностей по типу неисправности, - первая неисправность после последней калибровки.	- дата и время начала неисправности, - дата и время окончания неисправности, - тип неисправности, - тип и номер карточки (карточек), выдавшее её (их) государство-член и поколение карточки, введённой в начале и/или конце неисправности.

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 приёмника ГНСС или внешнего устройства ГНСС
- Неисправность средства удалённой связи

**6°) СОБЫТИЯ И НЕИСПРАВНОСТИ, СВЯЗАННЫЕ С КОНКРЕТНЫМ ПРОИЗВОДИТЕЛЕМ, БЕЗ СОГЛАСИЯ ВОДИТЕЛЯ**

<b>Событие или неисправность</b>	<b>Правила хранения</b>	<b>Данные по каждому событию, подлежащие регистрации</b>
Определяется производителем	Определяется производителем	Определяется производителем



# Приложение 2

ДИАГРАММЫ ПОСЛЕДОВАТЕЛЬНОСТИ ДЕЙСТВИЙ ОБМЕНА СООБЩЕНИЯМИ С  
УСТРОЙСТВОМ ИТС

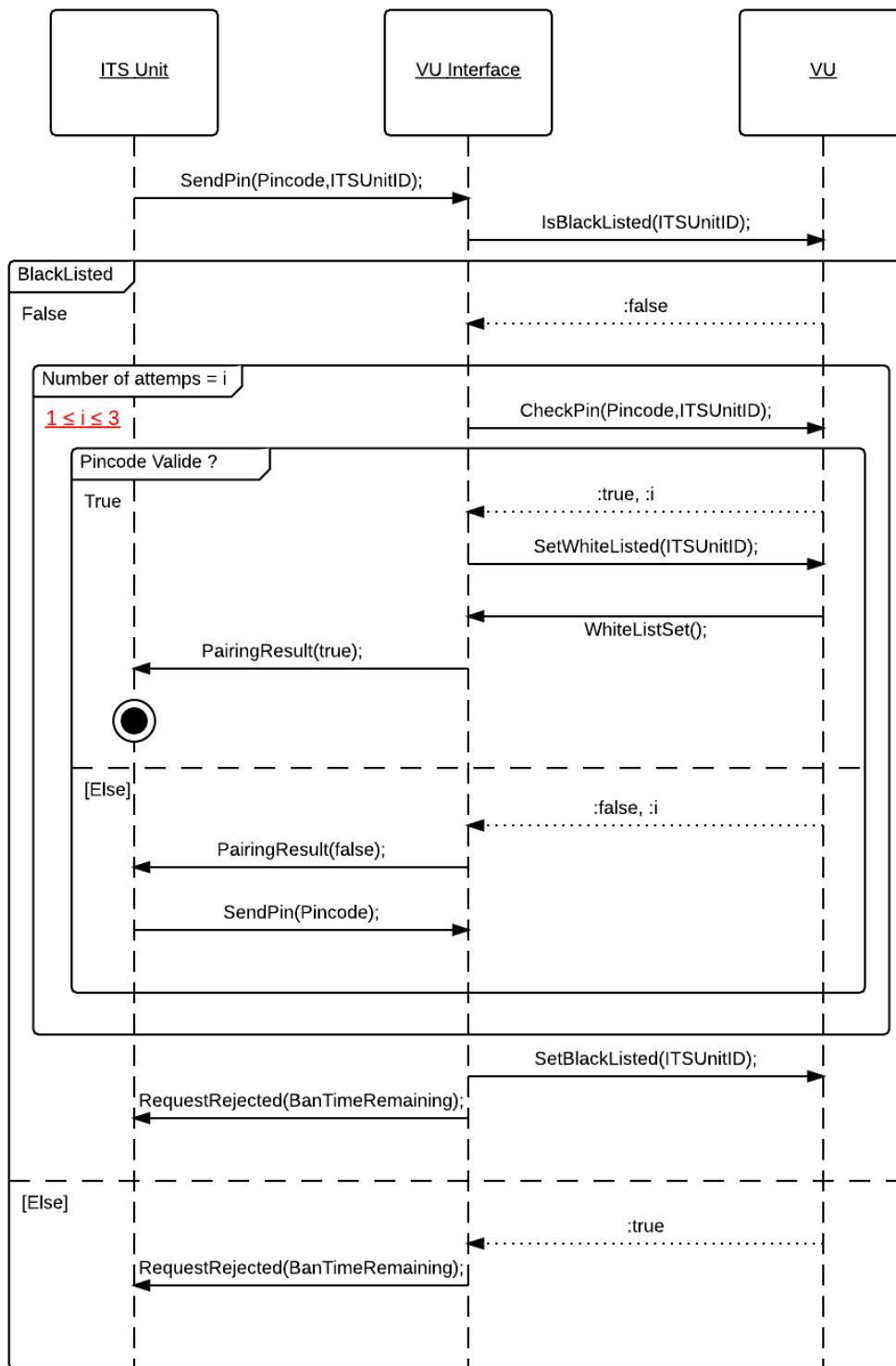


Рисунок 18. Диаграмма последовательности действий попытки ввода ПИН-кода

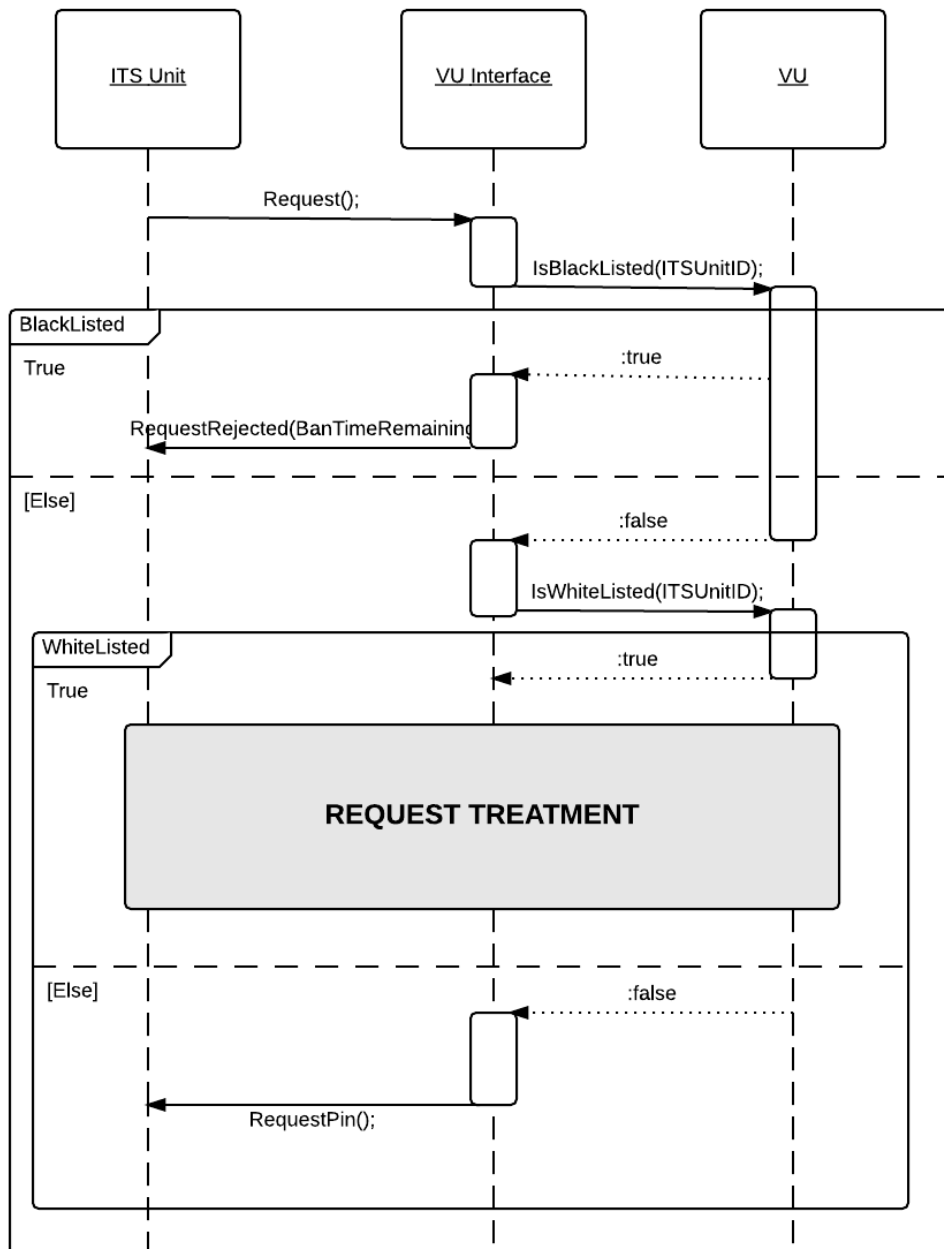


Рисунок 19. Диаграмма последовательности действий проверки полномочий устройства ИТС

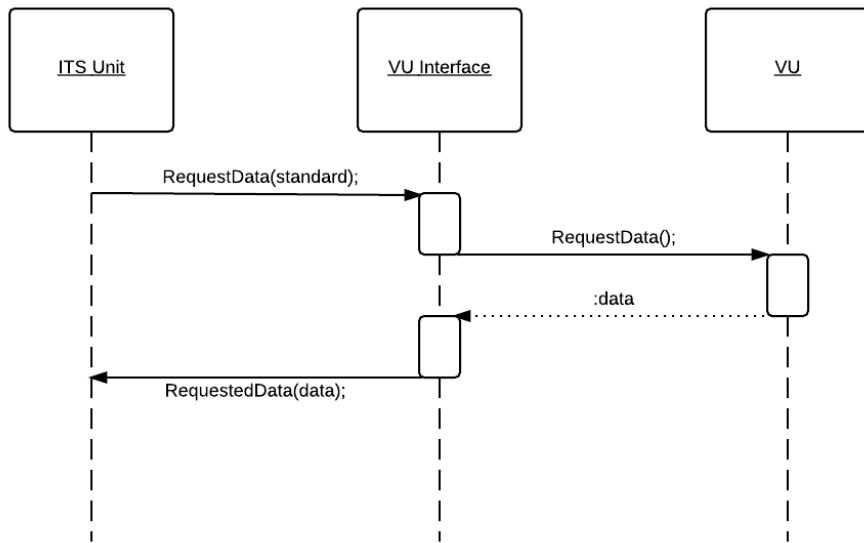


Рисунок 20. Диаграмма последовательности действий обработки запроса на данные, классифицируемые как неличные (после ввода верного ПИН-кода)

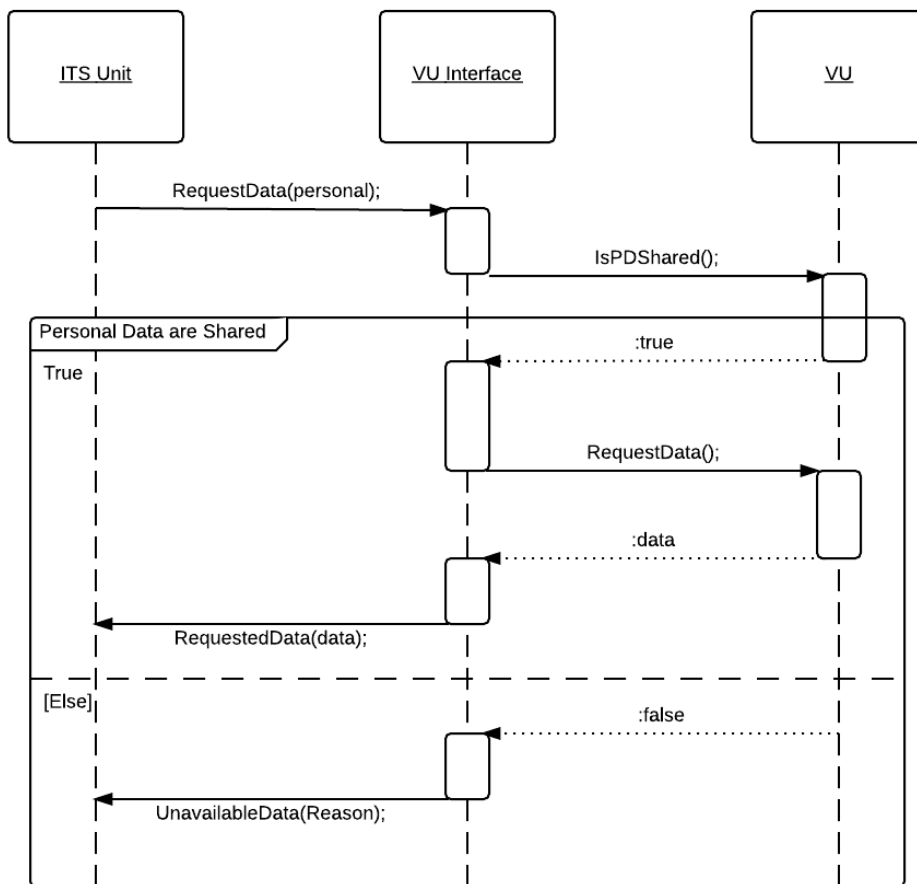


Рисунок 21. Диаграмма последовательности действий обработки запроса на данные, классифицируемые как личные

(после ввода верного ПИН-кода)

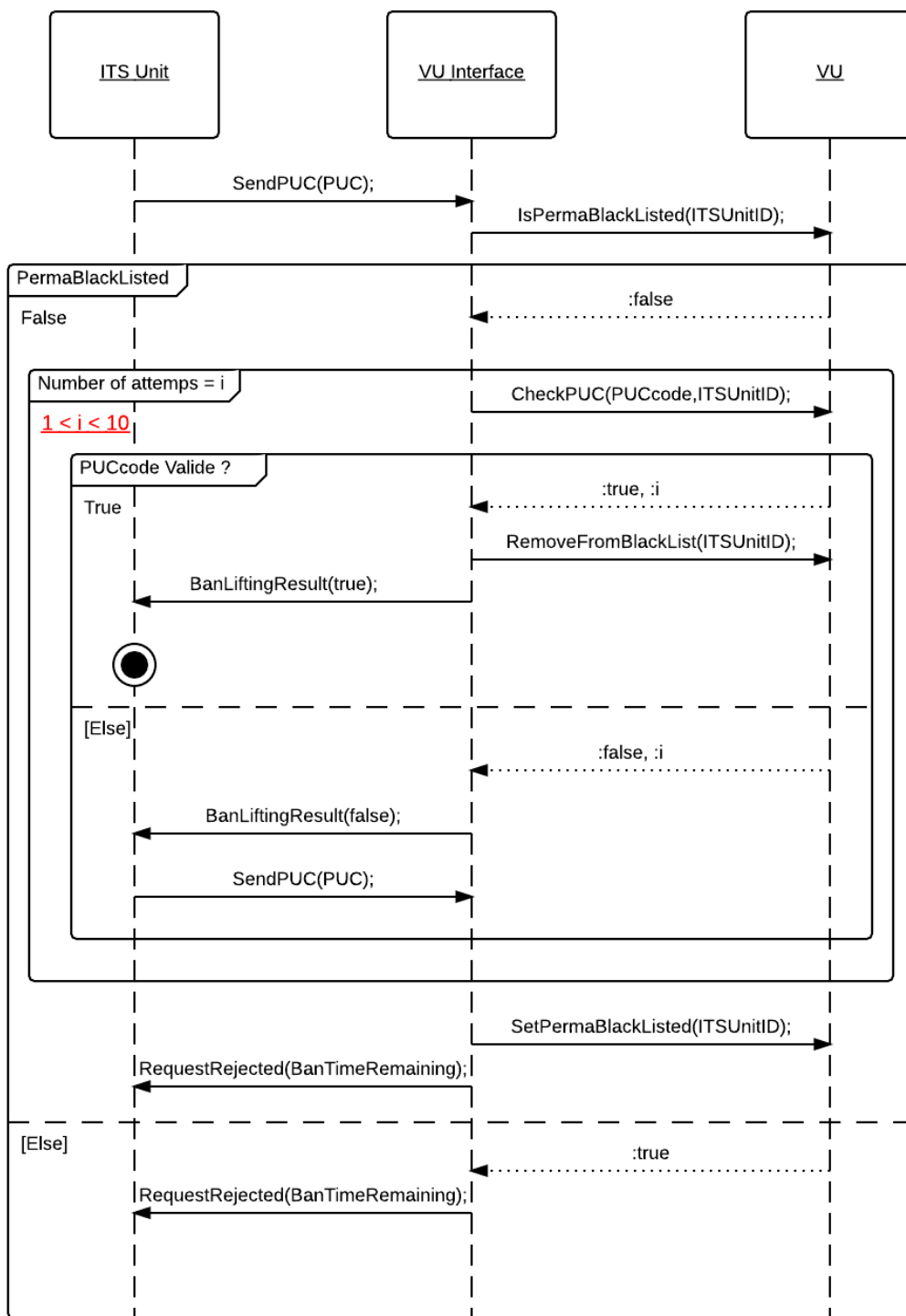


Рисунок 22. Диаграмма последовательности действий попытки ввода кода PUC

# Приложение 3

## ASN.1 СПЕЦИФИКАЦИИ

```

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,
    trtp BIT STRING,
    subMBytes SubMessageBytes,
    dataField Content,
    ...
}

```

```
SubMessageBytes ::= SEQUENCE{
    currentSubM BIT STRING,
    totalSubM BIT STRING
}

Content ::= CHOICE{
    requestPIN RequestPIN,
    sendITSID SendITSID,
    sendPin SendPIN,
    pairRslt 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/IEC 8859--
    surname UTF8String,
    codePageFirstname UTF8String, --See ISO/IEC 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 Appendix1; --See Appendix 1 for more information
about NationAlpha--

    SecurityBreachEvent ::=SEQUENCE{
        --See Annex 1B for more information--
    }

```

```

RecordingEquipmentFaultType ::= SEQUENCE{
    --See Annex 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,
    cardsType SEQUENCE OF UTF8String,
    cardsNumber SEQUENCE OF INTEGER,
    issuingMemberState SEQUENCE OF NationAlpha,
    cardsGeneration SEQUENCE OF INTEGER,
    numberOfSimilarEvent INTEGER
}

SecurityBreachAttempt ::= SEQUENCE{
    beginDate GeneralizedTime,
    endDate GeneralizedTime OPTIONAL,
    cardsType SEQUENCE OF UTF8String,
    cardsNumber SEQUENCE OF INTEGER,
    issuingMemberState SEQUENCE OF NationAlpha,
    numberOfSimilarEvent INTEGER,
    typeOfEvent SecurityBreachEvent
}

TimeConflict ::= SEQUENCE{
    beginDate GeneralizedTime,
    endDate GeneralizedTime,
    cardsType 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,
    cardsType 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
```

