



ЭКОНОМИЧЕСКИЙ
И СОЦИАЛЬНЫЙ СОВЕТ

Distr.
GENERAL

ECE/TRANS/SC.1/2006/2/Add.1
17 July 2008

RUSSIAN
Original: ENGLISH and FRENCH

ЕВРОПЕЙСКАЯ ЭКОНОМИЧЕСКАЯ КОМИССИЯ

КОМИТЕТ ПО ВНУТРЕННЕМУ ТРАНСПОРТУ

Рабочая группа по автомобильному транспорту

ЕВРОПЕЙСКОЕ СОГЛАШЕНИЕ, КАСАЮЩЕЕСЯ РАБОТЫ ЭКИПАЖЕЙ
ТРАНСПОРТНЫХ СРЕДСТВ, ПРОИЗВОДЯЩИХ МЕЖДУНАРОДНЫЕ
АВТОМОБИЛЬНЫЕ ПЕРЕВОЗКИ (ЕСТР)

Записка секретариата

Добавление

Добавление 1В к приложению ЕСТР, содержащее требования к конструкции,
испытаниям, установке и инспекции цифрового контрольного устройства,
используемого на автомобильном транспорте

Сводный вариант

1. Настоящий документ представляется в соответствии с мандатом, возложенным на секретариат Европейской экономической комиссии Организации Объединенных Наций (ЕЭК ООН) на основании пункта 2 статьи 1 (преамбула), предваряющей добавление 1В приложения к Европейскому соглашению, касающемуся работы экипажей транспортных средств, производящих международные автомобильные перевозки (ЕСТР) (см. ECE/TRANS/SC.1/2006/2). В соответствии с этим мандатом секретариат разработал сводный вариант данного добавления с учетом изменений, изложенных в статье 2, предваряющей настоящее добавление и включающей последовательные поправки и GE.08-24146 (R) 150908 081008

исправления, внесенные ЕС в основной текст (под названием "Приложение 1В"). Поскольку данный сводный текст имеет чисто информационное значение, **никакой юридической силы придавать ему не следует.**

2. Для ознакомления с официальным текстом приложения 1В (добавление 1В к которому является адаптированным вариантом), действующего в Европейском союзе, Договаривающимся сторонам предлагается использовать Правила Комиссии № 1360/2002 от 13 июня 2002 года и № 432/2004 от 5 марта 2004 года, которые приводят в соответствие Правила Совета (ЕЭС) № 3821/85, регламентирующие записывающие устройства в области автомобильного транспорта, в седьмой и восьмой раз с требованиями технического прогресса и преимущественно с подлинным вариантом этих документов на английском языке.

ДОБАВЛЕНИЕ 1В К ПРИЛОЖЕНИЮ ЕСТР

ТРЕБОВАНИЯ К КОНСТРУКЦИИ, ИСПЫТАНИЯМ, УСТАНОВКЕ И ИНСПЕКЦИИ ЦИФРОВОГО КОНТРОЛЬНОГО УСТРОЙСТВА, ИСПОЛЬЗУЕМОГО НА АВТОМОБИЛЬНОМ ТРАНСПОРТЕ

(Сводный вариант)

СОДЕРЖАНИЕ

	<u>Стр.</u>
I. ОПРЕДЕЛЕНИЯ.....	9
II. ОБЩИЕ ХАРАКТЕРИСТИКИ И ФУНКЦИИ КОНТРОЛЬНОГО УСТРОЙСТВА	19
1. Общие характеристики	19
2. Функции.....	20
3. Режимы работы.....	21
4. Защита.....	23
III. ТРЕБОВАНИЯ К КОНСТРУКЦИИ И ФУНКЦИЯМ КОНТРОЛЬНОГО УСТРОЙСТВА	24
1. Контроль за вводом и извлечением карточек	24
2. Измерение скорости и пробега.....	24
2.1 Измерение пробега	25
2.2 Измерение скорости	25
3. Измерение времени	26
4. Контроль за деятельностью водителя.....	26
5. Контроль за управлением	28
6. Ввод данных водителем вручную	28
6.1 Ввод названия мест, в которых начинаются и/или заканчиваются ежедневные периоды работы	28
6.2 Ручной ввод водителем данных о своей деятельности.....	28
6.3 Ввод данных об особых ситуациях	32

СОДЕРЖАНИЕ (продолжение)

	<u>Стр.</u>
7. Установка блокировки предприятием.....	32
8. Контроль за функциями проверки.....	33
9. Обнаружение событий и/или неисправностей	33
9.1 "Insertion of a non valid card" (ввод недействительной карточки)	33
9.2 "Card conflict" (несовместимость карточек)	33
9.3 "Time overlap" (несстыковка во времени).....	34
9.4 "Driving without an appropriate card" (управление без соответствующей карточки).....	34
9.5 "Card insertion while driving" (ввод карточки во время управления).....	34
9.6 "Last card session not correctly closed" (неправильное завершение последнего сеанса использования карточки)	35
9.7 "Over speeding" (превышение скорости)	35
9.8 "Power supply interruption" (прекращение электропитания).....	35
9.9 "Motion data error" (ошибочные данные о движении)	35
9.10 "Security breach attempt" (попытка нарушения системы защиты)	35
9.11 Отказ "Card" (сбой в работе карточки).....	35
9.12 Отказ "Control device" (сбой в работе контрольного устройства).....	36
10. Встроенная система проверки и самопроверки.....	36
11. Считывание данных, содержащихся в памяти	36
12. Регистрация и хранение данных в блоке памяти	37
12.1 Идентификационные данные оборудования	37
12.1.1 Идентификационные данные бортового устройства	37
12.1.2 Идентификационные данные датчика движения	37
12.2 Элементы защиты.....	37
12.3 Данные о вводе и извлечении карточки водителя	37
12.4 Данные о деятельности водителя.....	40
12.5 Места, в которых начинаются и/или заканчиваются ежедневные периоды работы	41
12.6 Данные о пробеге	42
12.7 Детальные данные о скорости.....	42
12.8 Данные о событиях.....	42
12.9 Данные о неисправностях.....	45
12.10 Данные калибровки.....	46
12.11 Данные о корректировке времени	47
12.12 Данные о контрольных операциях.....	48
12.13 Данные о блокировке, установленной предприятием	48

СОДЕРЖАНИЕ (продолжение)

	Стр.
12.14 Данные об операциях по загрузке	48
12.15 Данные об особых ситуациях.....	49
13. Считывание данных с карточки тахографа	49
14. Регистрация и хранение данных на карточках тахографа.....	50
15. Индикация данных	50
15.1 Индикация данных по умолчанию	51
15.2 Предупреждающая индикация.....	53
15.3 Меню доступа	53
15.4 Индикация иных данных	53
16. Распечатка данных	54
17. Предупреждения.....	55
18. Загрузка данных во внешние носители.....	56
19. Вывод данных на дополнительные внешние устройства.....	57
20. Калибровка.....	58
21. Корректировка времени.....	59
22. Условия работы	59
23. Материалы	60
24. Маркировка.....	60
IV. ТРЕБОВАНИЯ К КОНСТРУКЦИИ И ФУНКЦИЯМ КАРТОЧЕК ТАХОГРАФА	62
1. Видимые данные.....	62
2. Защита.....	66
3. Стандарты	67
4. Спецификации на окружающие условия и электромагнитную совместимость.....	67

СОДЕРЖАНИЕ (продолжение)