## Приложение 14. Функция удалённой связи

### СОДЕРЖАНИЕ

<b>1</b>	<b>ВВЕДЕНИЕ .....</b>	<b>490</b>
<b>2</b>	<b>ОБЛАСТЬ ПРИМЕНЕНИЯ.....</b>	<b>492</b>
<b>3</b>	<b>СОКРАЩЕНИЯ, ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ .....</b>	<b>493</b>
<b>4</b>	<b>СЦЕНАРИИ ДЕЙСТВИЙ.....</b>	<b>496</b>
<b>4.1</b>	<b>Обзор.....</b>	<b>496</b>
4.1.1	Обязательные условия передачи данных через интерфейс DSRC 5,8 ГГц .....	496
4.1.1.1	Данные, хранящиеся в БУ .....	498
4.1.1.2	Данные, передаваемые на устройство DSRC-VU .....	498
4.1.1.3	Содержание данных.....	498
4.1.1.4	Представление данных .....	498
4.1.1.5	Данные безопасности .....	499
4.1.1.6	Данные VUPM, имеющиеся в наличии для передачи через интерфейс DSRC .....	499
4.1.2	Набор характеристик 1a: при помощи направленной руки или временно установленной у обочины и направленной аппаратуры удалённой связи раннего обнаружения.....	498
4.1.3	Набор характеристик 1b: при помощи установленного на транспортном средстве и направленного считывающего устройства удалённой связи раннего обнаружения (REDCR) .....	498
<b>4.2</b>	<b>Безопасность/целостность .....</b>	<b>499</b>
<b>5</b>	<b>СТРУКТУРА И ПРОТОКОЛЫ УДАЛЁННОЙ СВЯЗИ .....</b>	<b>500</b>
<b>5.1</b>	<b>Структура .....</b>	<b>500</b>
<b>5.2</b>	<b>Рабочий процесс.....</b>	<b>504</b>
5.2.1	Операции .....	504
5.2.2	Толкование данных, полученных через связь DSRC.....	505
<b>5.3</b>	<b>Параметры физического интерфейса DSRC для удалённой связи.....</b>	<b>505</b>
5.3.1	Ограничения, связанные с расположением .....	505
5.3.2	Параметры нисходящих и восходящих данных .....	506
5.3.3	Проект антенны.....	511
5.3.3.1	Антенна REDCR.....	513
5.3.3.2	Антенна БУ.....	513
<b>5.4</b>	<b>Протокольные требования DSRC к RTM.....</b>	<b>511</b>
5.4.1	Обзор.....	511
5.4.2	Команды .....	514
5.4.3	Последовательность контрольных команд.....	514
5.4.4	Структуры данных.....	515
5.4.5	Элементы RtmData, выполняемые действия и определения.....	517
5.4.6	Механизм передачи данных.....	524

---

5.4.7	Подробное описание операции DSRC .....	524
5.4.8	Описание тестовой операции DSRC .....	531
<b>5.5</b>	<b>Поддержка Директивы 2015/71/ЕС .....</b>	<b>535</b>
5.5.1	Обзор.....	535
5.5.2	Команды .....	535
5.5.3	Последовательность контрольных команд.....	535
5.5.4	Структуры данных.....	536
5.5.5	Модуль ASN.1 для операции OWS DSRC .....	536
5.5.6	Элементы OwsData, выполняемые действия и определения .....	537
5.5.7	Механизмы передачи данных .....	538
<b>5.6</b>	<b>Передача данных между DSRC-VU и БУ.....</b>	<b>538</b>
5.6.1	Физическое соединение и интерфейсы.....	538
5.6.2	Протокол приложения .....	538
<b>5.7</b>	<b>Обработка ошибок .....</b>	<b>540</b>
5.7.1	Регистрация и передача данных в DSRC-VU .....	540
5.7.2	Ошибки беспроводной связи .....	540
5.7.2.1	Ошибки шифрования и подписи .....	542
5.7.2.2	Регистрация ошибок .....	543
<b>6</b>	<b>ИСПЫТАНИЯ ПРИ ВВОДЕ В ЭКСПЛУАТАЦИЮ И ПЕРИОДИЧЕСКИХ ПРОВЕРКАХ ФУНКЦИИ УДАЛЁННОЙ СВЯЗИ .....</b>	<b>542</b>
<b>6.1</b>	<b>Общие положения .....</b>	<b>542</b>
<b>6.2</b>	<b>ЕСНО .....</b>	<b>542</b>
<b>6.3</b>	<b>Испытания для подтверждения содержания данных безопасности.....</b>	<b>542</b>

## 1 Введение

В настоящем приложении представлены проект и процедуры осуществления удалённой связи (далее – связь) в соответствии с требованиями статьи 9 Регламента (ЕС) № 165/2014 (далее – регламент).

DSC\_1 В Регламенте (ЕС) № 165/2014 установлено, что тахограф должен быть снабжён функцией удалённой связи, позволяющей представителям компетентных органов контроля считывать информацию с тахографов проезжающих транспортных средств с помощью оборудования удалённого контроля (считывающего устройства удалённой связи раннего обнаружения [REDCR]), конкретно контрольного оборудования, обеспечивающего беспроводное соединение с помощью интерфейса выделенной связи ближнего действия CEN 5,8 ГГц (DSRC).

Важно понимать, что цель данной функции – выполнять роль предварительного фильтра для отбора транспортных средств для более тщательной проверки, и она не заменяет процедуры официальной проверки, как указано в положениях Регламента (ЕС) № 165/2014. См. 9 декларативную часть преамбулы настоящего регламента, в которой говорится, что удалённая связь между тахографом и контрольными органами для целей придорожных проверок помогает проводить целевые придорожные проверки.

DSC\_2 Обмен *данными* происходит при помощи беспроводной *связи* 5,8 ГГц DSRC в соответствии с настоящим приложением и тестируется на основе соответствующих параметров EN 300 674-1 «Электромагнитная совместимость и диапазон радиочастот (ERM); дорожный транспорт и телеинформатика транспортного движения (RTTT); передающее оборудование выделенной связи ближнего действия (DSRC) (500 кбит/с/250 кбит/с) в диапазоне частот промышленной, научной и медицинской связи (ISM) 5,8 ГГц; часть 1: общие характеристики и методы тестирования придорожных устройств (RSU) и бортовых устройств (OBU)».

DSC\_3 *Связь* с устройством связи устанавливается, только если есть запрос от устройства компетентного контрольного органа при помощи соответствующего требованиям радиокommunikационного оборудования (*считывающего устройства удалённой связи раннего обнаружения (REDCR)*).

DSC\_4 Для обеспечения целостности *данные* защищены.

DSC\_5 Доступ к передаваемым *данным* предоставляется только компетентным контрольным органам, уполномоченным совершать проверки на предмет нарушений Регламента (ЕС) № 561/2006 и Регламента (ЕС) № 165/2014, и мастерским, насколько это необходимо для проверки правильного функционирования тахографа.

DSC\_6 *Данные*, обмен которыми происходит во время *связи*, ограничиваются данными, необходимыми для целевых придорожных проверок транспортных средств, на которых замечены манипуляции с тахографом или злоупотребление им.

DSC\_7 Целостность и безопасность данных обеспечиваются путём защиты *данных* в бортовом устройстве (БУ) и передачи только защищённых данных о полезной нагрузке и данных безопасности (см. 5.4.4) при помощи беспроводного средства удалённой связи DSRC 5,8 ГГц, т.е. только уполномоченные представители компетентных контрольных органов могут понять данные, передаваемые по *связи*, и проверить их аутентичность. См. приложение 11 «Общие механизмы безопасности».

DSC\_8 *Данные* содержат временную метку времени последнего обновления.

DSC\_9 Содержание данных безопасности известны только компетентным контрольным органам и сторонам, которым предоставляется эта информация, и находится под их контролем и не

попадает в область применений положений *связи*, представляющих собой предмет настоящего приложения, за исключением того, что *связь* предусматривает возможность передачи пакета защищённых данных с каждым пакетом данных полезной нагрузки.

- DSC\_10 Для получения концепций других данных (таких как взвешивания на борту) можно использовать одинаковую архитектуру и оборудование на основе представленной здесь архитектуры.
- DSC\_11 Для уточнения в соответствии с положениями Регламента (ЕС) № 165/2014 (7 статьи) данные о личности водителя по *связи* не передаются.

## 2 Область применения

Область применения настоящего приложения – указать, каким образом представители компетентных контрольных органов пользуются беспроводной связью DSRC 5,8 ГГц для удалённого получения данных (*данные*) с выбранного транспортного средства, если есть признаки того, что оно, возможно, нарушает Регламент (ЕС) № 165/2014, и должен быть рассмотрен вопрос его остановки для дальнейшего расследования.

Регламент (ЕС) № 165/2014 требует, чтобы собираемые данные были только данные, указывающие 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 она носит целевой характер и работает на ближнем расстоянии. Кроме того, компетентные контрольные органы могут использовать такую же связь для удалённого мониторинга тахографов (RTM) и в других целях (таких как максимальные вес и габариты большегрузных транспортных средств, определённые в Директиве 2015/719/ЕС), и такие операции могут быть отдельными или последовательными на усмотрение компетентных контрольных органов.

В настоящем приложении обсуждается следующее.

Оборудование связи, процедуры и протоколы *связи*  
Стандарты и нормы, которым должно соответствовать радиооборудование  
Поставка *данных* в оборудование *связи*  
Процедуры запроса и загрузки и последовательность операций  
Передаваемые *данные*  
Возможное толкование *данных*, передаваемых в процессе *связи*  
Положения по данным безопасности, связанным со *связью*  
Наличие *данных* для компетентных контрольных органов  
Как *считывающее устройство удалённой связи раннего обнаружения* может запрашивать разные данные грузов и автомобильного парка

В качестве пояснения, в настоящем приложении не указывается следующее:

- осуществление и управление сбором данных в БУ (которые должны являться проектной функцией продукта, если в Регламенте (ЕС) № 165/2014 не указано иначе);
- форма поставки собранных данных представителю компетентных контрольных органов или критерии, используемые компетентными контрольными органами для решения, какое транспортное средство остановить (что является проектной функцией продукта, если в Регламенте (ЕС) № 165/2014 не указано иначе, или стратегическим решением компетентных контрольных органов). Для разъяснения: при помощи *связи данные* просто предоставляются компетентным контрольным органам, чтобы они могли принимать обоснованные решения;
- положения по безопасности данных (например, шифрованию), относительно содержания *данных* (это обсуждается в приложении 11 «Общие механизмы безопасности»);
- подробные описания любых понятий данных, кроме RTM, которые можно получать при помощи такой же архитектуры и оборудования;
- подробности поведения и управления между БУ и DSRC-VU или поведения внутри DSRC-VU (кроме случаев, когда надо предусмотреть поставку *данных* по требованию REDCR).



### 3 Сокращения, определения и обозначения

В настоящем приложении используются следующие сокращения и определения:

- антенна** электрический прибор, преобразующий электрическую мощность в радиоволны и наоборот, применяемый вместе с радиопередатчиком или радиоприёмником. На практике радиопередатчик подаёт электрический ток, колеблющийся на радиочастоте и поступающий в разъёмы антенны, а антенна излучает энергию от тока как электромагнитные волны (радиоволны). При приёме антенна перехватывает часть энергии электромагнитной волны, чтобы у разъёмов произвести маленькое напряжение, передаваемое на приёмник для усиления
- связь** обмен информацией/данными между DSRC-REDCR и DSRC-VU в соответствии с разделом 5 с целью получения данных в рамках соединения ведущего и ведомого
- данные** защищённые данные определённого формата (см. 5.4.4), запрашиваемые DSRC-REDCR и подаваемые на DSRC-REDCR из DSRC-VU через соединение 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 в дорожном транспорте и вносящий поправки в Регламент (ЕС) № 561/2006 Европейского парламента и Совета о гармонизации определённого социального законодательства, связанного с дорожным транспортом

<b>AID</b>	Идентификатор приложения
<b>BLE</b>	низкая энергия Bluetooth
<b>BST</b>	таблица использования радиомаяков
<b>CIWD</b>	ввод карточки во время управления
<b>CRC</b>	циклический контроль избыточности
<b>DSC (n)</b>	идентификатор требования конкретного приложения DSRC
<b>DSRC</b>	выделенная связь ближнего действия
<b>DSRC-REDCR</b>	DSRC – считывающее устройство удалённой связи раннего обнаружения
<b>DSRC-VU</b>	DSRC – бортовое устройство. Это устройство удалённого раннего обнаружения, представленное в приложении 1С.
<b>DWVC</b>	управление без действительной карточки
<b>EID</b>	идентификатор элемента
<b>LLC</b>	управление логической связью
<b>LPDU</b>	блока данных протокола LLC
<b>OWS</b>	бортовая система взвешивания
<b>PDU</b>	блок данных протокола
<b>REDCR</b>	считывающее устройство удалённой связи раннего обнаружения. Это считывающее устройство удалённой связи раннего обнаружения, представленное в приложении 1С.
<b>RTM</b>	удалённый мониторинг тахографа
<b>SM-REDCR</b>	модуль защиты - считывающее устройство удалённой связи раннего обнаружения
<b>TARV</b>	приложения телеинформатики для регулируемых транспортных средств (серия стандартов ISO 15638)
<b>VU (BY)</b>	бортовое устройство
<b>VUPM</b>	память бортового устройства
<b>VUSM</b>	модуль защиты бортового устройства
<b>VST</b>	таблица обслуживания транспортного средства
<b>WIM</b>	взвешивание в движении
<b>WOB</b>	взвешивание на борту

Спецификация, представленная в настоящем приложении, относится ко всем следующим регламентам и стандартам или их частям или опирается на них. В положениях настоящего приложения указываются конкретные стандарты или конкретные их условия. В случае противоречия преимущественную силу имеют положения настоящего приложения. В случае любых противоречий, если в настоящем приложении не дано конкретных указаний, преимущественную силу имеет работа по ERC 70-03 (и испытания по соответствующим параметрам EN 300 674-1), а затем в порядке убывания в зависимости от предпочтения – 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:

- [1] 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 в дорожном транспорте и вносящий поправки в Регламент (ЕС) № 561/2006 Европейского парламента и Совета о гармонизации определённого социального законодательства, связанного с дорожным транспортом.
- [2] Регламент (ЕС) № 561/2006 Европейского парламента и Совета от 15 марта 2006 г. о гармонизации определённого 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).
- [3] ERC 70-03 СЕПТ: Рекомендация ECC 70-03: об использовании устройств ближнего действия (SRD)
- [4] ISO 15638 Интеллектуальные транспортные системы. Рамки приложений телеинформатики на базе сотрудничества для регулируемых коммерческих грузовых транспортных средств (TARV).

- 
- [5] EN 300 674-1 Электромагнитная совместимость и диапазон радиочастот (ERM); дорожный транспорт и телеинформатика транспортного движения (RTTT); передающее оборудование выделенной связи ближнего действия (DSRC) (500 кбит/с/250 кбит/с) в диапазоне промышленных, научных и медицинских данных (ISM) 5,8 ГГц; часть 1: общие характеристики и методы тестирования придорожных устройств (RSU) и бортовых устройств (OBU).
  - [6] EN 12253 Телеинформатика дорожного транспорта и дорожного движения. Выделенная связь ближнего действия. Физический уровень с использованием микроволн при 5,8 ГГц.
  - [7] EN 12795 Телеинформатика дорожного транспорта и дорожного движения. Выделенная связь ближнего действия. Уровень канала передачи данных: доступ к носителям и управление логической связью.
  - [8] EN 12834 Телеинформатика дорожного транспорта и дорожного движения. Выделенная связь ближнего действия. Уровень приложения.
  - [9] EN 13372 Телеинформатика дорожного транспорта и дорожного движения. Выделенная связь ближнего действия. Характеристики приложений RTTT.
  - [10] ISO 14906 Электронный сбор платы. Определение интерфейса приложения для выделенной связи ближнего действия

## 4 Сценарии действий

### 4.1 Обзор

Регламент (ЕС) № 165/2014 предусматривает конкретные и контролируемые сценарии, в рамках которых следует прибегать к связи.

Поддерживаемые сценарии:

*Описание характеристик связи 1: придорожная проверка с использованием беспроводной связи ближнего действия и считывающего устройства удалённой связи раннего обнаружения, иницирующего физические придорожные проверки (ведущий-ведомый)*

*Характеристики считывающего устройства 1a: при помощи направленной руки или временно установленной у обочины и направленной аппаратуры удалённой связи раннего обнаружения*  
*Характеристики считывающего устройства 1b: при помощи установленного на транспортном средстве и направленного считывающего устройства удалённой связи раннего обнаружения.*

#### 4.1.1 Обязательные условия передачи данных через интерфейс DSRC 5,8 ГГц

ПРИМЕЧАНИЕ: чтобы понять контекст обязательных условий, считывающее устройство представлено на рисунке 14.3 ниже.

##### 4.1.1.1 Данные, хранящиеся в БУ

DSC\_12 БУ отвечает за обновление каждые 60 секунд и поддержку данных, хранящихся в БУ, без участия интерфейса функции связи DSRC. Методы, которыми это достигается, определяются самим БУ, как указано в Регламенте (ЕС) № 165/2014, приложение 1С, раздел 3.19 *Удалённая связь для целевых придорожных проверок*, и в настоящем приложении не указываются.

##### 4.1.1.2 Данные, передаваемые на устройство DSRC-VU

DSC\_13 БУ отвечает за обновление данных тахографа DSRC (*данные*) всякий раз, когда хранящиеся в БУ данные обновляются с интервалом, указанным в 4.1.1.1 (DSC\_12), без всякого участия функции связи DSRC.

DSC\_14 Данные БУ используются в качестве основы наполнения и обновления *данных*, а средства, которыми это достигается, описываются в приложении 1С, раздел 3.19 *Удалённая связь для целевых придорожных проверок*, или, если такой спецификации нет, являются проектной функцией изделия и в настоящем приложении не обсуждаются. Проект 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 представлены в структуре, форме и формате, описанных в 5.4.4 настоящего приложения (структуры данных).

##### 4.1.1.4 Представление данных

DSC\_16 *Данные*, которые часто обновляются в соответствии с процедурами, представленными в 4.1.1.1, защищаются до передачи в *DSRC-VU* и представлены в виде значения понятия защищённых 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 единицами. Форма физического инстанцирования для выполнения данных функций связана с проектными особенностями продукта, если в Регламенте (ЕС) № 165/2014 не указано иначе.

#### **4.1.1.5 Данные безопасности**

DSC\_17 Данные безопасности (*securityData*), включающие в себя данные: необходимые для *REDCR* для выполнения работы по расшифровке данных, предоставляются, как указано в приложении 11 «Общие механизмы безопасности», в виде значения данных для временного хранения в *DSRC-VU* в качестве текущей версии *securityData*, в форме, указанной в разделе 5.4.4 приложения.

#### **4.1.1.6 Данные VUPM, имеющиеся в наличии для передачи через интерфейс DSRC**

DSC\_18 Данные, всегда имеющиеся в функции DSRC VUPM для немедленной передачи по требованию *REDCR*, представлены в разделе 5.4.4 в отношении подробных спецификаций модуля ASN.1.

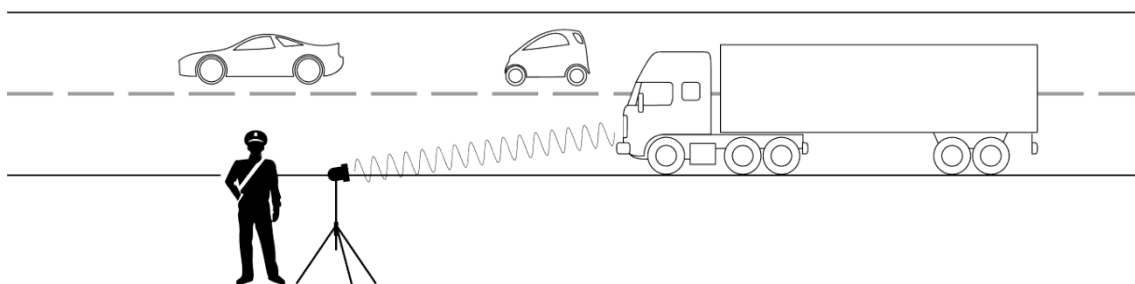
## Общий обзор характеристик связи 1

Данный набор характеристик связан с примером использования, когда представитель компетентных контрольных органов для удалённой связи ближнего действия пользуется считывающим устройством удалённой связи раннего обнаружения (интерфейсами DSRC 5,8 ГГц, интерфейсами, применяемыми в соответствии с ERC 70-03 и тестируемыми по соответствующим параметрам EN 300 674-1, как описано в разделе 5) (*REDCR*) с целью удалённой идентификации транспортного средства, которое, возможно, нарушает Регламент (ЕС) № 165/2014. После идентификации представитель компетентных контрольных органов, контролирующей ход проверки, решает, следует ли остановить транспортное средство.

#### 4.1.2 Набор характеристик 1а: при помощи направленной руки или временно установленной у обочины и направленной аппаратуры удалённой 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. Контроль осуществляется с помощью интерфейса DSRC 5,8 ГГц в рамках ERC 70-03, и проводятся испытания по соответствующим параметрам EN 300 674-1, как описано в разделе 5. См. рисунок 14.1 (вариант использования 1).

##### Use case 1



Придорожное  
устройство

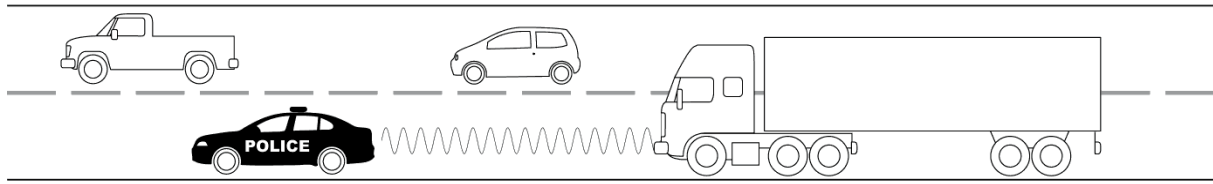
P REDCR

дорожный контроль с помощью DSRC 5,8 ГГц

#### 4.1.3 Набор характеристик 1b: при помощи установленного на транспортном средстве и направленного считывающего устройства удалённой связи раннего обнаружения (*REDCR*)

В данном случае представитель компетентных контрольных органов находится в движущемся транспортном средстве и вытягивает ручное переносное устройство *REDCR* с транспортного средства в направлении центральной части лобового стекла проверяемого транспортного средства, или *REDCR* установлено внутри транспортного средства или на нём так, чтобы было направлено на центр лобового стекла проверяемого транспортного средства, когда транспортное средство со считывающим устройством удалённого действия раннего обнаружения находится в определённом положении относительно проверяемого средства (например, непосредственно перед ним в потоке движения). Контроль осуществляется с помощью интерфейса DSRC 5,8 ГГц в рамках ERC 70-03, и проводятся испытания по соответствующим параметрам EN 300 674-1, как описано в разделе 5. См. рисунок 14.2. (вариант использования 2).

## Use case 2



Мобильное  
устройство  
REDCR

**унок 14.2. Контроль на транспортном  
средстве с помощью DSRC 5,8 гГц**

## 4.2 Безопасность/целостность

Для целей контроля подлинности и целостности загруженных данных при помощи удалённой связи защищённые *данные* проверяются и расшифровываются в соответствии с приложением 11 «Общие механизмы безопасности».

## 5 Структура и протоколы удалённой связи

### 5.1 Структура

Структура функции удалённой связи в «умном» тахографе показана на рисунке 14.3.

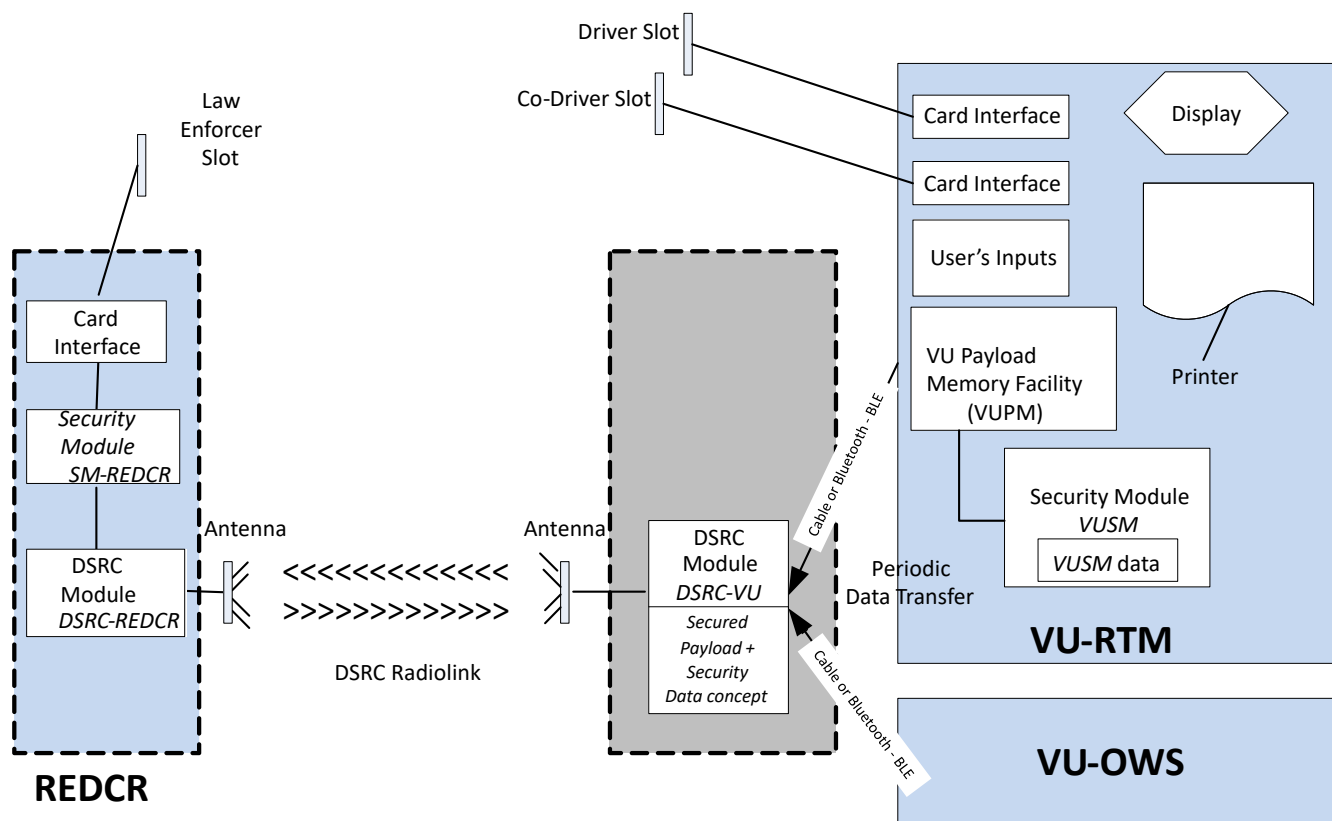


Рисунок 14.3. Структура функции удалённой связи

DSC\_19 В БУ представлены следующие функции:

- модуль безопасности (*VUSM*). Данная функция БУ отвечает за защиту данных, которые подлежат передаче с *DSRC-VU* представителю компетентных контрольных органов посредством удалённой связи.
- Защищённые данные хранятся в памяти *VUSM*. С интервалами, указанными в 4.1.1.1 (DSC\_12), БУ шифрует и пополняет данные RTM (включающие в себя значения данных полезной нагрузки и данных безопасности, представленные ниже в настоящем приложении), хранящиеся в памяти *DSRC-VU*. Работа модуля безопасности представлена в приложении 11 «Общие механизмы безопасности» и не входит в область применения настоящего приложения, кроме того, что требуется обновлённые данные предоставлять устройству связи БУ каждый раз, когда данные *VUSM* меняются.
- Связь между БУ и *DSRC-VU* может быть проводной или беспроводной Bluetooth Low Energy (BLE), а физическое расположение *DSRC-VU* может составлять единое целое с антенной или лобовым стеклом транспортного средства, быть внутри БУ или находиться где-то между ними.
- *DSRC-VU* обеспечивается надёжным источником питания в любой момент времени. Способы обеспечения питания определяются в рамках проектного решения.
- Память *DSRC-VU* энергонезависимая, чтобы данные на *DSRC-VU* сохранялись даже в том случае, если зажигание транспортного средства выключено.



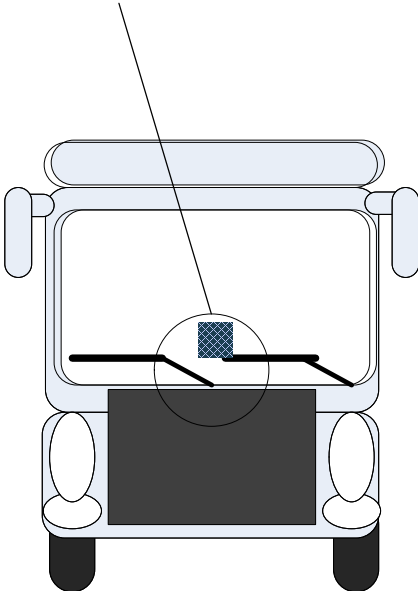
- Если связь между БУ и DSRC-VU осуществляется через BLE, а источник питания – неподзаряжаемая батарея, источник питания DSRC-VU заменяется при каждой регулярной проверке, а производитель оборудования DSRC-VU обязан позаботиться о том, чтобы питание было достаточным на весь период между двумя регулярными проверками и чтобы в течение этого периода любое устройство REDCR могло получить доступ к данным без сбоев или перерывов.
- Устройство полезной памяти БУ RTM (*VUPM*). Данная функция БУ отвечает за предоставление и обновление *данных*. Содержание *данных* (TachographPayload) представлено ниже в 5.4.4/5.4.5 и обновляется с интервалом, указанным в 4.1.1.1 (DSC\_12).
- DSRC-VU. Это функция, встроенная в антенну или соединённая с ней, обеспечивающая связь с БУ через проводное или беспроводное подключение (BLE), где хранятся текущие данные (*данные VUPM*) и осуществляется контроль ответов на запросы при помощи DSRC 5,8 ГГц. Разъединение устройства DSRC или помехи в функциях устройства DSRC при нормальной эксплуатации транспортного средства считаются нарушением Регламента (ЕС) № 165/2014.
- Модуль безопасности (REDCR) (*SM-REDCR*) – это функция, используемая для расшифровки и проверки целостности данных, исходящих из БУ. Средства, которыми это достигается, представлены в приложении 11 «Общие механизмы безопасности» и в настоящем приложении не обсуждаются.
- Функция DSRC (REDCR) (*DSRC-REDCR*) включает в себя трансивер 5,8 ГГц и встроенные программы и другое программное обеспечение контроля *связи* с *DSRC-VU* в соответствии с настоящим приложением.
- *DSRC-REDCR* запрашивает *DSRC-VU* проверяемого транспортного средства и получает *данные* (текущие данные *VUPM* проверяемого транспортного средства) через соединение и процессы DSRC и хранит полученные данные в своём *SM-REDCR*.
- Антенна DSRC-VU располагается в таком месте, откуда она оптимизирует связь DSRC между транспортным средством и придорожной антенной (в целом или ближе к центру лобового стекла транспортного средства...). На легковых транспортных средствах устройство может устанавливаться на уровне верхней части лобового стекла.
  - Перед антенной или вблизи неё не должны находиться никакие металлические объекты (например, именные таблички, наклейки, отражающие элементы из фольги (тонировка), козырьки от солнца, стеклоочистители лобового стекла в неподвижном состоянии), которые могут создать помехи связи.
  - Антенна устанавливается так, чтобы её осевое направление было примерно параллельно поверхности дороги.

DSC\_20 Антенна и связь работают в рамках ERC 70-03, проводятся испытания по соответствующим параметрам EN 300 674-1, как описано в разделе 5. Антенна и связь могут применять технику снижения риска беспроводных помех, как описано в отчёте ECC 228, например, с помощью фильтров связи CEN DSRC 5,8 ГГц.

DSC\_21 Антенна DSRC соединена с устройством DSRC-VU непосредственно в модуле, установленном на лобовом стекле или поблизости, или через выделенный кабель таким образом, чтобы усложнить незаконное отключение. Отключение или вмешательство в работы антенны является нарушением Регламента (ЕС) № 165/2014. Намеренная маскировка или иное неблагоприятное воздействие на работу антенны считаются нарушением Регламента (ЕС) № 165/2014.

DSC\_22 Параметры антенны не определены и зависят от коммерческого решения, если установленное устройство DSRC-VU соответствует требованиям раздела 5. Антенна устанавливается, как указано в DSC\_19 и на рисунке 14.4 (овальная линия), и фактически соответствует вариантам использования, представленным в 4.1.2 и 4.1.3.

CEN-DSRC Antenna Location



**Рисунок 14.4. Пример расположения антенны DSRC на лобовом стекле регулируемых транспортных средств**

Параметры *REDCR* и антенны могут варьироваться в зависимости от обстоятельств, связанных со считывающим устройством (установлено на треноге, ручное, установлено на транспортном средстве и проч.), и способа эксплуатации, которым пользуется представитель компетентных контрольных органов.

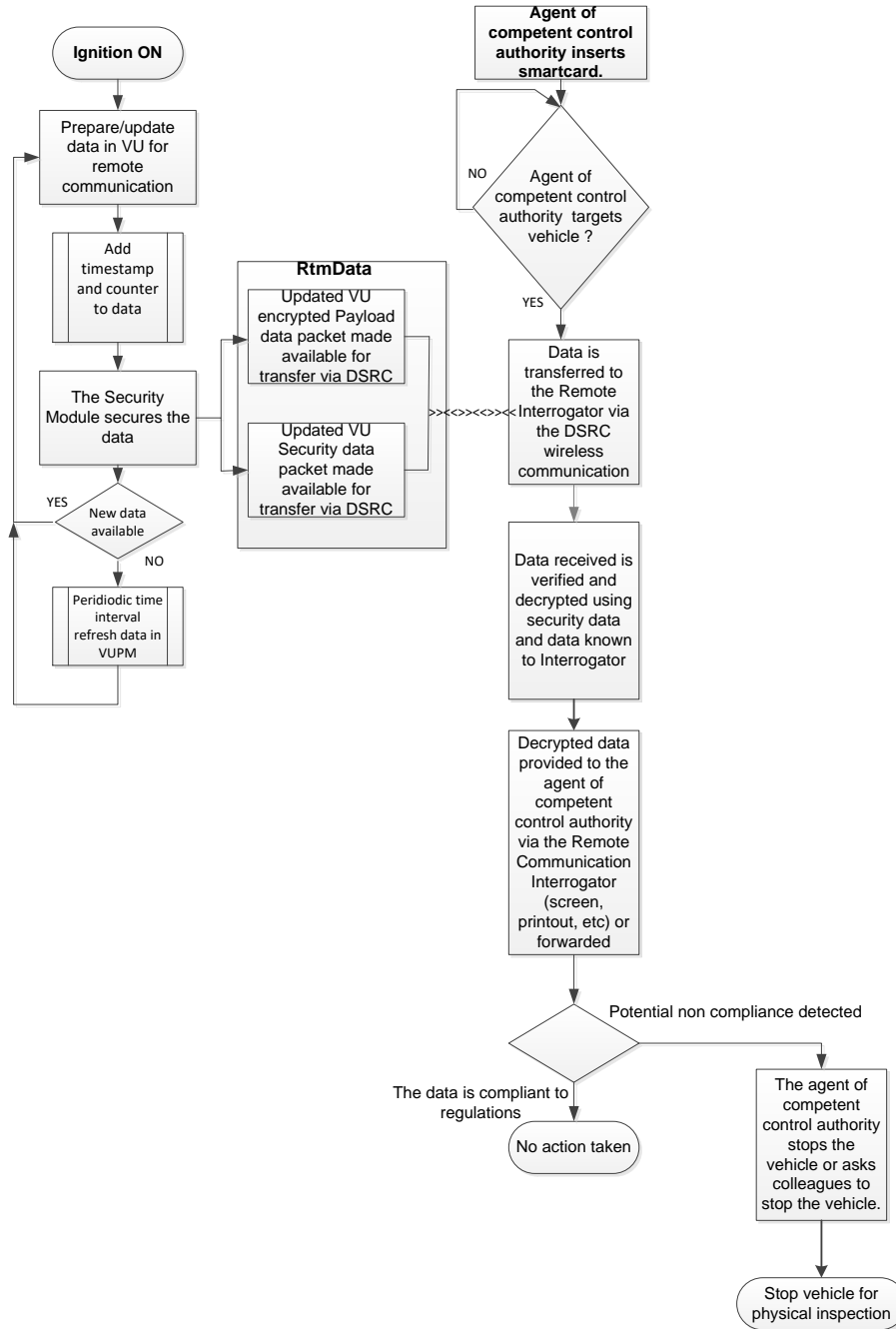
Функция отображения и/или уведомления используется для представления результатов функции удалённой связи представителю компетентных контрольных органов. Отображение возможно на экране, в распечатанном виде, в виде аудиосигнала или в разных сочетаниях этих форм. Форма отображения и/или уведомления зависит от требований представителей компетентных контрольных органов и проектных характеристик изделия и в данном приложении не обсуждается.

- DSC\_23 Проект и параметры *REDCR* зависят от коммерческого дизайна, соответствующего ERC 70-03, и проектных спецификаций и функций, указанных в настоящем приложении (раздел 5.3.2), таким образом обеспечивая максимальную рыночную гибкость при проектировании и поставке оборудования для охвата определённых сценариев контроля любого конкретного компетентного контрольного органа.
- DSC\_24 Проект и параметры *DSRC-VU* и его расположение внутри или снаружи БУ зависят от коммерческого дизайна, соответствующего ERC 70-03, и проектных спецификаций и функций, указанных в настоящем приложении (раздел 5.3.2) и в данном положении (5.1).
- DSC\_25 Однако *DSRC-VU* в состоянии на должном уровне принимать значения данных из другой интеллектуальной аппаратуры транспортного средства при помощи соединения и протоколов открытого промышленного стандарта. (Например, в случае оборудования для взвешивания на борту) если данные определяются уникальными известными идентификаторами приложений/названиями файлов, и Европейской комиссии и производителям соответствующего оборудования бесплатно предоставляются инструкции по управлению такими протоколами.