	Стр.
5. Хранение данных.....	68
5.1 Идентификация карточки и данные о защите	69
5.1.1 Идентификация приложений	69
5.1.2 Идентификация микропроцессора.....	69
5.1.3 Идентификация карточки на интегральной схеме	69
5.1.4 Элементы защиты.....	69
5.2 Карточка водителя.....	70
5.2.1 Идентификация карточки	70
5.2.2 Идентификация держателя карточки	70
5.2.3 Информация о водительском удостоверении	70
5.2.4 Данные об используемом транспортном средстве.....	70
5.2.5 Данные о деятельности водителя.....	71
5.2.6 Места, в которых начинаются и/или заканчиваются ежедневные периоды работы	72
5.2.7 Данные о событиях.....	73
5.2.8 Данные о неисправностях.....	74
5.2.9 Данные о проверочных операциях	75
5.2.10 Данные о сеансе использования карточки	76
5.2.11 Данные об особых ситуациях.....	76
5.3 Карточка мастерской.....	76
5.3.1 Элементы защиты.....	76
5.3.2 Идентификация карточки	77
5.3.3 Идентификация держателя карточки	77
5.3.4 Данные об используемом транспортном средстве.....	77
5.3.5 Данные о деятельности водителя.....	77
5.3.6 Данные о начале и/или завершении ежедневных периодов работы	78
5.3.7 Данные о событиях и неисправностях	78
5.3.8 Данные о проверочных операциях	78
5.3.9 Данные о калибровке и корректировке времени.....	78
5.3.10 Данные об особых ситуациях.....	79
5.4 Карточка контролера.....	79
5.4.1 Идентификация карточки	79
5.4.2 Идентификация держателя карточки	79
5.4.3 Данные о проверочных операциях	80
5.5 Карточка предприятия	80
5.5.1 Идентификация карточки	80
5.5.2 Идентификация держателя карточки	81
5.5.3 Данные о действиях предприятия.....	81

СОДЕРЖАНИЕ (продолжение)

	Стр.
V. УСТАНОВКА КОНТРОЛЬНОГО УСТРОЙСТВА	82
1. Установка	82
2. Установочная табличка	83
3. Наложение пломб	83
VI. ПРОВЕРКА, ИНСПЕКЦИЯ И РЕМОНТ	85
1. Утверждение механиков или мастерских	85
2. Проверка новых или отремонтированных приборов	85
3. Инспекция после установки	85
4. Периодические инспекции	86
5. Измерение погрешностей	86
6. Ремонт	87
VII. ВЫДАЧА КАРТОЧЕК	88
VIII. ОФИЦИАЛЬНОЕ УТВЕРЖДЕНИЕ ТИПА КОНТРОЛЬНОГО УСТРОЙСТВА И КАРТОЧЕК ТАХОГРАФА	89
1. Общие положения	89
2. Сертификат защиты	90
3. Сертификат функциональности	90
4. Сертификат эксплуатационной совместимости	90
5. Свидетельство об официальном утверждении типа	92
6. Исключительная процедура: первая проверка на эксплуатационную совместимость	92

СОДЕРЖАНИЕ (продолжение)

	Стр.
ПОДРАЗДЕЛЫ	
ПОДРАЗДЕЛ I - СЛОВАРЬ ДАННЫХ.....	93
ПОДРАЗДЕЛ II - СПЕЦИФИКАЦИИ НА КАРТОЧКИ ТАХОГРАФА ...	179
ПОДРАЗДЕЛ III - ПИКТОГРАММЫ.....	229
ПОДРАЗДЕЛ IV - РАСПЕЧАТКА ДАННЫХ	233
ПОДРАЗДЕЛ V - ИНДИКАЦИЯ НА ДИСПЛЕЕ.....	253
ПОДРАЗДЕЛ VI - ВНЕШНИЕ ИНТЕРФЕЙСЫ.....	255
ПОДРАЗДЕЛ VII - ПРОТОКОЛЫ ЗАГРУЗКИ ДАННЫХ.....	261
ПОДРАЗДЕЛ VIII - ПРОТОКОЛ КАЛИБРОВКИ	293
ПОДРАЗДЕЛ IX - ОФИЦИАЛЬНОЕ УТВЕРЖДЕНИЕ ТИПА - ПЕРЕЧЕНЬ МИНИМАЛЬНЫХ ТРЕБУЕМЫХ ИСПЫТАНИЙ.....	331
ПОДРАЗДЕЛ X - ОБЩИЕ КОНТРОЛЬНЫЕ ПОКАЗАТЕЛИ ЗАЩИТЫ.....	345
ПОДРАЗДЕЛ XI - ОБЩИЕ МЕХАНИЗМЫ ЗАЩИТЫ.....	415

I. ОПРЕДЕЛЕНИЯ

В настоящем приложении:

a) "активация" означает:

режим, в котором контрольное устройство становится полностью работоспособным и выполняет все функции, в том числе функции защиты;

Активация контрольного устройства производится с использованием карточки предприятия и присвоенного ей PIN-кода.

b) "аутентификация" означает:

функция, имеющая целью установить и проверить идентичность введенных данных;

c) "аутентичность" означает:

параметр, подтверждающий, что соответствующая информация вводится стороной, идентификационные данные которой могут быть проверены;

d) "встроенная система проверки (ВІТ)" означает:

проверки, производимые по команде, данной оператором или соответствующим внешним устройством;

e) "календарный день" означает:

сутки в интервале от 00:00 часов до 24:00 часов. Все календарные дни определяются по системе универсального времени (время UTC);

f) "калибровка" означает:

обновление или подтверждение параметров транспортного средства, которые должны храниться в блоке памяти. Параметры транспортного средства включают идентификационные данные транспортного средства (VIN, VRN и Договаривающейся стороны регистрации) и характеристики транспортного средства (w, k, l, размер шин, параметры регулировки устройства ограничения скорости

(в случае применимости), текущее время UTC, текущие показания счетчика пробега);

Калибровка контрольного устройства предполагает необходимость использования карточки предприятия.

g) "номер карточки" означает:

номер в виде 16 буквенно-цифровых знаков, который однозначно идентифицирует карточку тахографа в данной Договаривающейся стороне. Номер карточки включает порядковый индекс (в случае применимости), индекс замены и индекс возобновления;

Таким образом карточка однозначно идентифицируется с помощью кода выдавшей ее Договаривающейся стороны и номера карточки.

h) "порядковый индекс карточки" означает:

14-й буквенно-цифровой знак номера карточки, который используется для дифференциации различных карточек, выданных соответствующему предприятию или органу, которые имеют право на получение нескольких карточек тахографа. Данное предприятие или орган однозначно идентифицируются с помощью первых 13 знаков номера карточки;

i) "индекс возобновления карточки" означает:

16-й буквенно-цифровой знак номера карточки, который увеличивается в каждом случае возобновления карточки;

j) "индекс замены карточки" означает:

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

к) "характеристический коэффициент транспортного средства" означает:

числовая характеристика, придающая соответствующее значение выходному сигналу, подаваемому компонентом транспортного средства, связывающим его с контрольным устройством (вторичный вал коробки передач или ось) после пробега

транспортным средством расстояния в 1 км в стандартных условиях испытания (см. главу VI-5). Характеристический коэффициент выражается в импульсах на километр ($w = \dots$ имп./км);

l) "карточка предприятия" означает:

карточка тахографа, выданная компетентными органами Договаривающейся стороны владельцу или держателю транспортных средств, оснащенных контрольными устройствами;

Карточка предприятия идентифицирует предприятие и позволяет выводить на дисплей, загружать и распечатывать данные, хранящиеся в контрольном устройстве, на котором была установлена блокировка данным предприятием.

m) "постоянная контрольного устройства" означает:

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

n) "продолжительность управления", рассчитываемая контрольным устройством¹, означает непрерывное время управления транспортным средством, рассчитываемое в качестве суммы накопленного времени управления конкретным водителем с момента завершения его последнего периода ГОТОВНОСТЬ (AVAILABILITY) или ПЕРЕРЫВ/ОТДЫХ (BREAK/REST) или НЕТ ДАННЫХ (UNKNOWN)² продолжительностью 45 мин. или более (этот период может разбиваться на несколько периодов продолжительностью 15 мин. или более). В процессе этих расчетов учитываются, при необходимости, данные о прошлых видах деятельности, записанные в карточке водителя. Если водитель не вставил свою карточку, расчеты производятся на основе записанных данных, которые

¹ Этот способ расчета продолжительности управления и совокупной продолжительности времени перерывов используется контрольным устройством для расчета времени подачи предупредительного сигнала, указывающего на непрерывное время вождения. Он не предопределяет правовое толкование этих периодов времени.