## 5.2 Рабочий процесс

### 5.2.1 Операции

Рабочий процесс операций представлен на рисунке 14.5.



#### Рисунок 14.5. Рабочий процесс функции удалённой связи

Этапы описаны ниже:

- a. Во время эксплуатации транспортного средства (зажигание ON) тахограф передаёт данные на функцию БУ. Функция БУ подготавливает *данные* для функции удалённой связи (зашифрованной) и обновляет данные *VUPM*, хранящиеся в памяти *DSRC-VU* (как указано в 4.1.1.1-4.1.1.2). Собранные *данные* представлены в формате, описанном ниже в пунктах 5.4.4-5.4.5.
- b. Каждый раз, когда *данные* обновляются, обновляется и временная метка, указанная в данных безопасности.
- c. Функция *VUSM* защищает данные в соответствии с процедурами, указанными в приложении 11.
- d. Каждый раз, когда *данные* обновляются (см. 4.1.1.1-4.1.1.2), они передаются в *DSRC-VU*, где заменяют любые прежние данные, чтобы обновлённые текущие данные (*данные*) всегда были в наличии на случай проверки *REDCR*. При передаче данных из БУ в *DSRC-VU* *данные* поддаются идентификации по названию файла *RTMData* или по ApplicationID и идентификаторам свойств.
- e. Если представитель компетентных контрольных органов хочет выбрать какое-то транспортное средство и собрать его *данные*, сначала он вводит свою карточку в *REDCR*, чтобы установить *связь* и позволить *SM-REDCR* проверить её подлинность и расшифровать данные.
- f. Затем представитель компетентного контрольного органа проводит целевую проверку транспортного средства и запрашивает данные при помощи удалённой связи. *REDCR* открывает сеанс связи через интерфейс DSRC 5,8 ГГц с *DSRC-VU* проверяемого транспортного средства и запрашивает *данные*. *Данные* передаются в *REDCR* через систему беспроводной связи как свойство DSRC при помощи приложения GET, как указано в 5.4. Свойство выражено значениями зашифрованных полезных данных и данных безопасности DSRC.
- g. Данные анализирует аппаратура *REDCR*, и они передаются представителю компетентного контрольного органа.
- h. Представитель компетентного контрольного органа использует данные для принятия решения, остановить ли транспортное средство для тщательной проверки или попросить другого представителя компетентного контрольного органа остановить транспортное средство.

### 5.2.2 Толкование данных, полученных через связь DSRC

DSC\_26 Данные, полученные через интерфейс 5,8 ГГц, соответствуют определению в пунктах 5.4.4 и 5.4.5 и только ему и понимаются только в связи с обозначенными там целями. В соответствии с положениями Регламента (ЕС) № 165/2014 *данные* используются только для предоставления актуальной информации компетентному контрольному органу, чтобы помочь ему установить, какое транспортное средство следует задержать для физического осмотра, и впоследствии уничтожаются в соответствии со статьёй 9 Регламента (ЕС) № 165/2014.

## 5.3 Параметры физического интерфейса DSRC для удалённой связи

### 5.3.1 Ограничения, связанные с расположением

DSC\_27 Удалённый контроль 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 данных**

- DSC\_28 Оборудование, используемое для удалённого мониторинга тахографов, соответствует ERC70-03 и работает согласно этому стандарту и параметрам, представленным ниже в таблицах 14.1 и 14.2.
- DSC\_29 Кроме того, чтобы обеспечить совместимость с эксплуатационными параметрами других стандартизированных систем DSRC 5,8 Гц, оборудование, используемое для удалённого мониторинга тахографов, соответствует параметрам EN 12253 и EN 13372.

В частности:

Таблица 14.1. Параметры нисходящих данных

№	Параметр	Значение (-я)	Примечание
D1	Частоты несущих нисходящих данных	В REDCR могут использоваться четыре варианта: 5,7975 ГГц 5,8025 ГГц 5,8075 ГГц 5,8125 ГГц	Согласно ERC 70-03. Частоты несущих может выбрать установщик придорожной системы, и они не должны обязательно быть известны в DSRC-VU (в соответствии с EN 12253, EN 13372)
D1a (*)	Допустимое отклонение несущих	в диапазоне $\pm 5$ м.д.	(в соответствии с EN 12253)
D2(*)	Маскировка спектра передатчика RSU (REDCR)	Согласно ERC 70-03. REDCR соответствует классам В,С согласно определению в EN 12253 .  В настоящем приложении других конкретных требований нет	Параметр, используемый для контроля помех между находящимися поблизости контролёрами (в соответствии с определением в EN 12253 и EN 13372).
D3	Минимальный диапазон частот	5,795-5,815 ГГц	(в соответствии с EN 12253)
D4 (*)	Макс. E.I.R.P.	Согласно ERC 70-03 (без лицензии) и национальным нормам Макс. +33 dBm	(в соответствии с EN 12253)
D4a	Угловая маскировка E.I.R.P.	В соответствии с заявленной и опубликованной спецификацией проектировщика контрольного	(в соответствии с EN 12253)
D5	Поляризация	Левая круговая	(в соответствии с EN 12253)
D5a	Перекры́стная поляризация	XPD: В осевом направлении: (REDCR) RSU t 15 dB (DSRC-VU) OBU r 10 dB При -3 dB: (REDCR) RSU t 10 dB (DSRC-VU) OBU r 6 dB	(в соответствии с EN 12253)
D6 (*)	Модуляция	Двухуровневая амплитудная модуляция.	(в соответствии с EN 12253)
D6a (*)	Показатель модуляции	0,5 ... 0,9	(в соответствии с EN 12253)
D6b	Глазковая индикация	$\geq 90$ % (время) / $\geq 85$ % (амплитуда)	
D7 (*)	Кодирование данных	FM0 У «1» бит есть переключения в начале и конце межбитового интервала. У «0» бит есть дополнительное переключение в середине межбитового интервала по сравнению с «1» бит.	(в соответствии с EN 12253)

<b>D8 (*)</b>	Скорость передачи данных	500 кбит/с	(в соответствии с EN 12253)
<b>D8a</b>	Допустимое отклонение битового тактового сигнала	лучше, чем $\pm 100$ м.д.	(в соответствии с EN 12253)
<b>D9(*)</b>	Интенсивность битовых ошибок (В.Е.Р.) при связи	$\leq 10^{-6}$ , когда мощность падающего луча в OBU (DSRC-VU) находится в диапазоне, заданном [D11a-D11b].	(в соответствии с EN 12253)
<b>D10</b>	Сигнал побудки OBU (DSRC-VU)	OBU (DSRC-VU) активируется по получении любого фрейма с 11 или более октетами (включая преамбулу)	В особой модели побудки необходимости нет. DSRC-VU может активироваться при получении фрейма, в котором менее 11 октетов (в соответствии с EN 12253)
<b>D10a</b>	Макс. время начала	$\leq 5$ мс	(в соответствии с EN 12253)
<b>D11</b>	Зона связи	Область пространства, в которой достигается В.Е.Р. в соответствии с D9.	(в соответствии с EN 12253)
<b>D11a (*)</b>	Предел мощности при связи (верхний).	-24dBm	(в соответствии с EN 12253)
<b>D11b (*)</b>	Предел мощности при связи (нижний).	Мощность падающего луча: -43 dBm (осевое направление) -41 dBm (в пределах $-45^\circ$ - $+45^\circ$ в соответствии с плоскостью, параллельной поверхности дороги, когда впоследствии DSRC-VU устанавливается на транспортном средстве (азимут))	(в соответствии с EN 12253) Расширенное требование для горизонтальных углов до $\pm 45^\circ$ согласно вариантам использования, представленным в настоящем приложении.
<b>D12(*)</b>	Уровень отключённой мощности (DSRC-VU)	-60 dBm	(в соответствии с EN 12253)
<b>D13</b>	Преамбула	Преамбула обязательна.	(в соответствии с EN 12253)
<b>D13a</b>	Длина и модель преамбулы	16 бит $\pm$ 1 бит FM0 с кодировкой «1» бит	(в соответствии с EN 12253)
<b>D13b</b>	Форма волны преамбулы	Знакопеременная последовательность низкого и высокого уровней с продолжительностью импульса 2 мс. Допустимое отклонение указано в	(в соответствии с EN 12253)



<b>D13c</b>	Конечные биты	RSU (REDCR) может передавать не более 8 бит после конечной метки. OBU (DSRC-VU) не обязан учитывать эти дополнительные биты.	(в соответствии с EN 12253)
-------------	---------------	---	-----------------------------

(\*) - Параметры нисходящих данных, подлежащие аттестационным испытаниям в соответствии с определёнными испытаниями параметров согласно EN 300 674-1

**Таблица 14.2. Параметры восходящих данных**

№	Параметр	Значение (-я)	Примечание
<b>U1 (*)</b>	Частоты поднесущих	OBU (DSRC-VU) поддерживает 1,5 мГц и 2,0 мГц  RSU (REDCR) поддерживает 1,5 мГц или 2,0 мГц или оба. U1-0: 1,5 мГц U1-1:	Выбор частоты поднесущих (1,5 мГц или 2,0 мГц) зависит от выбранного набора характеристик EN 13372.
<b>U1a(*)</b>	Допустимое отклонение частот	в пределах 0,1%	(в соответствии с EN 12253)
<b>U1b</b>	Использование полос боковых частот	Одни и те же данные с обеих сторон	(в соответствии с EN 12253)
<b>U2 (*)</b>	Маскировка спектра передатчика OBU (DSRC-VU)	В соответствии с EN12253 1) Внеполосная мощность: см. ETSI EN 300674-1 2) Внутриполосная мощность: [U4a] dBm при 500 кГц 3) Излучение в любом другом восходящем канале: U2(3)-1 = -35 dBm при 500 кГц	(в соответствии с EN 12253)
<b>U4a (*)</b>	Макс. одна боковая полоса E.I.R.P. (осевое направление)	Два варианта: U4a-0: -14 dBm U4a-1: -21 dBm	В соответствии с заявленной и опубликованной спецификацией проектировщика оборудования
<b>U4b (*)</b>	Макс. одна боковая полоса E.I.R.P. (35°)	Два варианта: - Неприменимо - -17dBm	В соответствии с заявленной и опубликованной спецификацией проектировщика оборудования
<b>U5</b>	Поляризация	Левая круговая	(в соответствии с EN 12253)
<b>U5a</b>	Перекры́стная поляризация	XPD: В осевом направлении: (REDCR) RSU r 15 dB (DSRC-VU) OBU t 10 dB При -3 dB: (REDCR) RSU r 10 dB (DSRC-VU) OBU t 6 dB	(в соответствии с EN 12253)

<b>U6</b>	Модуляция поднесущих	2-PSK  Кодированные данные, синхронизируемые с поднесущими: Передачи кодированных данных совпадают с передачами поднесущих.	(в соответствии с EN 12253)
<b>U6b</b>	Цикл нагрузки	Цикл нагрузки: 50% ± α, α ≤ 5%	(в соответствии с EN 12253)
<b>U6c</b>	Модуляция несущих	Умножение модулированных поднесущих на несущие.	(в соответствии с EN 12253)
<b>U7 (*)</b>	Кодирование данных	NRZI (нет переключения в начале «1» бита, переключение в начале «0» бита, нет переключения внутри бита)	(в соответствии с EN 12253)
<b>U8 (*)</b>	Скорость передачи данных	250 кбит/с	(в соответствии с EN 12253)
<b>U8a</b>	Допустимое отклонение	в диапазоне ± 1000 м.д.	(в соответствии с EN 12253)
<b>U9</b>	Интенсивность битовых ошибок	≤ 10 <sup>-6</sup>	(в соответствии с EN 12253)
<b>U11</b>	Зона связи	Область пространства, в которой DSRC-VU расположено таким образом, чтобы его передачи получало REDCR с В.Е.Р. менее указанного в U9a.	(в соответствии с EN 12253)
<b>U12a(*)</b>	Усиление преобразования (нижний предел)	1 dB для каждой боковой полосы Угловой диапазон: Круговая симметрия между осевым направлением и ± 35° и в пределах -45°-+45° в соответствии с плоскостью, параллельной поверхности дороги, когда впоследствии DSRC-VU	Более конкретного диапазона значений, указанных для горизонтальных углов до ±45° согласно вариантам использования,
<b>U12b(*)</b>	Усиление преобразования (верхний предел)	10 dB для каждой боковой полосы	Менее конкретного диапазона значений для каждой боковой полосы в круговом конусе в районе осевого направления ± 45° угла раскрытия
<b>U13</b>	Преамбула	Преамбула обязательна.	(в соответствии с EN 12253)
<b>U13a</b>	Преамбула Длина и модель	32-36 μс, модулированная только для поднесущих, затем 8 битов NRZI с кодировкой «0» бит.	(в соответствии с EN 12253)
<b>U13b</b>	Конечные биты	DSRC-VU может передавать не более 8 бит после конечной метки. RSU (REDCR) не обязан учитывать эти дополнительные биты.	(в соответствии с EN 12253)

(\*) - Параметры восходящих данных, подлежащие аттестационным испытаниям в соответствии с определёнными испытаниями параметров согласно EN 300 674-1

### 5.3.3 Проект антенны

#### 5.3.3.1 Антенна REDCR

DSC\_30 Проект антенны *REDCR* зависит от коммерческого проекта и находится в пределах, указанных в пункте 5.3.2, адаптированных для оптимизации считывания *DSRC-REDCR* для конкретной цели и с учётом обстоятельств считывания, в которых *REDCR* должен работать.

#### 5.3.3.2 Антенна БУ

DSC\_31 Проект антенны *DSRC-VU* зависит от коммерческого проекта и находится в пределах, указанных в пункте 5.3.2, адаптированных для оптимизации считывания *DSRC-REDCR* для конкретной цели и с учётом обстоятельств считывания, в которых *REDCR* должен работать.

DSC\_32 Антенна БУ прикрепляется к переднему лобовому стеклу транспортного средства или рядом с ним, как указано в пункте 5.1.

DSC\_33 В испытательной среде в мастерской (см. раздел 6.3) антенна *DSRC-VU*, прикреплённая в соответствии с пунктом 5.1, успешно соединяется со стандартным испытательным оборудованием и успешно выполняет операцию RTM, как указано в настоящем приложении, на расстоянии от 2 до 10 метров, лучше, чем в 99% времени, при среднем значении более 1000 контрольных считываний.

## 5.4 Протокольные требования DSRC к RTM

### 5.4.1 Обзор

DSC\_34 Протокол операции по загрузке *данных* в соединении интерфейса DSRC 5,8 ГГц реализуется в рамках следующих этапов. В настоящем разделе описана последовательность операций в идеальных условиях без повторных передач или перерывов связи.

**ПРИМЕЧАНИЕ** Цель этапа инициализации (этап 1) – установить связь между *REDCR* и *DSRC-VU*, попавших в зону операции DSRC 5,8 ГГц (ведущий-ведомый), но ещё не установивших связь с *REDCR*, и передавать уведомления о процессах в приложении.

**Этап 1** Инициализация. *REDCR* передаёт 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 отвечает (см. ниже), выдавая перечень поддерживаемых приложений в области Freight&Fleet, или не отвечает, если никакие приложения не поддерживаются. Если *REDCR* не предлагает AID = 2, *DSRC-VU* не отвечает *REDCR*.

**Этап 2** *DSRC-VU* передаёт фрейм с запросом назначить частное окно.

**Этап 3** *REDCR* передаёт фрейм с назначенным частным окном.

**Этап 4** *DSRC-VU* использует назначенное частное окно для передачи фрейма с таблицей 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 контекстной метки приложения с указанием на приложение и поддерживаемый стандарт.

**Этап 5** Затем *REDCR* анализирует предложенную VST и прерывает связь (RELEASE), так как больше в VST ничего не интересует (т.е. получает VST из *DSRC-VU*, которое не поддерживает операцию RTM), или, если получает соответствующую VST, запускает инстанцирование приложения.

- Этап 6** Для этого REDCR передаёт фрейм с командой для извлечения данных RTM с указанием инстанцирования приложения RTM и идентификатора, соответствующего инстанцированию приложения RTM (как DSRC-VU указывает в VST), и назначает частное окно.
- Этап 7** DSRC-VU использует назначенное частное окно для передачи фрейма, в котором содержится адресный идентификатор, соответствующий инстанцированию приложения RTM, как указано в VST, с последующим свойством *RtmData* (полезный элемент + элемент безопасности).
- Этап 8** Если поданы запросы на многие услуги, значение «n» меняется на следующий номер услуги, и процесс повторяется.
- 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 к этапу 6.

Наглядное описание протокола операции представлено на рисунке 14.6.

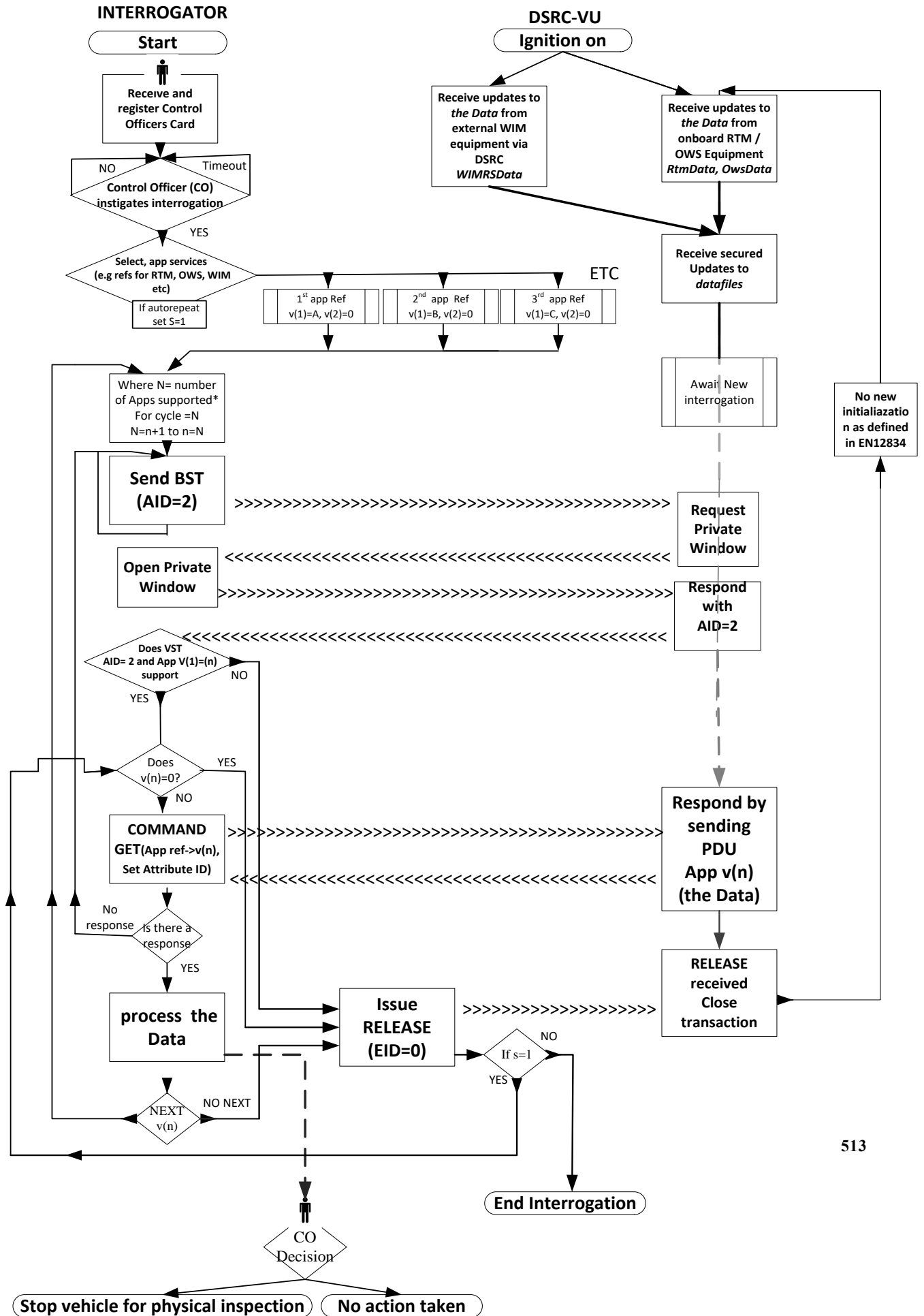


Рисунок 14.6. RTM в рамках последовательности процессов DSRC 5,8 ГГц

### 5.4.2 Команды

- DSC\_35 Следующие команды являются единственными функциями, используемыми на этапе операции RTM
- **INITIALISATION.request:** Команда, выдаваемая REDCR, в форме передачи определения приложений, которые поддерживает REDCR.
  - **INITIALISATION.response:** Ответ DSRC-VU, подтверждающий соединение и содержащий перечень поддерживаемых вариантов приложения с характеристиками и информацией об обращении к ним (EID).
  - **GET.request:** Команда, передаваемая REDCR в DSRC-VU, которая указывает на инстанцирование приложения с адресацией при помощи определённого EID, как получено в VST, и указанием DSRC-VU передать выбранное свойство (-а) вместе с *данными*. Цель команды GET – чтобы REDCR получало *данные* из DSRC-VU.
  - **GET.response:** Ответ DSRC-VU, в котором содержатся запрашиваемые *данные*.
  - **ACTION.request ECHO:** Команда, указывающая DSRC-VU отправить обратно данные с DSRC-VU в REDCR. Цель команды ECHO – позволить мастерским или испытательным органам официального утверждения типа испытывать, что связь DSRC работает, без необходимости доступа к данным безопасности.
  - **ACTION.response ECHO:** Ответ DSRC VU на команду ECHO.
  - **EVENT\_REPORT.request RELEASE:** Команда, указывающая DSRC-VU, что операция закончена. Цель команды RELEASE – завершить сеанс с DSRC-VU. По получении RELEASE DSRC-VU не отвечает на любые другие запросы в рамках данного сеанса связи. Следует отметить, 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 контрольного устройства.

### 5.4.3 Последовательность контрольных команд

DSC\_36 С точки зрения последовательности команды и ответа операция описывается следующим образом:

Последов	Отправ		Получа	Описание	Д
1	REDCR	>	DSRC-VU	Начало связи	REDCR передаёт BST
2	DSRC-VU	>	REDCR	– запрос Начало связи – ответ	Если BST поддерживает AID = 2, DSRC-VU запрашивает частное окно
3	REDCR	>	DSRC-VU	Предоставляет частное окно	Передаёт фрейм с назначенным
4	DSRC-VU	>	REDCR	Передаёт VST	Передаёт фрейм с VST
5	REDCR	>	DSRC-VU	Передаёт GET.request в отношении данных свойства	
6	DSRC-VU	>	REDCR	Передаёт GET.response с запрашиваемым свойством в отношении конкретного EID	Передаёт свойство (RTMData, OWSDData....) с
7	REDCR	>	DSRC-VU	Передаёт GET.request по данным другого свойства	

8	DSRC-VU	>	REDCR	Передаёт GET.response с запрашиваемым свойством	Передаёт свойство с данными о конкретном
9	REDCR	>	DSRC-VU	Подтверждает успешное получение данных	Передаёт команду RELEASE, закрывающую операцию
1	DSRC-VU			Закрывает операцию	

Пример последовательности операции и содержания фреймов, участвующих в обмене, представлен в пунктах 5.4.7 и 5.4.8

#### 5.4.4 Структуры данных

DSC\_37 Семантическая структура *данных*, передаваемых через интерфейс DSRC 5,8 Гц, соответствует описанию, данному в настоящем приложении. Структура таких данных описана в настоящем пункте.

DSC\_38 Полезная нагрузка (данные RTM) состоит из конкатенации

1. данных EncryptedTachographPayload, представляющих собой зашифрованные данные TachographPayload, описанные в ASN.1 в разделе 5.4.5. Метод шифрования описан в приложении 11
2. DSRCSecurityData, как указано в приложении 11.

DSC\_39 Обращение к данным RTM выглядит как свойство RTM = 1, и они передаются в хранилище RTM = 10.

DSC\_40 Метка контекста RTM определяет поддерживаемый стандарт в серии стандартов TARV (RTM соответствует части 9)

Определение модуля ASN.1 для данных DSRC в приложении RTM выглядит следующим образом:

```
TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
DEFINITIONS AUTOMATIC TAGS
 ::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for RTM
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
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 EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)}

-- Definitions of the RTM functions:
RTM-InitialiseComm-Request ::= BST
RTM-InitialiseComm-Response ::= VST
```

RTM-DataRetrieval-Request ::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT, iid ABSENT, attrIdList})

RTM-DataRetrieval-Response ::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})

RTM-TerminateComm ::= Event-Report-Request {RtmContainer} (WITH COMPONENTS {mode (FALSE), eid (0), eventType (0)})

RTM-TestComm-Request ::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType (15), accessCredentials ABSENT, iid ABSENT})

RTM-TestComm-Response ::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid (0), iid ABSENT})

-- Definitions of the RTM attributes:

RtmData ::= SEQUENCE {

    encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting TachographPayload as per Appendix 11 --}),

    DSRCSecurityData OCTET STRING

}

TachographPayload ::= SEQUENCE {

tp15638VehicleRegistrationPlate	LPN -- Vehicle Registration Plate as per EN 15509.
tp15638SpeedingEvent	BOOLEAN, -- 1= Irregularities in speed (see Annex 1C)
tp15638DrivingWithoutValidCard	BOOLEAN, -- 1= Invalid card usage (see Annex 1C)
tp15638DriverCard	BOOLEAN, -- 0= Indicates a valid driver card (see Annex 1C)
tp15638CardInsertion	BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
tp15638MotionDataError	BOOLEAN, -- 1= Motion data error (see Annex 1C)
tp15638VehicleMotionConflict	BOOLEAN, -- 1= Motion conflict (see Annex 1C)
tp156382ndDriverCard	BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
tp15638CurrentActivityDriving	BOOLEAN, -- 1= other activity selected; -- 0= driving selected
tp15638LastSessionClosed	BOOLEAN, -- 1= improperly, 0= properly, closed
tp15638PowerSupplyInterruption	INTEGER (0..127), -- Supply interrupts in the last 10 days
tp15638SensorFault	INTEGER (0..255), -- eventFaultType as per data dictionary

-- All subsequent time related types as defined in Annex 1C.

tp15638TimeAdjustment	INTEGER(0..4294967295), -- Time of the last time adjustment
tp15638LatestBreachAttempt	INTEGER(0..4294967295), -- Time of last breach attempt
tp15638LastCalibrationData	INTEGER(0..4294967295), -- Time of last calibration data
tp15638PrevCalibrationData	INTEGER(0..4294967295), -- Time of previous calibration data



```

tp15638DateTachoConnected    INTEGER(0..4294967295), -- Date tachograph connected

                                tp15638CurrentSpeed          INTEGER (0..255), -- Last current recorded speed
                                tp15638Timestamp             INTEGER(0..4294967295) -- Timestamp of current record2
                                }
Rtm-ContextMark ::= SEQUENCE {
    standardIdentifier StandardIdentifier, -- identifier of the TARV part and its version

    RtmCommProfile      INTEGER {
                                C1 (1),
                                C2 (2)
                                } (0..255) DEFAULT 1
    }
RtmTransferAck ::= INTEGER {
    Ok (1),
    NoK (2)
    } SIZE (1..255)

StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
    integer           [0] INTEGER,
    bitstring         [1] BIT STRING,
    octetstring       [2] OCTET STRING (SIZE (0..127, ...)),
    universalString   [3] UniversalString,
    beaconId          [4] BeaconID,
    t-apdu            [5] T-APDUs,
    dsrcApplicationEntityId [6] DSRCApplicationEntityID,
    dsrc-Ase-Id       [7] Dsrc-EID,
    attrIdList        [8] AttributeIdList,
    attrList          [9] AttributeList{RtmContainer},
    rtmData           [10] RtmData,
    rtmContextmark    [11] Rtm-ContextMark,
    reserved12        [12] NULL,
    reserved13        [13] NULL,
    reserved14        [14] NULL,
    time              [15] Time,
    -- values from 16 to 255 reserved for ISO/CEN usage
    }
END

```

### 5.4.5 Элементы RtmData, выполняемые действия и определения

DSC\_41 Значения данных, которые рассчитывает БУ и которые используются для обновления защищённых 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, производимое БУ		(3) Определение данных ASN 1
<b>RTM1</b> Регистрационный номер транспортного средства	БУ устанавливает значение элемента данных <i>tp15638VehicleRegistrationPlate</i> RTM1 по зарегистрированному значению типа данных <i>VehicleRegistrationIdentification</i> , как указано в приложении 1 <i>VehicleRegistrationIdentification</i>	Регистрационный номер транспортного средства в виде строки символов	<i>tp15638VehicleRegistrationPlate</i> LPN, --Регистрационный номер транспортного средства, импортированный из ISO 14906 с ограничением, указанным в EN 15509, т.е. SEQUENCE, включающая в себя код страны, затем алфавитный указатель и сам регистрационный номер, в которой уже есть 14 октетов (заполненных нулями), чтобы длина типа EN
<b>RTM2</b> Событие превышения скорости	БУ генерирует логическое значение элемента данных RTM2 <i>tp15638SpeedingEvent</i> .  Значение <i>tp15638SpeedingEvent</i> вычисляется БУ по числу событий превышения скорости, записанных в БУ за последние 10 дней, как указано в приложении 1С.  Если есть хотя бы одно <i>tp15638SpeedingEvent</i> за последние 10 дней, значение <i>tp15638SpeedingEvent</i> устанавливается как TRUE.	1 (TRUE) указывает на нарушения скорости за последние 10 дней	<i>tp15638speedingEvent</i> BOOLEAN,

<b>RTM3</b> <b>Управление без действительной карточки</b>	<p>БУ генерирует логическое значение элемента данных RTM3 tp15638DrivingWithoutValidCard.</p> <p>БУ присваивает значение True переменной tp15638DrivingWithoutValidCard, если за последние 10 дней данные БУ зарегистрировали хотя бы одно событие типа управления без действительной карточки, как указано в приложении 1С.</p> <p>ПИБО если за последние 10 дней</p>	<p>1 (TRUE) = указывает на использование недействительной карточки</p>	<p>tp15638DrivingWithoutValidCard          BOOLEAN,</p>
<b>RTM4</b> <b>Действительная карточка водителя</b>	<p>БУ генерирует логическое значение элемента данных RTM4 tp15638DriverCard на основе данных, хранящихся в БУ, как описано в приложении 1.</p> <p>Если действительной карточки водителя нет, БУ устанавливает значение переменной как TRUE</p>	<p>0 (FALSE) = указывает на отсутствие действительной карточки водителя</p>	<p>tp15638DriverCard          BOOLEAN,</p>
<b>RTM5</b> <b>Ввод карточки во время управления</b>	<p>БУ генерирует логическое значение элемента данных RTM5.</p> <p>БУ присваивает значение TRUE переменной tp15638CardInsertion, если за последние 10 дней данные БУ зарегистрировали хотя бы одно событие типа ввода карточки во время управления, как указано в приложении 1С.</p>	<p>1 (TRUE) = указывает на ввод карточки во время управления в течение последних 10 дней</p>	<p>tp15638CardInsertion          BOOLEAN,</p>
<b>RTM6</b> <b>Ошибочные данные о движении</b>	<p>БУ генерирует логическое значение элемента данных RTM6.</p> <p>БУ присваивает значение TRUE переменной tp15638MotionDataError, если за последние 10 дней данные БУ зарегистрировали хотя бы одно событие типа ошибочных данных о движении, как указано в приложении 1С.</p>	<p>1 (TRUE) = указывает на ошибочные данные о движении за последние 10 дней</p>	<p>tp15638motionDataError          BOOLEAN,</p>

<b>RTM7</b> <b>Противоречивые данные о движении транспортного средства</b>	<p>БУ генерирует логическое значение элемента данных RTM7.</p> <p>БУ присваивает значение TRUE переменной tp15638vehicleMotionConflict, если за последние 10 дней данные БУ зарегистрировали хотя бы одно событие типа противоречивых данных о движении транспортного средства</p>	<p>1 (TRUE) = указывает на противоречивые данные о движении за последние 10 дней</p>	<p>tp15638vehicleMotionConflict          BOOLEAN,</p>
<b>RTM8</b> <b>Карточка второго водителя</b>	<p>БУ генерирует логическое значение элемента данных RTM8 на основе приложения 1С (данные деятельности водителя CREW и CO-DRIVER).</p> <p>Если карточка второго водителя присутствует, БУ устанавливает значение переменной как TRUE</p>	<p>1 (FALSE) = указывает на то, что введена карточка второго водителя</p>	<p>tp156382ndDriverCard          BOOLEAN,</p>
<b>RTM9</b> <b>Текущая деятельность</b>	<p>БУ генерирует логическое значение элемента данных RTM9.</p> <p>Если текущая деятельность установлена в БУ как любая деятельность, кроме DRIVING, как указано в приложении 1С, БУ устанавливает значение переменной как TRUE</p>	<p>1 (TRUE) = выбрана другая деятельность;          0 (FALSE) = выбрано управление</p>	<p>tp15638currentActivityDriving          BOOLEAN</p>
<b>RTM10</b> <b>Закрытие последнего сеанса</b>	<p>БУ генерирует логическое значение элемента данных RTM10.</p> <p>Если последний сеанс с карточкой должным образом не завершён, как указано в приложении 1С, БУ устанавливает значение переменной как TRUE</p>	<p>1 (TRUE) = закрыто ненадлежащим образом          0 (FALSE) = закрыто надлежащим образом</p>	<p>tp15638lastSessionClosed          BOOLEAN</p>

<b>RTM11</b> <b>Перерыв</b> <b>в питании</b>	<p>БУ генерирует целое число как значение элемента данных RTM11.</p> <p>БУ присваивает значение переменной tp15638PowerSupplyInterruption, равное самому длительному перерыву питания в соответствии со статьёй 9 Регламента (ЕС) № 165/2014 типа перерыв в питании, как</p>	-- Число перерывов в питании за последние 10 дней	tp15638powerSupplyInterruption INTEGER (0..127),
<b>RTM12</b> <b>Неисправность датчика</b>	<p>БУ генерирует значение целого числа элемента данных RTM12.</p> <p>БУ присваивает переменной sensorFault значение:</p> <p>- 1, если за последние 10 дней зарегистрировано событие типа '35'Н Неисправность датчика,</p> <p>- 2 если за последние 10 дней зарегистрировано событие типа неисправности приёмника ГНСС (с внутренним или внешним значением '51'Н или '52'Н)</p> <p>- 3 если за последние 10 дней зарегистрировано событие типа '53'Н Неисправность связи внешнего устройства ГНСС.</p> <p>-4 если за последние 10 дней зарегистрированы неисправности и датчика, и приёмника ГНСС</p> <p>-5 если за последние 10 дней зарегистрированы неисправности датчика и связи внешнего устройства ГНСС</p>	-- неисправность датчика один октет в соответствии со словарём данных	tp15638SensorFault INTEGER (0..255),

<b>RTM13</b> <b>Корректировка</b> <b>времени</b>	<p>БУ генерирует целое число (timeReal из приложения 1) для элемента данных RTM13 на основе имеющихся данных корректировки времени, как указано в приложении 1С.</p> <p>БУ присваивает значение времени, когда произошло последнее событие корректировки времени.</p>	Время последней корректировки времени	tp15638TimeAdjustment INTEGER(0..4294967295),
<b>RTM14</b> <b>Попытка нарушения</b> <b>защиты</b>	<p>БУ генерирует целое число (timeReal из приложения 1) для элемента данных RTM14 на основе имеющихся данных попытки нарушения защиты, как указано в приложении 1С.</p> <p>БУ устанавливает значение времени последней попытки нарушения защиты, записанной в БУ.</p>	Время последней попытки нарушения -- Значение по умолчанию =0x00FF	tp15638LatestBreachAttempt INTEGER(0..4294967295),
<b>RTM15</b> <b>Последняя</b> <b>калибровка</b>	<p>БУ генерирует целое число (timeReal из приложения 1) для элемента данных RTM15 на основе имеющихся данных последней калибровки, как указано в приложении 1С.</p> <p>БУ устанавливает значение времени последних двух калибровок (RTM15 и RTM16), установленных в VuCalibrationData, как указано в</p>	Время последних данных калибровки	tp15638LastCalibrationData INTEGER(0..4294967295),
<b>RTM16</b> <b>Предыдущая</b> <b>калибровка</b>	<p>БУ генерирует целое число (timeReal из приложения 1) для элемента данных RTM16 на основе имеющихся данных предпоследней калибровки.</p> <p>ЛИБО если предыдущей калибровки не было, БУ устанавливает значение RTM16, равное 0.</p>	Данные времени предыдущей калибровки	tp15638PrevCalibrationData INTEGER(0..4294967295),

<b>RTM17</b> <b>Дата присоединения тахографа</b>	<p>Для элемента данных RTM17 БУ генерирует целое значение (timeReal из приложения 1).</p> <p>БУ устанавливает значение времени изначальной установки БУ.</p> <p>БУ извлекает эти данные из VuCalibrationData (приложение 1)</p>	Дата присоединения тахографа	tp15638DateTachoConnected INTEGER(0..4294967295),
<b>RTM18</b> <b>Текущая скорость</b>	<p>БУ генерирует целое число как значение элемента данных RTM18.</p> <p>БУ устанавливает значение RTM16 как последнюю записанную текущую скорость во время последнего обновления</p>	Последняя текущая зарегистрированная скорость	tp15638CurrentSpeed INTEGER (0..255),
<b>RTM19</b> <b>Timestamp</b>	<p>Для элемента данных RTM19 БУ генерирует целое значение (timeReal из приложения 1).</p> <p>БУ устанавливает значение RTM19 как время последнего обновления RtmData.</p>	Временная метка текущей записи TachographPayload	tp15638Timestamp INTEGER(0..4294967295),

### 5.4.6 Механизм передачи данных

DSC\_42 Полезные данные, описанные выше, запрашиваются REDCR после этапа инициализации и затем передаются *DSRC-VU* в выделенное окно. REDCR использует команду GET для извлечения данных.