² Периоды "НЕТ ДАННЫХ" соответствуют периодам, в течение которых карточка водителя не была вставлена в контрольное устройство и в отношении которых ручной ввод данных водителем о своей деятельности произведен не был.

относятся к текущему периоду времени, в течение которого карточка не вставлялась, и к соответствующему считывающему устройству;

о) "карточка контролера" означает:

карточка тахографа, выданная властями Договаривающейся стороны национальному компетентному контрольному органу;

Карточка контролера позволяет идентифицировать контрольный орган и, при возможности, сотрудника контрольного органа и открыть доступ к данным, хранящимся в блоке памяти, или в карточках водителя, для их просмотра, распечатки и/или загрузки.

р) "совокупное время перерывов", рассчитываемое контрольным устройством, означает:

совокупная продолжительность перерывов в течение всего времени управления, рассчитываемая в качестве совокупных периодов ГОТОВНОСТЬ или ПЕРЕРЫВ/ОТДЫХ или НЕТ ДАННЫХ² продолжительностью 15 мин. или более применительно к конкретному водителю с момента завершения его последнего периода ГОТОВНОСТЬ или ПЕРЕРЫВ/ОТДЫХ или НЕТ ДАННЫХ² продолжительностью 45 мин. или более (этот период может разбиваться на несколько периодов продолжительностью 15 мин. или более).

В процессе расчета учитываются, при необходимости, 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 контрольными устройствами, в процессе расчета не учитываются.

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

q) "блок памяти" означает:

электронное устройство хранения данных, встроенное в контрольное устройство;

г) "цифровая подпись" означает:

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

с) "загрузка" означает:

копирование вместе с цифровой подписью части или всего массива данных, записанных в блоке памяти транспортного средства или в блоке памяти карточки тахографа;

Загрузка не должна приводить к изменению или стиранию каких бы то ни было записанных данных.

т) "карточка водителя" означает:

карточка тахографа, выданная властями Договаривающейся стороны конкретному водителю;

Карточка водителя позволяет идентифицировать водителя и хранить данные о деятельности водителя.

и) "эффективная окружность шин" означает:

среднее значение расстояний, пройденных каждым из колес, приводящих в движение транспортное средство (ведущими колесами) за один полный оборот. Измерение этих расстояний производится в нормальных условиях испытания (глава VI-5) и выражается в виде " $l = \dots$ мм". Изготовители транспортных средств могут использовать вместо фактического измерения этого расстояния теоретический метод расчета, который учитывает распределение веса на оси транспортного средства в снаряженном состоянии без груза³. Методы такого теоретического расчета утверждаются компетентным органом Договаривающейся стороны;

³ Измерение расстояний производится в соответствии с положениями директивы Совета № 97/27/ЕС от 22 июля 1997 года, касающейся массы и габаритов некоторых категорий автотранспортных средств и их прицепов и изменяющей директиву 70/156/ЕЕС (ОJ No. L 233, 25.08.97).

v) "событие" означает:

сбой в работе, обнаруженный контрольным устройством, который может быть вызван попыткой фальсификации;

w) "неисправность" означает:

сбой в работе, обнаруженный контрольным устройством, который может быть обусловлен неисправностью или выходом из строя устройства;

x) "установка" означает:

установка контрольного устройства на транспортном средстве;

y) "датчик движения" означает:

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

z) "карточка недействительна" означает:

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

aa) "неприменимо" означает:

случай, когда использовать контрольное устройство в соответствии с положениями настоящего Соглашения не требуется;

bb) "превышение скорости" означает:

превышение разрешенной скорости транспортного средства, определяемое в качестве любого периода продолжительностью более 60 сек., в течение которого

измеренная скорость транспортного средства превышает предельное значение, на которое отрегулировано устройство ограничения скорости⁴;

cc) "периодическая инспекция" означает:

ряд операций, выполняемых в целях проверки надлежащей работы контрольного устройства и соответствия его регулировки параметрам транспортного средства;

dd) "печатающее устройство" означает:

компонент контрольного устройства, который позволяет распечатывать записанные данные;

ee) "контрольное устройство" означает:

комплект оборудования, предназначенный для установки на автотранспортных средствах в целях просмотра, регистрации и хранения в автоматическом и полуавтоматическом режиме данных о движении таких транспортных средств и некоторых периодах работы их водителей;

ff) "возобновление" означает:

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

gg) "ремонт" означает:

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

⁴ Предельное значение регулировки устройства ограничения скорости соответствует положениям директивы Совета № 92/6/ЕС от 10 февраля 1992 года, касающейся установки и использования устройства ограничения скорости некоторых категорий автотранспортных средств в Сообществе (ОJ No. L 057, 02/03/1992).

hh) "замена" означает:

выдача карточки тахографа вместо существующей карточки, которая, на основании полученного заявления, была потеряна, похищена или давала сбои в работе и не была возвращена выдавшему ее органу. Замена всегда предполагает наличие риска существования в одно и то же время двух действующих карточек;

ii) "сертификация защиты" означает:

процесс подтверждения сертифицирующим органом⁵, что контрольное устройство (или компонент) или карточка тахографа, подвергаемые контролю, выполняют требования в отношении защиты, определенные в подразделе 10 "Общие контрольные показатели защиты";

jj) "самопроверка" означает:

проверки, производимые на периодической основе и в автоматическом режиме контрольным устройством на предмет обнаружения неисправностей;

kk) "карточка тахографа" означает:

карточку со встроенной микросхемой, предназначенной для использования в контрольном устройстве. Карточки тахографа позволяют контрольному устройству проверить идентификационные данные держателя карточки (или идентификационные данные соответствующей группы) и передавать и хранить данные. Карточки тахографов могут быть следующего вида:

- карточка водителя,
- карточка контролера,
- карточка мастерской,
- карточка предприятия;

⁵ Положения, регламентирующие защиту, соответствуют положениям, изложенным в рекомендации Совета 95/144/СЕ от 7 апреля 1995 года, касающейся общих критериев оценки безопасности информационных технологий (О.Ж. No. L093, 26/04/1995).

п) "официальное утверждение типа" означает:

процесс подтверждения Договаривающейся стороной того факта, что данное контрольное устройство (или компонент) или карточка тахографа, подвергаемые проверке, удовлетворяют требованиям ЕСТР;

mm) "размер шины" означает:

обозначение размеров шин (внешних ведущих колес) в соответствии с Правилами ЕЭК № 54⁶;

nn) "идентификация транспортного средства" означает:

номера, идентифицирующие транспортное средство: номер регистрации транспортного средства (VRN) с указанием Договаривающейся стороны регистрации и опознавательный номер транспортного средства (VIN)⁷;

oo) "бортовое устройство (БУ)" означает:

контрольное устройство, за исключением датчика движения и электропроводки для подсоединения датчика движения. Бортовое устройство может представлять собой либо единое устройство, либо несколько устройств, установленных в различных местах транспортного средства, при условии что оно соответствует требованиям ЕСТР в отношении защиты;

pp) "неделя" для целей расчетов, производимых контрольным устройством, означает:

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

⁶ Исходным текстом, действующим в ЕС, является директива 92/23/ЕЕС от 31 марта 1992 года, касающаяся шин автотранспортных средств и их прицепов и их установки (OJ No. L 129, 14/05/1992).

⁷ Идентификация транспортного средства соответствует положениям директивы Совета № 76/114/ЕЕС от 18 декабря 1975 года, касающейся сближения законодательства государств-членов, регламентирующего предусмотренные таблички с данными и маркировку автотранспортных средств и их прицепов и местоположение и метод их нанесения (OJ, No. L 24, 30/01/1976).

qq) "карточка мастерской" означает:

карточка тахографа, выданная властями Договаривающейся стороны изготовителю контрольного устройства, механику, изготовителю транспортного средства или мастерской, уполномоченных данной Договаривающейся стороной.