DSC\_43 Для любого обмена DSRC данные кодируются при помощи PER (правил уплотнённого кодирования).

### 5.4.7 Подробное описание операции DSRC

DSC\_44 Инициализация осуществляется в соответствии с DSC\_44-DSC\_48 и таблицами 14.4-14.9. Во время этапа инициализации REDCR начинает передачу фрейма, содержащего BST (таблицу использования радиомаяков) в соответствии с EN 12834 и EN 13372, 6.2, 6.3, 6.4 и 7.1 с настройками, как указано в следующей таблице 14.4.

**Таблица 14.4. Инициализация. Настройки фрейма BST**

Поле	Настро йки
Идентификатор	Адрес трансляции
BeaconId	Согласно EN 12834
Время	Согласно EN 12834
Характеристики	Без расширения, используются 0 или 1
MandApplications	Без расширения, EID нет, параметра нет, AID = 2 Freight&Fleet
NonMandApplications	Отсутствует
ProfileList	Без расширения, число наборов характеристик в перечне =
Заголовок	Фрагментации нет
Настройки 2-го	Команда PDU, команда UI

Практический пример настроек, перечисленных в таблице 14.4 с указанием битовых шифров, приводится в следующей таблице 14.5.

**Таблица 14.5. Инициализация. Пример содержания фрейма BST**

№ октета	Свойство/поле	Биты в октете	Описание
1	МЕТКА	0111 1110	Стартовая метка
2	Идентификатор трансляции	1111 1111	Адрес трансляции
3	Контрольное поле MAC	1010 0000	Команда PDU
4	Контрольное поле LLC	0000 0011	Команда UI
5	Заголовок фрагментации	1xxx x001	Фрагментации нет
6	BST	1000	Запрос инициализации
	SEQUENCE { OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	Приложений NonMand нет
		xxx	Идентификатор



№ октета	Свойство/поле	Биты в октете	Описание
7		xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	27-битный идентификатор для производителя
9		xxxx xxxx	
10		xxxx xxxx	
11		xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	32-битный UNIX в реальном
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,...)	0000 0000	Без расширения. Пример
17	MandApplications SEQUENCE (SIZE(0..127,...)) OF {	0000 0001	Без расширения, число mandApplications = 1
18	SEQUENCE { OPTION indicator OPTION indicator AID DSRCApplicationEntityID }	0	EID отсутствует
		0	Параметр отсутствует
		00 0010	Без расширения. AID = 2 Freight&Fleet
19	ProfileList SEQUENCE (0..127,...) OF Profile }	0000 0000	Без расширения, число наборов характеристик в
20	FCS	xxxx xxxx	Последовательность проверки фрейма
21		xxxx xxxx	
22	Метка	0111 1110	Конечная метка

DSC\_45 DSRC-VU, получив BST, запрашивает частное окно, как указано в EN 12795 и EN 13372, 7.1.1, без определённых настроек RTM. В таблице 14.6 приводится пример битового шифра.

**Таблица 14.6. Инициализация. Содержание фрейма запроса частного окна**

№ октета	Свойство/поле	Биты в октете	Описание
1	МЕТКА	0111 1110	Стартовая метка
2	Частный LID	xxxx xxxx	Адрес канала конкретного DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Контрольное поле MAC	0110 0000	Запрос на частное окно
7	FCS	xxxx xxxx	Последовательность проверки фрейма
8		xxxx xxxx	
9	Метка	0111 1110	Конечная метка

DSC\_46 Затем REDCR отвечает, выделяя частное окно, как указано в EN 12795 и EN 13372, 7.1.1, без определённых настроек RTM.  
В таблице 14.7 приводится пример битового шифра.

**Таблица 14.6. Инициализация. Содержание фрейма назначения частного окна**

№ октета	Свойство/поле	Биты в октете	Описание
1	МЕТКА	0111 1110	Стартовая метка
2	Частный LID	xxxx xxxx	Адрес канала конкретного DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Контрольное поле MAC	0010 s000	Выделение частного окна
7	FCS	xxxx xxxx	Последовательность проверки фрейма
8		xxxx xxxx	
9	Метка	0111 1110	Конечная метка

DSC\_47 DSRC-VU, получив выделенное частное окно, передаёт 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	Настро
Частный LID	Согласно EN 12834
Параметры VST	Fill = 0, затем для каждого поддерживаемого приложения: EID присутствует, параметр присутствует,
Параметр	Без расширения, содержит метку контекста RTM
ObeConfiguration	Может быть факультативное поле ObeStatus, но REDCR его не использует
Заголовок	Фрагментации нет
Настройки 2-го	Команда PDU, команда UI

DSC\_48 DSRC-VU поддерживает приложение Freight and Fleet, определяемое по идентификатору приложения '2'. Могут поддерживаться 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 отношении каждого поддерживаемого приложения даётся ссылка на соответствующий стандарт, состоящая из метки контекста Rtm в виде OBJECT IDENTIFIER, представляющим соответствующий стандарт, его части (9 в случае RTM) и, возможно, версии, а также EID, который генерирует DSRC-VU, с учётом данного варианта приложения.

Практический пример настроек, перечисленных в таблице 14.8 с указанием битовых шифров, приводится в таблице 14.9.

**Таблица 14.4. Инициализация. Пример  
содержания фрейма VST**

№	Свойство/поле	Биты в октете	Описание
1	МЕТКА	0111 1110	Стартовая метка
2	Частный LID	xxxx xxxx	Адрес канала конкретного DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6		Контрольное поле MAC	
7	Контрольное поле LLC	0000 0011	Команда UI
8	Заголовок фрагментации	1xxx x001	Фрагментации нет
9	VST SEQUENCE { Fill BIT STRING (SIZE(4))	1001	Ответ инициализации
		0000	Не используется и установлено на 0
10	Profile INTEGER (0..127,...)	0000 0000	Без расширения. Пример набора характеристик 0
11		0000 0001	
12	SEQUENCE { OPTION indicator OPTION indicator AID DSRCApplicationEntityID	1	EID присутствует
		1	Параметр присутствует
		00 0010	Без расширения. AID = 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Определяется внутри OBU и определяет вариант приложения.
14	Параметр Container {	0000 0010	Без расширения, выбор хранилища = 02, Октетная строка
15		0000 1000	Без расширения, длина метки контекста Rtm = 8
16	Rtm-ContextMark ::= standardIdentifier	0000 0110	Идентификатор объекта поддерживаемого стандарта, часть и версия. Пример: ISO (1) стандарт (0) TARV (15638) часть 9 (9) Версия 1 (1). Первый октет – 06H, который представлен идентификатором объекта Второй октет – 06H, его длина. Последующие 6 октетов кодируют пример идентификатора объекта Следует отметить, что присутствует только один элемент
17		0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence { OPTION indicator	0	ObeStatus отсутствует
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	

26	ManufacturerId (0..65535)	INTEGER	xxxx xxxx	Идентификатор производителя DSRC-VU, как описано в регистре ISO 14816
27			xxxx xxxx	
28	FCS		xxxx xxxx	Последовательность проверки фрейма
29			xxxx xxxx	
30	Метка		0111 1110	Конечная метка

DCS\_49 Затем REDCR считывает данные, выдавая команду GET, придерживаясь команды GET, представленной в EN 13372, 6.2, 6.3, 6.4 и EN 12834, а настройки – как указано в таблице 14.10.

**Таблица 14.8. Выражение. Настройки фрейма запроса GET**

Поле	Настро
Идентификатор	Отсутствует
Идентификатор канала	Адрес канала конкретного DSRC-VU
Формирование цепочки	Нет
Идентификатор элемента	Как указано в VST. Без расширения
Права доступа	Нет
AttributeIdList	Без расширения, 1 свойство, AttributeID = 1 (RtmData)
Фрагментация	Нет
Настройки 2-го уровня	Команда PDU, команда Polled ACn

Таблица 14.11 приводит пример считывания данных RTM.

**Таблица 14.11. Выражение. Пример фрейма запроса GET**

№	Свойство/поле	Биты в октете	Описание
1	МЕТКА	0111 1110	Стартовая метка
2	Частный LID	xxxx xxxx	Адрес канала конкретного DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Контрольное поле MAC	1010 s000	Команда PDU
7	Контрольное поле LLC	n111 0111	Команда Polled ACn, n бит
8	Заголовок фрагментации	1xxx x001	Фрагментации нет
9	Get.request SEQUENCE { OPTION indicator OPTION indicator OPTION indicator Fill BIT STRING(SIZE(1))	0110	Запрос GET
		0	Права доступа отсутствуют
		0	IID отсутствует
		1	AttributeIdList присутствует
		0	Установлен 0.
10	EID INTEGER(0..127,...)	xxxx xxxx	EID варианта приложения RTM, как указано в VST. Без расширения

11	AttributeldList SEQUENCE OF {	0000 0001	Без расширения, число свойств = 1
12		0000 0001	Attributeld=1, RtmData. Без расширения
13	FCS	xxxx xxxx	Последовательность проверки фрейма
14		xxxx xxxx	
15	Метка	0111 1110	Конечная метка

DSC\_50 *DSRC-VU*, получив запрос GET, передаёт ответ GET с запрашиваемыми данными, придерживаясь команды GET, представленной в EN 13372, 6.2, 6.3, 6.4 и EN 12834, а настройки – как указано в таблице 14.12.

**Таблица 14.12. Выражение. Настройки фрейма ответа GET**

Поле	Настрой
Идентификатор	Отсутствует
Идентификатор канала	Согласно EN 12834
Формирование цепочки	Нет
Идентификатор элемента	Как указано в VST.
Права доступа	Нет
Фрагментация	Нет
Настройки 2-го уровня	Ответ PDU, ответ предоставлен, и команда принята, команда AСп

Таблица 14.13 приводит пример считывания данных RTM.

Таблица 14.13. Выражение. Пример содержания фрейма ответа

№ октета	Свойство/поле	Биты в октете	Описание
1	МЕТКА	0111 1110	Стартовая метка
2	Частный LID	xxxx xxxx	Адрес канала конкретного DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Контрольное поле MAC	1101 0000	PDU ответа
7	Контрольное поле LLC	n111 0111	Ответ предоставлен, команда ACn, n бит
8	Поле статуса LLC	0000 0000	Ответ предоставлен, и команда принята
9	Заголовок фрагментации	1xxx x001	Фрагментации нет
10	Get.response SEQUENCE {	0111	Ответ Get
	OPTION indicator	0	IID отсутствует
	OPTION indicator	1	Перечень свойств присутствует
	OPTION indicator	0	Статус возврата отсутствует
	Fill BIT STRING(SIZE(1))	0	Не используется
11	EID INTEGER(0..127,...)	xxxx xxxx	Ответ из варианта приложения RTM. Без расширения,
12	AttributeList SEQUENCE OF {	0000 0001	Без расширения, число свойств = 1
13	Attributes SEQUENCE { Attributeld	0000 0001	Без расширения, Attributeld = 1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Без расширения, выбор хранилища = 10 <sub>10</sub> .
15		kkkk kkkk	
16		kkkk kkkk	
17		kkkk kkkk	
...		...	
n		}}} kkkk kkkk	
n+1	FCS	xxxx xxxx	Последовательность проверки фрейма
n+2		xxxx xxxx	
n+3	Метка	0111 1110	Конечная метка

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. Таблица 14.14 показывает пример битового шифра команды RELEASE.

Таблица 14.14. Завершение. Содержание фрейма EVENT\_REPORT Release

№	Свойство/поле	Биты в октете	Описание
1	МЕТКА	0111 1110	Стартовая метка
2	Частный LID	xxxx xxxx	Адрес канала конкретного DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Контрольное поле MAC	1000 s000	Фрейм содержит команду LPDU
7	Контрольное поле LLC	0000 0011	Команда UI
8	Заголовок фрагментации	1xxx x001	Фрагментации нет
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Права доступа отсутствуют
	OPTION indicator	0	Параметр события отсутствует
	OPTION indicator Mode BOOLEAN	0	IID отсутствует Ответа не ожидается
10	EID INTEGER (0..127,...)	0000 0000	Без расширения, EID = 0 (система)
11	EventType INTEGER (0..127,...) }	0000 0000	Тип события 0 = Release
12	FCS	xxxx xxxx	Последовательность проверки фрейма
13		xxxx xxxx	
14	Метка	0111 1110	Конечная метка

DSC\_52 Ответа *DSRC-VU* на команду Release не ожидается. После этого связь закрыта.

#### 5.4.8 Описание тестовой операции DSRC

DSC\_53 Полные испытания, включающие в себя и защиту данных, должны проводиться, как описано в приложении 11 «Общие механизмы безопасности», уполномоченными лицами с доступом к процедурам защиты, с обычным использованием команды GET, как описано выше.

DSC\_54 Испытания ввода в эксплуатацию и периодические проверки, требующие расшифровки и понимания содержания расшифрованных данных, проводятся, как описано в приложении 11 «Общие механизмы безопасности» и приложении 9 «Перечень минимальных требуемых испытаний официального утверждения типа».

Однако базовую связь DSRC можно испытать при помощи команды ECHO. Такие испытания могут быть необходимы при вводе в эксплуатацию, периодических проверках или по требованию компетентного контрольного органа или по Регламенту (ЕС) № 165/2014 (см. 6 ниже)

DSC\_55 Для проведения такого базового испытания связи во время сеанса REDCR выдаёт команду ECHO, т.е. после успешного завершения этапа инициализации. Так, последовательность действий похожа на последовательность контрольного запроса:

Этап 1 *REDCR* передаёт 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 Freight&Fleet (AID = 2), *DSRC-VU* выдаёт ответ. Если *REDCR* не предлагает AID = 2, *DSRC-VU* завершает операцию с *REDCR*.

Этап 2 *DSRC-VU* передаёт запрос на частное окно.

Этап 3 *REDCR* шлёт выделенное частное окно.

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 ничего не интересует (т.е. получает VST из DSRC-VU, которое не является БУ RTM), или, если получает соответствующую VST, запускает инстанцирование приложения.

Этап 6 REDCR выдаёт команду (ECHO) конкретному DSRC-VU и выделяет частное окно.

Этап 7 DSRC-VU использует выделенное частное окно для передачи фрейма ответа

ECHO.

В таблице ниже приводится практический пример сеанса обмена командой ECHO.

DSC\_56 Инициализация осуществляется в соответствии с 5.4.7 (DSC\_44-DSC\_48) и таблицами 14.4-14.9.

DSC\_57 Затем REDCR выдаёт команду ACTION, ECHO в соответствии с ISO 14906, содержащую 100 октетов данных, без конкретных настроек RTM. Таблица 14.15 показывает содержание фрейма, который передаёт REDCR.

Таблица 14.15. Пример фрейма запроса ACTION, ECHO

№	Свойство/поле	Биты в октете	Описание	
1	МЕТКА	0111 1110	Стартовая метка	
2	Частный LID	xxxx xxxx	Адрес канала конкретного DSRC-VU	
3		xxxx xxxx		
4		xxxx xxxx		
5		xxxx xxxx		
6		Контрольное поле MAC		1010 s000
7	Контрольное поле LLC	n111 0111	Команда Polled ACn, n бит	
8	Заголовок фрагментации	1xxx x001	Фрагментации нет	
9	ACTION.request	0000	Запрос действия (ECHO)	
	SEQUENCE {			
	OPTION indicator	0		Права доступа отсутствуют
	OPTION indicator	1		Параметр действия присутствует
	OPTION indicator	0		IID отсутствует
	Mode BOOLEAN	1	Ответ ожидается	
10	EID INTEGER	0000 0000	Без расширения, EID = 0 (система)	
11	ActionType INTEGER	0000 1111	Без расширения, тип действия запроса	
12	ActionParameter CONTAINER {	0000 0010	Без расширения, выбор хранилища =	
13		0110 0100	Без расширения. Длина строки = 100	
14		xxxx xxxx	Данные, подлежащие дублированию	
...		...		
113		}} xxxx xxxx		
114	FCS	xxxx xxxx	Последовательность проверки фрейма	
115		xxxx xxxx		
116	Метка	0111 1110	Конечная метка	

DSC\_58 *DSRC-VU*, получив запрос ECHO, передаёт ответ ECHO из 100 октетов данных, отражая полученную команду в соответствии с ISO 14906, без конкретных настроек RTM. Таблица 14.16 приводит пример кодирования на уровне битов.

Таблица 14.16. Пример фрейма ответа ACTION, ECHO

№ октета	Свойство/поле	Биты в октете	Описание
1	МЕТКА	0111 1110	Стартовая метка
2	Частный LID	xxxx xxxx	Адрес канала конкретного БУ
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Контрольное поле MAC	1101 0000	PDU ответа
7	Контрольное поле LLC	n111 0111	Команда ACn n бит
8	Поле статуса LLC	0000 0000	Ответ предоставлен
9	Заголовок фрагментации	1xxx x001	Фрагментации нет
10	ACTION.response SEQUENCE {	0001	Ответ ACTION (ECHO)
	OPTION indicator	0	IID отсутствует
	OPTION indicator	1	Параметр ответа присутствует
	OPTION indicator	0	Статус возврата отсутствует
	Fill BIT STRING (SIZE (1))	0	Не используется
11	EID INTEGER (0..127,...)	0000 0000	Без расширения, EID = 0 (система)
12	ResponseParameter CONTAINER {	0000 0010	Без расширения, выбор хранилища
13		0110 0100	Без расширения. Длина строки = 100
14		xxxx xxxx	Дублируемые данные
...		....	
113		xxxx xxxx	
114	FCS	xxxx xxxx	Последовательность проверки фрейма
115		xxxx xxxx	
116	Метка	0111 1110	Конечная метка

## 5.5 Поддержка Директивы 2015/71/ЕС

### 5.5.1 Обзор

DSC\_59 Для поддержки Директивы 2015/719/ЕС о максимальном весе и габаритах большегрузных транспортных средств протокол операции загрузки данных OWS через канал интерфейса DSRC 5,8 ГГц будет таким же, как протокол, используемый для данных RTM (см. 5.4.1), с единственной разницей в том, что идентификатор объекта, связанный со стандартом TARV, будет обращаться к стандарту ISO 15638 (TARV), часть 20, связанному с WOB/OWS.

### 5.5.2 Команды

DSC\_60 Команды, используемые для операции OWS, такие же, как команды, используемые для операции RTM.

### 5.5.3 Последовательность контрольных команд

DSC\_61 Последовательность контрольных команд для данных OWS такая же, как и для данных RTM.