Карточка мастерской позволяет идентифицировать держателя карточки и производить проверку, калибровку и/или загрузку данных с контрольного устройства.

II. ОБЩИЕ ХАРАКТЕРИСТИКИ И ФУНКЦИИ КОНТРОЛЬНОГО УСТРОЙСТВА

000 Любое транспортное средство, оснащенное контрольным устройством, удовлетворяющим положениям настоящего добавления, должно быть оборудовано спидометром и счетчиком пробега. Эти функции могут быть включены в контрольное устройство.

1. Общие характеристики

Цель контрольного устройства состоит в регистрации, хранении, отображении, распечатке и генерации данных о деятельности водителя.

001 Контрольное устройство включает электропроводку, датчик движения и бортовое устройство.

002 Бортовое устройство включает устройство обработки данных, блок памяти, часы, работающие в реальном масштабе времени, два интерфейса для карточек с встроенной микросхемой (для водителя и второго водителя), печатающее устройство, дисплей, систему визуального предупреждения, калибровочный/загрузочный разъем и устройство ввода данных пользователем.

Контрольное устройство может подсоединяться к другим устройствам с помощью дополнительных разъемов.

003 Любое включение или подсоединение к контрольному устройству любой функции, устройства или устройств, сертифицированных или не сертифицированных, не должно нарушать или создавать помехи, которые могут нарушить надлежащую и безопасную работу контрольного устройства и привести к нарушению положений настоящего Соглашения.

Пользователи контрольного устройства вводят свои идентификационные данные в данное устройство с помощью карточек тахографа.

004 Контрольное устройство предоставляет право селективного доступа к данным и функциям в зависимости от вида и/или идентификационных данных пользователя.

Контрольное устройство регистрирует и хранит данные в блоке памяти и в карточках тахографа.

Эти функции выполняются в соответствии с Европейскими положениями, регламентирующими защиту частных лиц в части обработки личных данных и беспрепятственной передачи таких данных⁸.

2. Функции

005 Контрольное устройство должно выполнять следующие функции:

- контроль за вводом и извлечением карточек,
- измерение скорости и пробега,
- измерение времени,
- контроль за деятельностью водителя,
- контроль за статусом управления,
- различные виды ручного ввода данных:
 - ввод данных о местах, в которых начинаются или заканчиваются еще дневные периоды работы,
 - ручной ввод данных о деятельности водителя,
 - ввод данных об особых ситуациях,
- реагирование на блокировку, установленную предприятием,
- контроль за операциями по проверке,
- обнаружение соответствующих 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,

⁸ Защита частных лиц в части обработки личных данных и беспрепятственной передачи таких данных соответствует положениям Директивы Совета № 95/46/ЕС от 24 октября 1995 года с включенными в нее последними поправками (ОJ, No. L 281, 23/11/1995).

- регистрация и хранение данных в карточках тахографа,
- вывод данных на дисплей,
- распечатка,
- предупреждение,
- загрузка данных на внешние носители,
- вывод данных на дополнительные внешние устройства,
- калибровка,
- корректировка времени.

3. Режимы работы

006 Контрольное устройство должно иметь четыре режима работы:

- рабочий режим,
- режим контроля,
- режим калибровки,
- режим предприятия.

007 Контрольное устройство должно переходить в следующий режим работы в соответствии с действующими карточками тахографа, вставленными в считывающее устройство карточки:

Режим работы		Считывающее устройство "Водитель"				
		Карточка не вставлена	Карточка водителя	Карточка контролера	Карточка мастерской	Карточка предприятия
Считывающее устройство "Второй водитель"	Карточка не вставлена	Рабочий	Рабочий	Контроль	Калибровка	Предприятие
	Карточка водителя	Рабочий	Рабочий	Контроль	Калибровка	Предприятие
	Карточка контролера	Контроль	Контроль	Контроль *	Рабочий	Рабочий
	Карточка мастерской	Калибровка	Калибровка	Рабочий	Калибровка *	Рабочий
	Карточка предприятия	Предприятие	Предприятие	Рабочий	Рабочий	Предприятие *

008 * В этих случаях контрольное устройство будет использовать только карточку тахографа, вставленную в считывающее устройство "Водитель".

009 Контрольное устройство не реагирует на вставленные недействительные карточки, за исключением вывода на дисплей, на печать или загрузки данных, содержащихся на карточке, срок действия которой истек. Эти функции должны быть возможны.

010 Все функции, перечисленные в пункте II.2, должны работать во всех режимах с учетом следующих исключений:

- функция калибровки доступна только в режиме калибровки,
- функция корректировки времени ограничена, за исключением режима калибровки,
- функции ручного ввода данных водителем доступны только в рабочем режиме или режиме калибровки,
- функция блокировки, производимой предприятием, доступна только в режиме предприятия,
- функция контроля операций по проверке работает только в режиме контроля,
- функция загрузки данных в рабочем режиме недоступна (за исключением случая, предусмотренного требованием 150).

011 Контрольное устройство может выводить любые данные на дисплей, печать или на внешние интерфейсы с учетом следующих исключений:

- в рабочем режиме любые личные идентификационные данные (фамилия и имя (имена), не соответствующие данным на вставленной карточке тахографа, должны гаситься, а любой номер карточки, не соответствующий данным на вставленной карточке тахографа, должен гаситься частично (должен гаситься каждый нечетный знак слева направо),
- в режиме предприятия данные, касающиеся водителя (требования 081, 084 и 087), могут выводиться только в течение периодов, когда они не заблокированы другим предприятием (идентифицируемым с помощью первых 13 цифр номера карточки предприятия),

- когда в контрольное устройство карточка не вставлена, данные, касающиеся водителя, могут выводиться только за текущий и восемь предыдущих календарных дней.

4. Защита

Система защиты имеет целью предохранить блок памяти от несанкционированного доступа к зарегистрированным данным и их манипуляции и регистрировать любые случаи таких попыток, предохранить целостность и аутентичность данных, передаваемых по каналу связи между датчиком движения и бортовым устройством, предохранить целостность и аутентичность данных, передаваемых по каналу связи между контрольным устройством и карточками тахографа, и проверять целостность и аутентичность загружаемых данных.

- 012 В целях обеспечения защиты системы контрольное устройство должно удовлетворять требованиям, предъявляемым к защите, которые предусмотрены общими контрольными показателями защиты датчика движения и бортового устройства (подраздел 10).

III. ТРЕБОВАНИЯ К КОНСТРУКЦИИ И ФУНКЦИЯМ КОНТРОЛЬНОГО УСТРОЙСТВА

1. Контроль за вводом и извлечением карточек

- 013 Контрольное устройство должно контролировать интерфейс для считки карточек в целях обнаружения факта ввода и извлечения карточки.
- 014 После ввода карточки контрольное устройство должно установить, является ли вставленная карточка действующей карточкой тахографа, и определить тип карточки.
- 015 Контрольное устройство должно быть сконструировано таким образом, чтобы карточки тахографов, после того как они были надлежащим образом вставлены в интерфейс для считки карточек, блокировались в нем в правильном положении.
- 016 Извлечение карточки тахографа должно быть возможным только в случае остановки транспортного средства и после записи соответствующих данных в память карточки. Извлечение карточки производится посредством преднамеренного действия пользователя.

2. Измерение скорости и пробега

- 017 Эта функция должна обеспечивать постоянное измерение и указывать величину пробега, соответствующего полному расстоянию, пройденному транспортным средством.
- 018 Эта функция должна обеспечивать постоянное измерение и указывать значение скорости транспортного средства.
- 019 Функция измерения скорости также обеспечивает информацию, указывающую на то, 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.

Устройства, показывающие скорость (спидометр) и общее пройденное расстояние (счетчик пробега), установленные на любом транспортном средстве, оснащенном контрольным устройством, соответствующим положениям настоящего Соглашения,

должны удовлетворять требованиям, касающимся максимальных допусков, указанных в настоящем добавлении (главы III.2.1 и III.2.2).

2.1 Измерение пробега

020 Пробег может измеряться таким образом:

- чтобы он включал суммарное перемещение как вперед, так и назад или
- чтобы он включал только перемещение вперед.

021 Контрольное устройство должно иметь возможность измерять расстояние от 0 до 9 999 999,9 км.

022 Пробег должен измеряться с соблюдением следующих допусков (расстояния не менее 1 000 м):

- $\pm 1\%$ до установки,
- $\pm 2\%$ при установке и периодических инспекциях,
- $\pm 4\%$ в процессе эксплуатации.

023 Пробег должен измеряться с точностью не менее 0,1 км.

2.2 Измерение скорости

024 Контрольное устройство должно обеспечивать измерение скорости в диапазоне от 0 до 220 км/ч.

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

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

контрольное устройство должно обеспечивать, в диапазоне скоростей от 20 до 180 км/ч, и специфических коэффициентов транспортного средства от 4 000

до 25 000 имп./км, измерение скорости с точностью ± 1 км/ч (при постоянной скорости).

Примечание: Точность хранения данных обуславливает дополнительный допуск на данные скорости, регистрируемой контрольным устройством, на уровне $\pm 0,5$ км/ч.

025a Скорость должна измеряться правильно в пределах нормальных допусков в течение 2 секунд с момента завершения фазы изменения скорости, в условиях, когда показатель изменения скорости составляет не более 2 м/с^2 .

026 Точность измерения скорости должна составлять не менее 1 км/ч.

3. Измерение времени

027 Функция измерения времени должна обеспечивать постоянное измерение времени и цифровое отображение даты и времени UTC.

028 Дата и время UTC должны использоваться для датирования всех операций, осуществляемых контрольным устройством (регистрация, распечатка, обмен данными, вывод на дисплее, ...).

029 Для визуализации местного времени необходимо предусмотреть возможность изменения разницы в выводимом на дисплей времени с помощью получасовых интервалов.

030 Отклонение времени не должно превышать ± 2 секунды в день в условиях, предусмотренных для официального утверждения типа.

031 Точность измерения времени должна составлять не менее 1 секунды.

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

4. Контроль за деятельностью водителя

033 Эта функция должна обеспечивать постоянный и отдельный контроль за деятельностью одного водителя и одного второго водителя.

- 034 Деятельность водителя должна включать DRIVING, WORK, AVAILABILITY или BREAK/REST (УПРАВЛЕНИЕ, РАБОТА, ГОТОВНОСТЬ ИЛИ ПЕРЕРЫВ/ОТДЫХ).
- 035 Водитель и/или второй водитель должны иметь возможность выбирать ручную функцию WORK, AVAILABILITY или BREAK/REST (РАБОТА, ГОТОВНОСТЬ ИЛИ ПЕРЕРЫВ/ОТДЫХ).
- 036 Когда транспортное средство движется, функция DRIVING (УПРАВЛЕНИЕ) выбирается автоматически в случае водителя, а функция AVAILABILITY (ГОТОВНОСТЬ) выбирается автоматически в случае второго водителя.
- 037 Когда транспортное средство останавливается, в случае водителя автоматически выбирается функция WORK (РАБОТА).
- 038 Считается, что первое изменение вида деятельности в течение 120 секунд после автоматического переключения на функцию WORK (РАБОТА) в связи с остановкой транспортного средства производится в момент остановки транспортного средства (что может предполагать отмену перехода на функцию РАБОТА).
- 039 Эта функция должна обеспечивать передачу данных об изменении вида деятельности в устройство регистрации с интервалом в одну минуту.
- 040 Если в течение данной календарной минуты регистрируется факт деятельности DRIVING (УПРАВЛЕНИЕ), то вся эта минута регистрируется как УПРАВЛЕНИЕ.
- 041 Если применительно к данной календарной минуте любая деятельность, относящаяся к категории УПРАВЛЕНИЯ, зарегистрирована непосредственно до этой минуты или сразу же после нее, то вся эта минута зачитывается как УПРАВЛЕНИЕ.
- 042 Если данная календарная минута не зачитывается в соответствии с предыдущими требованиями 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).
- 043 Эта функция также обеспечивает постоянный контроль за непрерывным временем управления и совокупным временем перерывов в работе водителя.

5. Контроль за управлением

- 044 Эта функция обеспечивает постоянный и автоматический контроль за статусом управления.
- 045 Если в устройство вставляются две действительные карточки водителя, то регистрируется статус управления GREW (ЭКИПАЖА), а во всех других случаях регистрируется статус управления SINGE (ОДИН).

6. Ввод данных водителем вручную

6.1 Ввод названия мест, в которых начинаются и/или заканчиваются ежедневные периоды работы

- 046 Эта функция позволяет вводить названия мест, в которых начинаются и/или заканчиваются ежедневные периоды работы водителя и/или второго водителя.
- 047 Места определяются в виде названия страны и дополнительно, в случае применимости, названия района.
- 048 В момент извлечения карточки водителя (или мастерской) контрольное устройство предлагает второму водителю ввести "название места, в котором заканчивается ежедневный период работы" (place where the daily work period ends).
- 049 Контрольное устройство должно давать возможность игнорировать это предложение.
- 050 Должна быть предусмотрена возможность ввода названия мест, в которых начинаются и/или заканчиваются ежедневные периоды работы, без карточки или в другое время, помимо моментов ввода и извлечения карточки.

6.2 Ручной ввод водителем данных о своей деятельности

- 050a После ввода карточки водителя (или мастерской) и только в этот момент контрольное устройство должно:
- напомнить держателя карточки дату и время последнего извлечения им своей карточки и

- предложить держателя карточки указать, означает ли данный ввод карточки продолжение текущего ежедневного периода работы.

Контрольное устройство должно давать возможность держателя карточки игнорировать данный вопрос, не отвечая на него или отвечая положительно или отрицательно:

- В том случае, если держатель карточки игнорирует вопрос, контрольное устройство предлагает держателю карточки указать "название места, в котором начинается ежедневный период работы" (place where the daily work period begins). Контрольное устройство должно давать возможность игнорировать это предложение. Если название места введено, то оно регистрируется в блоке памяти и в карточке тахографа с указанием времени ввода карточки
- В случае отрицательного или положительного ответа контрольное устройство должно предложить держателю карточки ввести данные о деятельности вручную с указанием дат и времени начала и завершения этой деятельности только из числа следующих видов деятельности: WORK, AVAILABILITY или BREAK/REST (РАБОТА, ГОТОВНОСТЬ или ПЕРЕРЫВ/ОТДЫХ), которые должны строго относиться только к периоду между моментом последнего извлечения карточки и моментом нынешнего ввода, не допуская при этом накладок таких видов деятельности. Это должно производиться в соответствии со следующими процедурами:
- В том случае, если держатель карточки утвердительно отвечает на указанный вопрос, контрольное устройство предлагает держателю карточки ввести вручную данные о деятельности в хронологическом порядке за период между моментом последнего извлечения карточки и текущим моментом ввода. Этот процесс заканчивается, когда время завершения деятельности, введенное вручную, соответствует времени ввода карточки.
- В том случае, если держатель карточки отвечает отрицательно на указанный вопрос, контрольное устройство:
 - предлагает держателю карточки ввести данные о деятельности вручную в хронологическом порядке с момента извлечения карточки до момента завершения соответствующего ежедневного периода работы (или деятельности, относящейся к данному транспортному средству в том

случае, если продолжение ежедневного периода работы записывается на регистрационном листке). В этом случае контрольное устройство, прежде чем предложить держателю карточки ввести данные о каждом виде деятельности вручную, предлагает ему указать, является ли время завершения последней зарегистрированной деятельности временем завершения предыдущего периода работы (см. примечание ниже),

Примечание: В том случае, если держатель карточки не указывает, когда завершился предыдущий период работы, и вводит вручную данные о деятельности, время завершения которой соответствует времени вводу карточки, контрольное устройство,