## 5.5.4 Структуры данных

DSC\_62 Полезная нагрузка (данные OWS) состоит из конкатенации

1. данных EncryptedOwsPayload, представляющих собой зашифрованные данные OwsPayload, описанные в ASN.1 в разделе 5.5.5. Способ шифрования такой же, как и для RtmData, как описано в приложении 11
2. DSRCSecurityData, вычисляемые при помощи тех же алгоритмов, что RtmData, как указано в приложении 11.

## 5.5.5 Модуль ASN.1 для операции OWS DSRC

DSC\_63. Определение модуля ASN.1 для данных DSRC в приложении RTM выглядит следующим образом:

```
TarvOws {iso(1) standard(0) 15638 part20(20)
version1(1)} DEFINITIONS AUTOMATIC TAGS
 ::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for OWS
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
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 EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

-- Definitions of the OWS functions:
OWS-InitialiseComm-Request ::= BST
OWS-InitialiseComm-Response ::= VST
OWS-DataRetrieval-Request ::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT, iid
ABSENT, attrIdList})
OWS-DataRetrieval-Response ::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
OWS-TerminateComm ::= Event-Report-Request {OwsContainer} (WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})
OWS-TestComm-Request ::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0), ActionType
(15), accessCredentials ABSENT, iid ABSENT})
OWS-TestComm-Response ::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})

-- Definitions of the OWS attributes:
OwsData ::= SEQUENCE {
    encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting OwsPayload as per
Appendix 11 --}),
    DSRCSecurityData OCTET STRING
}
OwsPayload ::= SEQUENCE {
```

```

    tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
    recordedWeight INTEGER (0..65535), -- 0= Total measured weight of the heavy goods
    vehicle -- with 10 Kg resolution.
    axlesConfiguration OCTET STRING SIZE (3), -- 0= 20 bits allowed for the number
    -- of axles for 10 axles.
    axlesRecordedWeight OCTET STRING SIZE (20), -- 0= Recorded Weight for each axle
    -- with 10 Kg resolution.
    tp15638Timestamp INTEGER(0..4294967295) -- Timestamp of current record
  }

Ows-ContextMark ::= SEQUENCE {
  standardIdentifier StandardIdentifier, -- identifier of the TARV part and its version
}

StandardIdentifier ::= OBJECT IDENTIFIER
OwsContainer ::= CHOICE {
  integer [0] INTEGER,
  bitstring [1] BIT STRING,
  octetstring [2] OCTET STRING (SIZE (0..127, ...)),
  universalString [3] UniversalString,
  beaconId [4] BeaconID,
  t-apdu [5] T-APDUs,
  dsrcApplicationEntityId [6] DSRCApplicationEntityID,
  dsrc-Ase-Id [7] Dsrc-EID,
  attrIdList [8] AttributeIdList,
  attrList [9] AttributeList{RtmContainer},
  reserved10 [10] NULL,
  OwsContextmark [11] Ows-ContextMark,
  OwsData [12] OwsData,
  reserved13 [13] NULL,
  reserved14 [14] NULL,
  time [15] Time,
  -- values from 16 to 255 reserved for ISO/CEN usage
}
}

END

```

### 5.5.6 Элементы OwsData, выполняемые действия и определения

Элементы OwsData установлены для поддержки Директивы 2015/719/ЕС о максимальном весе и габаритах большегрузных транспортных средств. Их значение таково:

- recordedWeight представляет собой общий измеряемый вес большегрузных транспортных средств с разрешением 10 кг, как указано в EN ISO 14906. Например, значение 2500 соответствует весу 25 тонн.
- axlesConfiguration представляет собой конфигурацию большегрузного транспортного средства по числу осей. Конфигурация определяется битовой маской 20 бит (расширение по сравнению с EN ISO 14906). 2-битовая маска представляет собой конфигурацию оси в следующем формате:
  - Значение 00B означает, что величина недоступна, так как транспортное средство не снабжено аппаратурой для сбора данных веса на ось.
  - Значение 01B означает, что оси нет.
  - Значение 10B означает, что ось есть, вес вычислен, и данные по нему собраны и указаны в поле axlesRecordedWeight.
  - Значение 11B зарезервировано для будущего использования.

Последние 4 бита зарезервированы для будущего использования.

Число осей тягача			Число осей							RFU (4 бита)
			Число осей прицепа							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	

- axlesRecordedWeight представляет собой конкретный вес, зарегистрированный в отношении каждой оси с разрешением 10 кг. Для каждой оси используются два октета. Например, значение 150 соответствует весу 1500 кг.

Другие типы данных представлены в 5.4.5.

## 5.5.7 Механизмы передачи данных

DSC\_64 Механизм передачи данных OWS между контрольным устройством и устройством DSRC на транспортном средстве такой же, как для данных RTM (см. 5.4.6).

DSC\_65 Передача данных между платформой, собирающей данные о максимальном весе, и устройством DSRC в транспортном средстве опирается на физическое соединение и интерфейсы и протокол, представленные в разделе 5.6.

## 5.6 Передача данных между DSRC-VU и БУ

### 5.6.1 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) Чтобы можно было нанимать различных поставщиков для поставок БУ и DSRC-VU и для различных партий DSRC-VU, соединение между БУ и DSRC-VU – открытое стандартное соединение. БУ соединяется с DSRC-VU либо

- i) при помощи фиксированного кабеля длиной не менее 2 метров, с использованием прямого коннектора DIN 41612 H11, утверждённого 11-контактного штекерного соединителя DSRC-VU, подходящего к соответствующему утверждённому гнездовому разъёму DIN/ISO со стороны БУ,
- ii) при помощи Bluetooth Low Energy (BLE)
- iii) в соответствии со стандартом ISO 11898 или соединения SAE J1939

DSC\_69 б) определение интерфейсов и соединений между БУ и DSRC-VU должно поддерживать команды протокола приложения, представленные в 5.6.2. и

DSC\_70 в) БУ и DSRC-VU должны поддерживать передачу данных через соединение с точки зрения эксплуатационных показателей и питания.

### 5.6.2 Протокол приложения

DSC\_71 Протокол приложения между устройством удалённой связи БУ и DSRC-VU отвечает за периодическую передачу данных удалённой связи из БУ в DSRC.

DSC\_72 Имеются следующие основные команды:

1. Инициализация канала связи – запрос
2. Инициализация канала связи – ответ
3. Передача данных с идентификатором приложения RTM и полезной нагрузкой, определяемой по данным RTM
4. Подтверждение получения данных
5. Закрытие канала связи – запрос
6. Закрытие канала связи – ответ

DSC\_73 В ASN1.0 предыдущие команды можно определить следующим образом:

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

    RCDT-Communication Link Initialization - Request ::= SEQUENCE { LinkIdentifier
        INTEGER
    }

    RCDT-Communication Link Initialization - Response ::= SEQUENCE { LinkIdentifier
        INTEGER,
        answer    BOOLEAN
    }

    RCDT- Send Data ::= SEQUENCE {
        LinkIdentifier INTEGER,
        DataTransactionId INTEGER,
        RCDTData SignedTachographPayload
    }

    RCDT Data Acknowledgment :: SEQUENCE {
        LinkIdentifier INTEGER, DataTransactionId
        INTEGER,
        answer    BOOLEAN
    }

    RCDT-Communication Link Termination - Request ::= SEQUENCE { LinkIdentifier
        INTEGER
    }

    RCDT-Communication Link Termination - Response ::= SEQUENCE { LinkIdentifier
        INTEGER,
        answer    BOOLEAN
    }