- допускает, что ежедневный период работы завершился в начале первого периода ОТДЫХА (или периода, за который НЕТ ДАННЫХ) после извлечения или в момент извлечения карточки, если данные о периоде отдыха введены не были (и если ни одного периода, за который НЕТ ДАННЫХ, не осталось),
 - допускает, что время начала (см. ниже) соответствует времени ввода карточки,
 - производит операции, изложенные ниже.
- Затем, если время завершения соответствующего периода работы отличается от времени извлечения карточки или если в этот момент времени не было введено название места завершения ежедневного периода работы, предлагает держателю карточки "подтвердить или ввести название места, в котором завершился ежедневный период работы" (confirm or enter the place where the daily work period ended) (контрольное устройство допускает возможность пропустить это предложение). Если название места введено, оно регистрируется только в карточке тахографа и только в том случае, если оно отличается от места, введенного в момент извлечения карточки (если оно было введено) с указанием времени завершения периода работы.
- Затем предлагает держателю карточки "ввести время начала" (enter a start time) текущего ежедневного периода работы (или деятельности, относящейся к данному транспортному средству, в том случае, если до этого держатель карточки использовал в течение этого периода

регистрационный листок) и предлагает держателю карточки указать "место, в котором начинается ежедневный период работы" (place where the daily work period begins) (контрольное устройство допускает возможность пропустить это предложение). Если название места введено, оно регистрируется в карточке тахографа с указанием этого времени начала деятельности. Если это время начала соответствует времени ввода карточки, то название места также регистрируется в блоке памяти.

- Затем, если это время начала отличается от времени ввода карточки, предлагает держателю карточки ввести вручную данные о деятельности в хронологическом порядке за период со времени начала до момента ввода карточки. Этот процесс заканчивается, когда время завершения деятельности, введенное вручную, соответствует времени ввода карточки.
- После этого контрольное устройство дает держателю карточки возможность изменить любые данные о деятельности, введенные вручную, до их подтверждения с помощью выбранной конкретной команды, после чего любые такие изменения произвести невозможно.
- Если такие ответы на первоначальный вопрос не подтверждаются вводом соответствующих данных о деятельности, контрольное устройство интерпретирует это так, как если бы держатель карточки пропустил этот вопрос.

В течение всего этого процесса контрольное устройство ждет ввод данных не дольше следующих интервалов времени:

- в случае отсутствия действий со стороны человека на уровне интерфейса "человек-устройство" в течение одной минуты (с подачей визуального и, в случае возможности, звукового предупреждения по истечении 30 с.) или
- если карточка извлечена или вставлена другая карточка водителя (или предприятия) или
- как только транспортное средство приходит в движение,

в этом случае контрольное устройство регистрирует любые данные, которые уже были введены.

6.3 Ввод данных об особых ситуациях

050b Контрольное устройство дает возможность водителю ввести в реальном масштабе времени следующие две особые ситуации:

"OUT OF SCOPE" ("НЕПРИМЕНИМО") (начало, конец)

"FERRY / TRAIN CROSSING" ("ПЕРЕЕЗД НА ПАРОМЕ/ПОЕЗДЕ")

Функция "FERRY / TRAIN CROSSING" может не открыться, если открыта функция "OUT OF SCOPE".

Открытая функция "OUT OF SCOPE" должна автоматически закрываться контрольным устройством в случае ввода или извлечения карточки водителя.

7. Установка блокировки предприятием

- 051 Эта функция позволяет предприятию устанавливать блокировку в целях ограничения доступа к данным в режиме работы "предприятия" только для уполномоченных им лиц.
- 052 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).
- 053 Блокировку можно поставить в положение "in" ("включено") или "out" ("выключено") только в реальном масштабе времени.
- 054 Разблокировку может произвести только предприятие, которое произвело блокировку (идентифицируемое с помощью первых 13 цифр номера карточки предприятия), или
- 055 Разблокировка производится автоматически, если блокировку производит другое предприятие.
- 055a В том случае, если какое-либо предприятие производит блокировку и если предыдущая блокировка была произведена этим же предприятием, то в данном

случае предполагается, что предыдущая блокировка не была снята и все еще находится в положении "включено".

8. Контроль за функциями проверки

- 056 Эта функция предусмотрена для осуществления контроля за операциями DISPLAYING, PRINTING, VU (ВЫВОД НА ДИСПЛЕЙ, ВЫВОД НА ПЕЧАТЬ, БОРТОВОЕ УСТРОЙСТВО) и за функцией DOWNLOADING (ЗАГРУЗКА), осуществляемой в режиме контроля.
- 057 Эта функция также предусматривает осуществление операций OVER SPEEDING CONTROL (КОНТРОЛЬ ЗА ПРЕВЫШЕНИЕМ СКОРОСТИ) в режиме контроля. Считается, что контроль за превышением скорости производится в том случае, если в режиме контроля на принтер или на дисплей выведена надпись "over speeding" или когда из блока памяти для записей данных бортового устройства загружаются данные "events and faults" ("события и неисправности").

9. Обнаружение событий и/или неисправностей

- 058 Эта функция позволяет обнаруживать следующие события и/или неисправности:

9.1 "Insertion of a non valid card" (ввод недействительной карточки)

- 059 Этот факт отражается в случае ввода любой недействительной карточки и/или в случае истечения срока действия вставленной карточки.

9.2 "Card conflict" (несовместимость карточек)

- 060 Этот факт отображается в том случае, когда имеет место комбинация из любых действительных карточек, отмеченных в следующей таблице знаком "X":

Несовместимость карточки		Считывающее устройство "Водитель"				
		Карточка не вставлена	Карточка водителя	Карточка контролера	Карточка мастерской	Карточка предприятия
Считывающее устройство "Второй водитель"	Карточка не вставлена					
	Карточка водителя				X	
	Карточка контролера			X	X	X
	Карточка мастерской		X	X	X	X
	Карточка предприятия			X	X	X

9.3 "Time overlap" (нестыковка во времени)

061 Этот факт отражается в том случае, когда текущая дата/время ввода карточки в контрольное устройство, считанное с карточки, предшествует дате/времени последнего извлечения карточки водителя.

9.4 "Driving without an appropriate card" (управление без соответствующей карточки)

062 Этот факт отображается в случае любой комбинации карточек тахографа, отмеченной знаком "X" в следующей таблице, когда вид деятельности водителя изменяется на DRIVING (УПРАВЛЕНИЕ) или когда изменяется режим работы в то время, когда деятельность водителя соответствует функции УПРАВЛЕНИЕ:

Управление без соответствующей карточки		Считывающее устройство "Водитель"				
		Карточка не вставлена (или недействительная карточка)	Карточка водителя	Карточка контролера	Карточка мастерской	Карточка предприятия
Считывающее устройство "Второй водитель"	Карточка не вставлена (или недействительная карточка)	X		X		X
	Карточка водителя	X		X	X	X
	Карточка контролера	X	X	X	X	X
	Карточка мастерской	X	X	X		X
	Карточка предприятия	X	X	X	X	X

9.5 "Card insertion while driving" (ввод карточки во время управления)

063 Этот факт отображается в том случае, когда карточка тахографа вставляется в любое считывающее устройство в то время, когда вид деятельности водителя соответствует функции DRIVING (УПРАВЛЕНИЕ).

9.6 "Last card session not correctly closed" (неправильное завершение последнего сеанса использования карточки)

064 Этот факт отображается в том случае, когда в момент ввода карточки в контрольное устройство оно обнаруживает, что, несмотря на положение, изложенное в пункте Ш.1, предыдущий сеанс использования карточки был завершен неправильно (карточка была извлечена прежде, чем на ней были записаны соответствующие данные). Этот факт касается только карточек водителя и мастерской.

9.7 "Over speeding" (превышение скорости)

065 Этот факт отображается в каждом случае превышения скорости.

9.8 "Power supply interruption" (прекращение электропитания)

066 Этот отображается, за исключением режима калибровки, в случае прекращения питания датчика движения и/или бортового устройства в течение более 200 мс. В случае падения напряжения в результате запуска двигателя транспортного средства этот факт отображаться не должен.

9.9 "Motion data error" (ошибочные данные о движении)

067 Этот факт отображается в случае нарушения нормального потока данных между датчиком движения и бортовым устройством и/или в случае ошибки, указывающей на нарушение целостности или аутентичности данных в процессе передачи данных датчиком движения в бортовое устройство.

9.10 "Security breach attempt" (попытка нарушения системы защиты)

068 Этот факт отображается в случае любого другого факта нарушения защиты датчика движения и/или бортового устройства, предусмотренной общими контрольными показателями защиты этих компонентов, за исключением режима калибровки.

9.11 Отказ "Card" (сбой в работе карточки)

069 Этот факт отображается в случае неисправности карточки тахографа, возникшей в процессе работы.

9.12 Отказ "Control device" (сбой в работе контрольного устройства)

070 Этот факт отображается в случае любых отказов, за исключением режима калибровки:

- внутренняя неполадка бортового устройства
- сбой в работе печатающего устройства
- неполадка дисплея
- сбой в работе системы загрузки
- сбой в работе датчика

10. Встроенная система проверки и самопроверки

071 Контрольное устройство должно самостоятельно обнаруживать неисправности посредством проведения самопроверки и с помощью встроенной системы проверки в соответствии со следующей таблицей:

Компонент, подвергаемый проверке	Самопроверка	Встроенная система проверки
Программное обеспечение		Целостность
Блок памяти	Доступ	Доступ, целостность данных
Интерфейсы для считки карточек	Доступ	Доступ
Клавиатура		Ручная проверка
Печатающее устройство	(по усмотрению изготовителя)	Распечатка
Дисплей		Визуальная проверка
Загрузка (осуществляется только в процессе загрузки)	Надлежащая работа	
Датчик	Надлежащая работа	Надлежащая работа

11. Считывание данных, содержащихся в памяти

072 Контрольное устройство должно быть способным считывать любые данные, содержащиеся в его памяти.

12. Регистрация и хранение данных в блоке памяти

Для целей этого пункта

- "365 дней" означает 365 календарных суток усредненной продолжительности деятельности водителя на транспортном средстве. Усредненная продолжительность деятельности в день на транспортном средстве определяется в расчете как минимум 6 водителей или вторых водителей, 6 циклов ввода и извлечения карточек и 256 фактов изменения деятельности. Таким образом, термин "365 дней" включает данные, касающиеся как минимум 2 190 водителей (вторых водителей), 2 190 циклов ввода и извлечения карточек и 93 440 случаев изменения деятельности,
- время регистрируется с точностью до одной минуты, если не предусмотрено иное,
- показания счетчика пробега регистрируются с точностью до одного километра,
- скорость регистрируется с точностью 1 км/ч.

073 Данные, которые хранятся в блоке памяти, не должны нарушаться в результате прекращения внешнего электропитания продолжительностью не более 12 месяцев в условиях, предусмотренных официальным утверждением типа.

074 Контрольное устройство должно быть способно регистрировать и хранить самостоятельно или по команде следующие данные в своей памяти:

12.1 Идентификационные данные оборудования

12.1.1 Идентификационные данные бортового устройства

075 Контрольное устройство должно быть способно хранить в своей памяти следующие идентификационные данные бортового устройства:

- наименование изготовителя,
- адрес изготовителя,
- номер компонентов,

- серийный номер,
- номер версии программного обеспечения,
- дата установки версии программного обеспечения,
- год изготовления устройства,
- номер официального утверждения.

076 Идентификационные данные бортового устройства регистрируются и хранятся раз и навсегда изготовителем бортового устройства, за исключением даты и номера официального утверждения программного обеспечения, которые могут быть изменены в случае перехода на улучшенную версию программы.

12.1.2 Идентификационные данные датчика движения

077 Датчик движения должен быть способен хранить в своей памяти следующие идентификационные данные:

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

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

079 Бортовое устройство должно быть способно регистрировать и хранить в своей памяти следующие идентификационные данные датчика движения, к которому он подсоединен:

- серийный номер,
- номер официального утверждения,
- дата первого подсоединения,

12.2 Элементы защиты

080 Контрольное устройство должно быть способно хранить следующие элементы защиты:

- европейский код общего пользования,
- сертификат Договаривающейся стороны,
- сертификат на устройство,
- закрытый ключ устройства.

Элементы защиты контрольного устройства встраиваются в оборудование изготовителем бортового устройства.

12.3 Данные о вводе и извлечении карточки водителя

081 В случае каждого цикла ввода в устройство карточки водителя или мастерской и ее извлечения из него контрольное устройство должно регистрировать и хранить в своей памяти следующие данные:

- фамилия и имя (имена) держателя карточки, записанные в блоке памяти карточки:
- номер карточки, название выдавшей ее Договаривающейся стороны и дата истечения срока действия, записанные в блоке памяти карточки:
- дата и время ввода,
- показание счетчика пробега транспортного средства в момент ввода карточки,
- считывающее устройство, в которое вставляется карточка,
- дата и время извлечения,
- показания счетчика пробега транспортного средства в момент извлечения карточки,
- следующая информация о предыдущем транспортном средстве, использованном водителем, записанная в блоке памяти карточки:

- VRN (регистрационный номер транспортного средства) и Договаривающаяся сторона регистрации,
- дата и время извлечения карточки,
- метка, указывающая на то, ввел держатель карточки данные о своей деятельности вручную или нет в момент ввода карточки.

082 Блок памяти должен быть способен хранить эти данные в течение не менее 365 дней.

083 Когда объем памяти заполнен, новые данные записываются на самые старые данные.

12.4 Данные о деятельности водителя

084 Контрольное устройство должно регистрировать и хранить в своей памяти все факты изменения деятельности водителя и/или второго водителя и/или все случаи изменения статуса управления и/или все случаи ввода или извлечения карточки водителя или мастерской:

- статус управления (CREW, SINGLE) (ЭКИПАЖ, ОДИН)
- считывающее устройство (DRIVER, CO-DRIVER) (ВОДИТЕЛЬ, ВТОРОЙ ВОДИТЕЛЬ),
- положение карточки в соответствующем считывающем устройстве (INSERTED, NOT INSERTED) (ВСТАВЛЕНА, НЕ ВСТАВЛЕНА) (см. примечание),
- вид деятельности (DRIVING, AVAILABILITY, WORK, BREAK/REST) (УПРАВЛЕНИЕ, ГОТОВНОСТЬ, РАБОТА, ПЕРЕРЫВ/ОТДЫХ),
- дата и время изменения.

Примечание: INSERTED означает, что в считывающее устройство вставлена действительная карточка водителя или мастерской. NOT INSERTED означает обратное, т. е. в считывающем устройстве нет ни действительной карточки водителя, ни действительной карточки мастерской (например, вставлена карточка предприятия или никакая карточка не вставлена).

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

- 085 Блок памяти должен быть способен хранить данные о деятельности водителя как минимум за 365 дней.
- 086 Когда объем памяти заполнен, новые данные записываются на самые старые данные.

12.5 Места, в которых начинаются и/или заканчиваются ежедневные периоды работы

- 087 Контрольное устройство должно регистрировать и хранить в своей памяти все случаи ввода водителем (вторым водителем) названия места, в котором начинается и/или заканчивается ежедневный период работы:
- в случае применимости, номер карточки водителя (второго водителя) и название Договаривающейся стороны, выдавшей карточку,
 - дата и время ввода данных (или дата/время, относящиеся к вводу данных в том случае, когда эта операция производится во время процедуры ручного ввода данных),
 - тип ввода (начало или конец, условие ввода),
 - введенное название страны и района,
 - показания счетчика пробега транспортного средства.
- 088 Блок памяти должен быть способен хранить данные о начале и/или завершении ежедневных периодов работы в течение как минимум 365 дней (при предположении, что один водитель вводит две записи в день).
- 089 Когда объем памяти заполнен, новые данные записываются на самые старые данные.