End
```

DSC\_74 Описание команд и параметров:

RCDT-Communication Link Initialization - Request используется для инициализации канала связи. БУ передаёт команду в DSRC-VU. LinkIdentifier устанавливает БУ и передаёт его DSRC-VU, чтобы отслеживать конкретный канал связи.

(Примечание: это для поддержки будущих каналов и других приложений/модулей, например, взвешивания на борту).

RCDT-Communication Link Initialization – Response используется для ответа на запрос инициализации канала связи. DSRC-VU передаёт команду в БУ. Команда выдаёт результат инициализации в качестве ответ = 1 (успешно) или =0 (неуспешно).

DSC\_75 Инициализация канала связи происходит только после включения установки, калибровки и запуска двигателя/  
БУ.

RCDT-Send Data используется БУ для передачи подписанных RCDTData (т.е. *данных удалённой связи*) в DSRC-VU. Данные передаются каждые 60 секунд. Параметр DataTransactionId идентифицирует конкретную передачу данных. LinkIdentifier также используется для обеспечения выбора правильного канала. RCDT-Data Acknowledgment передаёт DSRC-VU как отзыв БУ о получении данных из команды RCDT-Send Data с идентификацией по параметру DataTransactionId. Параметр ответа – 1 (успешно) или = 0 (неуспешно). Если БУ получает более трёх ответов, равных 0, или БУ не получает подтверждения о получении данных RCDT относительно конкретных ранее переданных данных RCDT-Send Data с конкретным, БУ генерирует и регистрирует событие. RCDT-Communication Link Termination request передаётся БУ в DSRC-VU, чтобы закрыть канал связи с определённым LinkIdentifier.

DSC\_76 После перезагрузки DSRC-VU или БУ все существующие каналы связи должны быть удалены, так как в случае внезапного выключения БУ могут остаться незакрытые каналы. RCDT-Communication Link Termination – Response передаётся DSRC-VU в БУ для подтверждения запроса закрытия канала со стороны БУ с определённым LinkIdentifier.

## 5.7 Обработка ошибок

### 5.7.1 Регистрация и передача данных в DSRC-VU

DSC\_77 Данные предоставляются всегда в защищённом виде функцией *VUSM* в *DSRC-VU*. *VUSM* проверяет, правильно ли записаны данные, зарегистрированные в *DSRC-VU*. Регистрация и сообщения о любых ошибках при передаче данных из БУ в память *DSRC-VU* записываются при помощи типа EventFaultType со значением '62'Н Ошибка связи устройства удалённой связи вместе с временной меткой.

DSC\_78 БУ хранит файл с уникальным названием, который могут легко найти инспекторы с целью регистрации сбоев внутренней связи БУ.

DSC\_79 Если VUPM пытается получить данные БУ из модуля безопасности (чтобы передать их VU-DSRC), но безуспешно, формируется запись о такой безуспешной попытке с типом EventFaultType и значением '62'Н Ошибка связи устройства удалённой связи вместе с временной меткой. Ошибка связи обнаруживается, когда не получено сообщение RCDT Data Acknowledgment относительно соответствующих RCDT Send Data (т.е. с таким же DataTransactionId в сообщениях Send Data and Acknowledgment) более трёх раз подряд.

### 5.7.2 Ошибки беспроводной связи

DSC\_80 Обработка ошибок связи соответствует определённым стандартам DSRC, как-то EN 300 674-1, EN 12253, EN 12795, EN 12834 и соответствующим параметрам EN 13372.

#### 5.7.2.1 Ошибки шифрования и подписи

DSC\_81 Ошибки шифрования и подписи обрабатываются, как описано в приложении 11 «Общие механизмы безопасности» и отсутствуют в сообщениях об ошибках, связанных с передачей данных DSRC.



### 5.7.2.2 Регистрация ошибок

DSRC предлагает динамичную беспроводную связь в среде неопределённых атмосферных условий и условий вмешательства, в частности, в комбинациях портативных REDCR и движущегося транспортного средства в рамках настоящего приложения. Поэтому необходимо чётко видеть разницу между безуспешной попыткой считывания и условием ошибки. В случае операции через беспроводный интерфейс безуспешная попытка считывания встречается довольно часто, что приводит к тому, что обычно совершается повторная попытка ретрансляции BST и повторения последовательности, что в большинстве случаев обеспечивает успешное соединение связи и передачу данных, кроме случаев, когда транспортное средство покидает радиус за время, необходимое для повторной передачи. (Успешный вариант считывания может включать в себя несколько попыток и повторных попыток).

Безуспешное считывание может быть связано с тем, что не были должным образом настроены антенны (неудачное прицеливание), потому что одна из антенн загорожена (что может быть намеренным или может быть вызвано физическим присутствием другого транспортного средства), из-за радиопомех, особенно примерно с 5,8 ГГц Wi-Fi или другой открытой беспроводной связи, или из-за радарных помех или сложных атмосферных условий (например, в грозу), или просто из-за того, что транспортное средство покинуло радиус связи DSRC. Отдельные случаи безуспешного считывания по своей природе не могут регистрироваться, просто потому что связь не была установлена.

Однако, если представитель компетентного контрольного органа нацеливается на транспортное средство и пытается направить контрольный запрос в *DSRC-VU*, но успешной передачи данных не происходит, такая неудача может возникнуть в результате намеренного взлома, и потому представителю компетентного контрольного органа нужно средство регистрации такой неудачи и возможность предупредить коллег далее по цепочке, что может быть нарушение. Коллеги могут позднее остановить транспортное средство и провести физический досмотр. Однако, поскольку связь успешно не была установлена, *DSRC-VU* не может предоставить данные о неудачной попытке. Потому регистрация таких случаев предусматривается как проектная функция аппаратуры REDCR.

Безуспешное считывание ошибкой технически не является. В данном контексте ошибка – это получение неверного значения.

Данные, передаваемые в *DSRC-VU*, предоставляются уже в защищённом виде и потому должны проверяться поставщиком этих данных (см. 5.4).

Данные, впоследствии передаваемые через воздушный интерфейс, проверяются при помощи циклического контроля избыточности на уровне связи. Если проверка CRC успешна, значит, данные верны. Если проверка CRC не даёт подтверждения, данные передаются снова. Вероятность, что данные могут успешно пройти через CRC в неправильном виде, статистически настолько низка, что её можно не принимать во внимание.

Если CRC не даёт подтверждения и нет времени на повторную передачу и получение верных данных, в результате будет получена не ошибка, а инстанцирование определённого типа безуспешного считывания.

Единственные значимые данные безуспешного действия, которые можно зарегистрировать, – это число успешных инициаций операций, в результате которых не удалось провести успешной передачи данных в REDCR.

DSC\_82 Так, *REDCR* записывает, ставит временную метку и регистрирует число, если этап инициализации запроса DSRC успешен, но операция прерывается до того, как *данные* будут успешно извлечены REDCR. Эти данные должны быть доступны для представителя компетентного контрольного органа и хранятся в памяти оборудования REDCR. Способы, которыми это достигается, зависят от проекта изделия или указаний компетентного контрольного органа.

Единственные значимые данные ошибки, которые можно зарегистрировать, – это число случаев, когда REDCR не может расшифровать полученные данные. Однако следует отметить, что это касается только эффективности программного обеспечения REDCR. Данные могут быть технически расшифрованы, но семантически непонятны.

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 Испытания при вводе в эксплуатацию и периодических проверках функции удалённой связи

### 6.1 Общие положения

DSC\_84 В отношении функции удалённой связи предусмотрены два типа испытаний:

- 1) Испытание ECHO для подтверждения канала беспроводной связи DSRC-REDCR >>:-<DSRC-VU.
- 2) Сквозные испытания безопасности, чтобы удостовериться, что карточка мастерской может получить доступ к зашифрованным и подписанным данным в БУ, передаваемым по каналу беспроводной связи.

### 6.2 ECHO

Данная часть содержит положения, конкретно связанные с испытаниями только функциональной активности DSRC-REDCR >>:-<DSRC-VU.

Цель команды ECHO – позволить мастерским или испытательным органам официального утверждения типа испытывать, что связь DSRC работает, без необходимости доступа к данным безопасности. Потому оборудование испытателя должно быть способно только запустить связь DSRC (отправить BST с AID = 2) и затем передать команду ECHO и, при условии, что DSRC работает, получить ответ ECHO. Более подробно см. 5.4.8. При условии получения верного ответа связь DSRC (DSRC-REDCR >>:-<DSRC-VU) может быть подтверждена как действующая должным образом.

### 6.3 Испытания для подтверждения содержания данных безопасности

DSC\_85 Данные испытания проводятся для подтверждения всего потока данных с точки зрения безопасности. Для таких испытаний нужно испытательное считывающее устройство DSRC. Испытательное считывающее устройство DSRC выполняет примерно такую же функцию и соответствует такой же спецификации считывающего устройства, которым пользуются правоохранительные органы, с той лишь разницей, что для аутентификации пользователя испытательного считывающего устройства DSRC используется карточка мастерской, а не контрольная карточка. Испытания могут проводиться после первой активации «умного» тахографа или в конце процедуры калибровки. После активации бортовое устройство генерирует и передаёт DSRC-VU защищённые данные раннего обнаружения.

DSC\_86 Работники мастерской должны расположить испытательное считывающее устройство DSRC на расстоянии от 2 до 10 метров перед транспортным средством.

DSC\_87 Затем персонал мастерской вводит карточку мастерской в испытательное считывающее устройство DSRC для запроса данных раннего обнаружения у бортового устройства. После успешного контрольного запроса персонал мастерской получает доступ к полученным данным, чтобы проверить, успешно ли подтверждена их целостность и успешно ли они расшифрованы.

RU

## Приложение 15

## Миграция: управление сосуществованием оборудования разных поколений

## СОДЕРЖАНИЕ

1.	ОПРЕДЕЛЕНИЯ .....	544
2.	ОБЩИЕ ПОЛОЖЕНИЯ.....	544
2.1.	Обзор перехода.....	544
2.2.	Эксплуатационная совместимость между БУ и карточками .....	544
2.3.	Эксплуатационная совместимость между БУ и датчиком движения.....	545
2.4.	Эксплуатационная совместимость между бортовыми устройствами, карточками тахографа и оборудованием для загрузки данных .....	545
2.4.1	Прямая загрузка данных карточки на СПА.....	545
2.4.2	Загрузка данных карточки через бортовое устройство .....	545
2.4.3	Загрузка данных с бортового устройства .....	546
2.5.	Эксплуатационная совместимость между БУ и калибровочным оборудованием .....	546
3.	ОСНОВНЫЕ ЭТАПЫ ПЕРИОДА ДО ДАТЫ ВВОДА .....	546
4.	ПОЛОЖЕНИЯ ОТНОСИТЕЛЬНО ПЕРИОДА ПОСЛЕ ДАТЫ ВВОДА.....	546

## 1. Определения

В настоящем приложении используются следующие определения:

**система «умного» тахографа:** см. определение в настоящем дополнении (глава 1: определение bbb);

**система тахографа первого поколения:** см. определение в настоящем регламенте (статья 2: определение 1);

**система тахографа второго поколения:** см. определение в настоящем регламенте (статья 2: определение 7);

**дата ввода:** см. определение в настоящем дополнении (глава 1: определение ccc);

**специализированная программируемая аппаратура (IDE (СПА)):** оборудование, используемое для загрузки данных, в соответствии с определением в приложении 7 настоящего дополнения.

## 2. Общие положения

### 2.1. Обзор перехода

В преамбуле настоящего дополнения представлен обзор перехода между системами тахографов первого и второго поколений.

В дополнение к положениям преамбулы:

- датчики движения первого поколения несовместимы с бортовыми устройствами второго поколения.
- датчики движения второго поколения будут устанавливаться на транспортных средствах вместе с бортовыми устройствами второго поколения.
- оборудование загрузки данных и калибровки должно будет развиваться, чтобы поддерживать записывающее оборудование и карточки тахографов обоих поколений.

### 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), а карточки тахографа второго поколения совместимы с бортовыми устройствами второго поколения (в соответствии с дополнением 1С к настоящему регламенту). Кроме того, применяются следующие требования.

- MIG\_001 За исключением случаев, предусмотренных в требованиях MIG\_004 и MIG\_005, карточки тахографа первого поколения могут и дальше использоваться в бортовых устройствах второго поколения до истечения срока их действия. Однако их владельцы могут попросить их заменить карточками тахографа второго поколения, как только они станут доступны.
- MIG\_002 Бортовые устройства второго поколения способны использовать любые вводимые в них карточки водителя, контроля и предприятия первого поколения.
- MIG\_003 Такую способность бортовых устройств могут окончательно и бесповоротно устранить мастерские, чтобы карточки тахографа первого поколения больше не принимались. Это можно будет сделать только после того, как Европейская комиссия начнёт процедуру, в рамках которой к мастерским будет обращена просьба принять такие меры, например, во время регулярной проверки тахографа.
- MIG\_004 Бортовые устройства второго поколения способны использовать только карточки мастерской второго поколения.
- MIG\_005 Для определения режима работы бортовые устройства второго поколения учитывают только типы введённых в них карточек, но не поколения.
- MIG\_006 Любые действительные карточки тахографа второго поколения можно использовать в бортовых устройствах первого поколения точно так же, как карточки 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. Кроме того, применяются следующие требования.

- MIG\_007 Бортовые устройства второго поколения нельзя будет соединять и использовать с датчиками движения первого поколения.
- MIG\_008 Датчики движения второго поколения можно соединять и использовать с бортовыми устройствами только второго или обоих поколений.

### **2.4. Эксплуатационная совместимость между бортовыми устройствами, карточками тахографа и оборудованием для загрузки данных**

- MIG\_009 Оборудование для загрузки данных может использоваться только с одним поколением бортовых устройств и карточек тахографа или с обоими поколениями.

#### **2.4.1 Прямая загрузка данных карточки на СПА**

- MIG\_010 СПА загружает данные с карточек тахографа одного поколения, введённых в считывающие устройства, при помощи механизмов защиты и протокола загрузки данных соответствующего поколения; данные загружаются в формате соответствующего поколения.
- MIG\_011 Чтобы водителей могли контролировать органы третьих стран, не ЕС, также можно загружать данные карточек водителя (и мастерской) второго поколения таким же образом, как и данные карточек водителя (мастерской) первого поколения. Среди таких загружаемых данных:
- неподписанные EF IC и ICC,
  - неподписанные EF (первого поколения) Card\_Certificate и CA\_Certificate,
  - данные других приложений EF (в TACHO DF), запрашиваемые по протоколу загрузки данных с карточки первого поколения. Данная информация защищается цифровой подписью в соответствии с механизмами безопасности первого поколения.

Загружаемые данные не включают в себя данные приложений EF, присутствующих только на карточках водителя (и мастерской) второго поколения (данные приложений EF в TACHO\_G2 DF).

#### **2.4.2 Загрузка данных карточки через бортовое устройство**

- MIG\_012 Данные загружаются с карточки второго поколения, введённой в бортовое устройство первого поколения, с применением протокола загрузки данных первого поколения. Карточка отвечает на команды бортового устройства точно так же, как карточка первого поколения; формат загружаемых данных такой же, как данных, загружаемых с карточки первого поколения.
- MIG\_013 Данные загружаются с карточки первого поколения, введённой в бортовое устройство второго поколения, с применением протокола загрузки данных, представленного в приложении 7 настоящего дополнения. Бортовое устройство передаёт команды на карточку точно так же, как бортовое устройство первого поколения; формат загружаемых данных соответствует формату, определённому для карточек первого поколения.

### **2.4.3 Загрузка данных с бортового устройства**

- MIG\_014 Данные загружаются с бортовых устройств второго поколения, использующих механизмы безопасности второго поколения, с применением протокола загрузки данных, представленного в приложении 7 настоящего дополнения.
- MIG\_015 Чтобы водителей могли контролировать органы третьих стран, не ЕС, а данные бортовых устройств могли загружать мастерские не ЕС, можно также загружать данные с бортовых устройств второго поколения с применением механизмов безопасности первого поколения и протокола загрузки данных первого поколения. Формат загружаемых данных такой же, как данных, загружаемых с бортового устройства первого поколения. Такую 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 с применением протокола калибровки соответствующего поколения. Калибровочное оборудование может использоваться с тахографами только одного или обоих поколений.

#### **3. Основные этапы периода до даты ввода**

- MIG\_017 Испытательные ключи и сертификаты предоставляются производителям не позднее чем за **30 месяцев** до даты ввода.
- MIG\_018 Производители могут начинать испытания на эксплуатационную совместимость не позднее чем за **15 месяцев** до даты ввода.
- MIG\_019 Официальные ключи и сертификаты предоставляются производителям не позднее чем за **12 месяцев** до даты ввода.
- MIG\_020 Государства-члены могут выпускать карточки мастерской второго поколения не позднее чем за **3 месяца** до даты ввода.
- MIG\_021 Государства-члены могут выпускать все типы карточек тахографа второго поколения не позднее чем за **1 месяц** до даты ввода.

#### **4. Положения относительно периода после даты ввода**

- MIG\_022 После даты ввода государства-члены выпускают только карточки тахографа второго поколения.
- MIG\_023 Производитель бортовых устройств/датчиков движения могут производить бортовые устройства/датчики движения первого поколения до тех пор, пока они будут применяться на практике, чтобы можно было менять неисправные компоненты.
- MIG\_024 Производители бортовых устройств/датчиков движения могут подавать заявки и получать утверждение типа для технического обслуживания бортовых устройств/датчиков движения первого поколения, которым уже выдано утверждение типа.

RU

## Приложение 16. Адаптер для транспортных средств категорий m1 и n1

### Содержание

<b>1.</b>	<b>Сокращения и справочные документы .....</b>	<b>548</b>
1.1.	Сокращения .....	548
1.2.	Справочные стандарты.....	548
<b>2.</b>	<b>Общие характеристики и функции адаптера .....</b>	<b>548</b>
2.1.	Общее описание адаптера .....	548
2.2.	Функции.....	548
2.3.	Защита .....	548
<b>3.</b>	<b>Требования к записывающему оборудованию, если установлен адаптер .....</b>	<b>548</b>
<b>4.</b>	<b>Требования к конструкции и функциям адаптера .....</b>	<b>549</b>
4.1.	Обеспечение интерфейса и адаптация входящих импульсов скорости.....	549
4.2.	Обеспечение поступления входящих импульсов на встроенный датчик движения.....	549
4.3.	Встроенный датчик движения .....	549
4.4.	Требования к безопасности.....	550
4.5.	Рабочие характеристики.....	550
4.6.	Материалы .....	550
4.7.	Маркировка .....	550
<b>5.</b>	<b>Установка записывающего оборудования, если используется адаптер .....</b>	<b>551</b>
5.1.	Установка .....	551
5.2.	Пломбирование .....	551
<b>6.</b>	<b>Проверки, инспекции и ремонтные работы.....</b>	<b>551</b>
6.1.	Регулярные проверки.....	551
<b>7.</b>	<b>Утверждение типа записывающего оборудования, если используется адаптер.....</b>	<b>551</b>
7.1.	Общие вопросы .....	551
7.2.	Сертификат функциональности.....	552

## 1. Сокращения и справочные документы

### 1.1. Сокращения

TBD Подлежит утверждению

VU (БУ) Бортовое устройство

### 1.2. Справочные стандарты

ISO16844-3 Дорожные транспортные средства. Системы тахографов. Часть 3: интерфейс датчика движения

## 2. Общие характеристики и функции адаптера

### 2.1. Общее описание адаптера

ADA\_001 Адаптер обеспечивает присоединённое БУ защищёнными данными движения, постоянно отражающими скорость транспортного средства и пройденное расстояние.

Адаптер предназначен только для тех транспортных средств, которые обязательно должны быть снабжены записывающим оборудованием в соответствии с настоящим регламентом.

Он устанавливается и используется только на транспортных средствах, указанных в определении адаптера (уу) в дополнении IC, если механически невозможно установить никакие другие датчики движения, которые в остальном соответствуют положениям настоящего дополнения и его приложений 1-16.

Адаптер механически связывается не с движущейся частью транспортного средства, а с импульсами скорости/расстояния, генерируемыми интегрированными датчиками, или другими интерфейсами.

ADA\_002 Датчик движения утверждённого типа (в соответствии с положениями дополнения IC, раздел 8 «Утверждение типа записывающего оборудования и карточек тахографов») устанавливается в корпус адаптера, который также вмещает в себя устройство конвертации импульсов, способствующее поступлению входящих импульсов на встроенный датчик движения. Сам встроенный датчик движения соединяется с БУ так, чтобы интерфейс между БУ и адаптером соответствовал требованиям ISO16844-3.

### 2.2. Функции

ADA\_003 Адаптер включает в себя следующие функции:

- обеспечение интерфейса и адаптация входящих импульсов скорости,
- обеспечение поступления входящих импульсов на встроенный датчик движения,
- все функции встроенного датчика движения, обеспечивая защищённую передачу данных о движении в БУ.

### 2.3. Защита

ADA\_004 Для адаптера не проводится сертификация защиты в соответствии с общим уровнем защиты датчика движения, установленным в приложении 10 настоящего дополнения. Вместо этого применяются требования по безопасности, указанные в разделе 4.4 настоящего приложения.

## 3. Требования к записывающему оборудованию, если установлен адаптер

Требования в последующих главах указывают, как следует понимать требования настоящего дополнения в тех случаях, когда используется адаптер. В скобках указаны номера соответствующих требований дополнения IC.

ADA\_005 Записывающее оборудование любого транспортного средства, снабжённое адаптером, должно соответствовать всем положениям настоящего дополнения, за исключением случаев, когда в приложении указано иначе.

ADA\_006 В случае установки адаптера в состав записывающего оборудования входят кабели, адаптер (включая датчик движения) и БУ [01].



ADA\_007 Функция записывающего оборудования 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]
- событие «ошибка датчика движения» отображается БУ в случае нарушения нормального потока данных между встроенным датчиком движения и БУ и/или в случае ошибки, указывающей на нарушение целостности или подлинности данных в процессе передачи данных между встроенным датчиком движения и БУ [83]
- событие «попытка нарушения системы защиты» отображается БУ в отношении любого другого события, оказывающего воздействие на безопасность встроенного датчика движения, за исключением режима калибровки [85]
- неисправность записывающего оборудования отображается БУ, за исключением режима калибровки, в случае любой неисправности встроенного датчика движения [88]

ADA\_008 Неисправности адаптера, которые может обнаружить записывающее оборудование, связаны с неисправностями встроенного датчика 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 интерфейса и адаптация входящих импульсов скорости

ADA\_011 Входной интерфейс адаптера принимает импульсы частоты, отражающие скорость транспортного средства и пройденное расстояние. Электрические характеристики входящих импульсов: *Подлежит утверждению производителем*. Корректировки, доступные только для производителя адаптера и апробированной мастерской, выполняющей установку адаптера, позволяют обеспечить правильный интерфейс адаптера с транспортным средством, если применимо.

ADA\_012 Входной интерфейс адаптера, если применимо, способен умножать или делить импульсы частоты входящих импульсов скорости на определённый коэффициент, чтобы адаптировать сигнал к диапазону коэффициента  $k$ , как описано в настоящем дополнении (4000-25000 имп./км). Этот определённый коэффициент могут запрограммировать только производитель адаптера и апробированная мастерская, выполняющая установку адаптера.

##### 4.2. Обеспечение поступления входящих импульсов на встроенный датчик движения

ADA\_013 Входящие импульсы, возможно, адаптированные, как описано выше, поступают на встроенный датчик движения, чтобы датчик движения опознавал каждый поступающий импульс.

##### 4.3. Встроенный датчик движения

ADA\_014 Встроенный датчик движения стимулируется поступающими импульсами, таким образом приобретая способность генерировать данные о движении, точно отражающие движение транспортного средства, как если бы он был механически сопряжён с движущейся частью транспортного средства.

ADA\_015 БУ использует идентификационные данные встроенного датчика движения для идентификации адаптера [95].

ADA\_016 Считается, что данные установки, хранящиеся во встроенном датчике движения, отражают данные установки адаптера [122].

#### **4.4. Требования к безопасности**

- ADA\_017 Корпус адаптера сконструирован таким образом, чтобы его нельзя было открыть. Он пломбируется, чтобы можно было легко обнаружить попытки физического взлома (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 вынуть из адаптера, не повредив пломбу (-ы) корпуса адаптера или пломбу между датчиком и корпусом адаптера (см. ADA\_034).
- ADA\_019 Адаптер обеспечивает обработку и получение данных о движении только из входных данных адаптера.

#### **4.5. Рабочие характеристики**

- ADA\_020 Адаптер полностью работоспособен в диапазоне температур, указанном производителем.
- ADA\_021 Адаптер полностью работоспособен в диапазоне влажности от 10% до 90% [214].
- ADA\_022 Адаптер защищён от перепадов напряжения, несоблюдения полярности источника питания и короткого замыкания [216].
- ADA\_023 Адаптер:  
реагирует на магнитное поле, нарушающее распознавание движения транспортного средства. В подобных обстоятельствах бортовое устройство регистрирует и хранит неисправность датчика [88] или снабжается чувствительным элементом, защищённым от магнитных полей или не реагирующим на них [217].
- ADA\_024 Адаптер соответствует международному регламенту ЕЭК ООН Р10 об электромагнитной совместимости и защищён от электростатических разрядов и переходных процессов [218].

#### **4.6. Материалы**

- ADA\_025 Адаптер соответствует уровню защиты (*подлежит утверждению производителем в зависимости от расположения при установке*) [220, 221].
- ADA\_026 Цвет корпуса адаптера – жёлтый.

#### **4.7. Маркировка**

- ADA\_027 К адаптеру прикреплена поясняющая табличка с указанием следующих данных:
- название и адрес производителя адаптера,
  - номер детали, присвоенный производителем, и год изготовления адаптера,
  - знак официального утверждения типа адаптера или типа записывающего оборудования, включающего в себя адаптер,
  - дата установки адаптера,
  - идентификационный номер транспортного средства, на котором он установлен.
- ADA\_028 Поясняющая табличка также содержит следующие сведения (если их нельзя прочесть непосредственно на внешней поверхности встроенного датчика движения):
- название производителя встроенного датчика движения,
  - номер детали, присвоенный производителем, и год изготовления встроенного датчика движения,
  - знака официального утверждения встроенного датчика движения.

## 5. Установка записывающего оборудования, если используется адаптер

### 5.1. Установка

- ADA\_029 Адаптеры, подлежащие установке на транспортных средствах, устанавливаются только производителями транспортных средств или апробированные мастерские, уполномоченные устанавливать, активировать и калибровать цифровые и «умные» тахографы.
- ADA\_030 Такая апробированная мастерская, устанавливающая адаптер, корректирует входной интерфейс и выбирает коэффициент деления входного сигнала (если применимо).
- ADA\_031 Такая апробированная мастерская, устанавливающая адаптер, пломбирует корпус адаптера.
- ADA\_032 Адаптер устанавливается как можно ближе к части транспортного средства, передающей входящие импульсы.
- ADA\_033 Провода, обеспечивающие питание адаптера, красного (положительный ток) и чёрного цветов (заземление).

### 5.2. Пломбирование

- ADA\_034 Применяются следующие требования пломбирования:
- пломбируется корпус адаптера (см. ADA\_017),
  - корпус встроенного датчика пломбируется с присоединением к корпусу адаптера, за исключением случаев, когда датчик невозможно вынуть из корпуса адаптера, не повредив пломбу (-ы) корпуса адаптера (см. ADA\_018),
  - корпус адаптера пломбируется с присоединением к транспортному средству,
  - соединение между адаптером и оборудованием, передающим входящие импульсы, пломбируется с обеих сторон (насколько это возможно).

## 6. Проверки, инспекции и ремонтные работы

### 6.1. Регулярные проверки

- ADA\_035 Если используется адаптер, каждая регулярная проверка (средства регулярной проверки соответствуют требованиям [409]-[413] дополнения 1С) записывающего оборудования включает в себя следующие проверки:
- адаптер помечен соответствующими знаками официального утверждения типа,
  - пломбы на адаптере и его соединениях не повреждены,
  - адаптер установлен так, как указано на его табличке установки,
  - адаптер установлен в соответствии с указаниями производителя адаптера и/или транспортного средства,
  - установка адаптера на инспектируемом транспортном средстве разрешена.
- ADA\_036 Эти проверки включают в себя калибровку и замену всех пломб вне зависимости от их состояния.

## 7. Утверждение типа записывающего оборудования, если используется адаптер

### 7.1. Общие вопросы

- ADA\_037 Записывающее оборудование представляется на официальное утверждение типа в полной комплектации, вместе с адаптером [425].
- ADA\_038 Любой адаптер можно отдельно представить на официальное утверждение типа или на утверждение типа в качестве компонента записывающего оборудования.
- ADA\_039 Такое утверждение типа включает в себя функциональные испытания, в том числе адаптера. Положительные результаты каждого из таких испытаний подтверждаются соответствующим сертификатом [426].

## 7.2. Сертификат функциональности

ADA\_040 Сертификат функциональности адаптера или записывающего оборудования, в состав которого входит адаптер, производителю адаптера выдаётся только после того, как будут успешно проведены следующие обязательные функциональные испытания.

№	Испытание	Описание	Соответствующие требования
<b>1.</b>	<b>Административная проверка</b>		
1.1	Документация	Правильность документации адаптера	
<b>2.</b>	<b>Визуальный осмотр</b>		
2.1.	Соответствие адаптера документации		
2.2.	Идентификационные данные/маркировка адаптера		ADA_027, ADA_028
2.3	Материалы адаптера		[219]-[223] ADA_026
2.4.	Пломбирование		ADA_017, ADA_018, ADA_034
<b>3.</b>	<b>Функциональные испытания</b>		
3.1	Обеспечение поступления импульсов скорости на встроенный датчик движения		ADA_013
3.2	Обеспечение интерфейса и адаптация входящих импульсов скорости		ADA_011, ADA_012
3.3	Точность измерения движения		[30]-[35], [217]
<b>4.</b>	<b>Экологические испытания</b>		
4.1	Результаты испытаний производителя	Результаты экологических испытаний производителя	ADA_020, ADA_021, ADA_022, ADA_024
<b>5.</b>	<b>ЭМС</b>		
5.1	излучения и электромагнитная защищённость	Проверка соответствия Директиве 2006/28/EC	ADA_024
5.2	Результаты испытаний производителя	Результаты экологических испытаний производителя	ADA_024