12.6 Данные о пробеге

- 090 Контрольное устройство должно регистрировать в своей памяти показания счетчика пробега транспортного средства и соответствующую дату в полночь каждого календарного дня.
- 091 Блок памяти должен быть способен хранить показания счетчика пробега, зарегистрированные в полночь каждый день, в течение как минимум 365 календарных дней.
- 092 Когда объем памяти заполнен, новые данные записываются на самые старые данные.

12.7 Детальные данные о скорости

- 093 Контрольное устройство должно регистрировать и хранить в своей памяти мгновенную скорость транспортного средства и соответствующую дату и время с интервалом в 1 секунду как минимум за последние 24 часа, в течение которых транспортное средство находилось в процессе движения.

12.8 Данные о событиях

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

- 094 Устройство должно регистрировать и хранить в своей памяти следующие данные по каждому событию, обнаруженному в соответствии со следующими правилами хранения:

Событие	Правила хранения	Данные по каждому событию, подлежащие регистрации
Несовместимость карточек	<ul style="list-style-type: none"> - 10 самых последних событий 	<ul style="list-style-type: none"> - дата и время начала события - дата и время наступления события - дата и время завершения события - тип карточки, номер карточки и Договаривающаяся сторона, выдавшая две карточки, которые явились причиной несовместимости
Управление без соответствующей карточки	<ul style="list-style-type: none"> - наиболее длительное событие за каждые из 10 последних дней - 5 наиболее продолжительных событий за последние 365 дней 	<ul style="list-style-type: none"> - дата и время начала события - дата и время завершения события - тип карточки, номер карточки и Договаривающаяся сторона, выдавшая любую карточку, вставленную на момент начала и/или завершения данного события - число аналогичных событий за данный день
Ввод карточки в процессе управления	<ul style="list-style-type: none"> - последнее событие за каждый из последних 10 дней 	<ul style="list-style-type: none"> - дата и время события - тип карточки, номер карточки и выдавшая ее Договаривающаяся сторона - число аналогичных событий за указанный день
Неправильное завершение последнего сеанса использования карточки	<ul style="list-style-type: none"> - 10 самых последних событий 	<ul style="list-style-type: none"> - дата и время ввода карточки - тип карточки, номер карточки и выдавшая ее Договаривающаяся сторона - последняя дата сеанса использования, записанная на карточке:

Событие	Правила хранения	Данные по каждому событию, подлежащие регистрации
		<ul style="list-style-type: none"> - дата и время ввода карточки, - регистрационный номер транспортного средства и Договаривающая сторона регистрация
Превышение скорости (1)	<ul style="list-style-type: none"> - наиболее серьезное событие за последние 10 дней (т.е. случай регистрации самой высокой средней скорости) - 5 наиболее серьезных событий за последние 365 дней, - первое событие, наступившее после последней калибровки. 	<ul style="list-style-type: none"> - дата и время начала события - дата и время конца события - максимальная скорость, измеренная во время события - среднее арифметическое скорости, измеренной во время события - тип карточки, номер карточки и выдавшая ее Договаривающаяся сторона водителя (в случае применимости) - число аналогичных событий в указанный день
Прекращение электропитания (2)	<ul style="list-style-type: none"> - самое длительное событие за каждый из 10 последних дней - 5 самых длительных событий за последние 365 дней 	<ul style="list-style-type: none"> - дата и время начала события - дата и время конца события - тип карточки, номер и Договаривающая сторона, выдавшая любую карточку, вставленную в начале и/или конце события - число аналогичных событий в указанный день
Ошибочные данные о движении	<ul style="list-style-type: none"> - самое длительное событие за каждый из 10 последних дней - 5 самых длительных событий за последние 365 дней 	<ul style="list-style-type: none"> - дата и время начала события - дата и время конца события - тип карточки, номер и Договаривающая сторона, выдавшая любую карточку,

Событие	Правила хранения	Данные по каждому событию, подлежащие регистрации
		вставленную в начале и/или конце события - число аналогичных событий в указанный день
Попытка нарушения системы защиты	- 10 самых последних событий по типу события	- дата и время начала события - дата и время конца события (в случае применимости) - тип карточки, номер и Договаривающая сторона, выдавшая любую карточку, вставленную в начале и/или конце события - тип события

095 1) Контрольное устройство должно также регистрировать и хранить в своей памяти :

- дату и время последнего КОНТРОЛЯ ЗА ПРЕВЫШЕНИЕМ СКОРОСТИ (OVER SPEEDING CONTROL),
- дату и время первого превышения скорости после этого 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 должно быть известно с точностью до минуты.

12.9 Данные о неисправностях

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

096 Контрольное устройство должно быть способно регистрировать и хранить в своей памяти следующие данные по каждому обнаруженному сбою в работе в соответствии со следующими правилами хранения:

Неисправность	Правила хранения	Данные о неисправности, подлежащей регистрации
Сбой в работе карточки	- 10 самых последних сбоев в работе карточки водителя	- дата и время начала сбоя - дата и время конца сбоя - тип карточки, номер и выдавшая ее Договаривающаяся сторона
Сбой в работе контрольного устройства	- 10 самых последних сбоев по каждому типу сбоя - первый сбой после последней калибровки	- дата и время начала сбоя - дата и время конца сбоя - тип ошибки - тип карточки, номер и Договаривающаяся сторона, выдавшая любую карточку, вставленную в начале и/или конце ошибки

12.10 Данные калибровки

097 Контрольное устройство должно регистрировать и хранить в своей памяти данные, касающиеся:

- известных параметров калибровки в момент включения,
- самые первые параметры калибровки после включения,
- самые первые параметры калибровки на данном транспортном средстве (идентифицируемом с помощью его опознавательного номера VIN),
- самые последние 5 калибровок (если последние калибровки производятся в течение одного календарного дня, должны храниться данные только о самой последней калибровке в указанный день).

098 По каждой из этих калибровок должны регистрироваться следующие данные:

- цель калибровки (активация, первая установка, установка, периодическая инспекция),
- название и адрес мастерской,

- номер карточки мастерской, Договаривающаяся сторона, выдавшая карточку, и дата истечения срока действия карточки,
- идентификация транспортного средства,
- обновленные или подтвержденные параметры: w, k, l, размер шин, регулировка устройства ограничения скорости, счетчик пробега (прежние и новые показания), дата и время (прежние и новые значения).

099 Датчик движения должен регистрировать и хранить в своей памяти следующие данные, касающиеся установки датчика движения:

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

12.11 Данные о корректировке времени

100 Контрольное устройство должно регистрировать и хранить в своей памяти данные, касающиеся:

- самых последних корректировок времени,
- пяти наиболее серьезных корректировок времени после последней калибровки,

произведенных в режиме калибровки, не относящейся к системе регулярной калибровки (определение f)).

101 Для каждой из этих корректировок времени должны регистрироваться следующие данные:

- дата и время, прежнее значение,
- дата и время, новое значение,
- название и адрес мастерской,
- номер карточки мастерской, Договаривающаяся сторона, выдавшая карточку, и дата истечения срока действия карточки.

12.12 Данные о контрольных операциях

102 Контрольное устройство должно регистрировать и хранить в своей памяти следующие данные, касающиеся самых последних 20 контрольных операций:

- дата и время контроля,
- номер карточки контролера и Договаривающаяся сторона, выдавшая карточку,
- тип контроля (вывод на дисплей и/или на печать и/или загрузка данных с бортового устройства и/или загрузка с карточки).

103 В случае загрузки данных регистрируются также даты самого раннего и самого последнего дня загрузки.

12.13 Данные о блокировке, установленной предприятием

104 Контрольное устройство должно регистрировать и хранить в своей памяти следующие данные, касающиеся 20 самых последних случаев блокировки, установленной предприятием:

- дата и время блокировки,
- дата и время разблокировки,
- номер карточки предприятия и Договаривающаяся сторона, выдавшая карточку,
- название и адрес предприятия.

12.14 Данные об операциях по загрузке

105 Контрольное устройство должно регистрировать и хранить в своей памяти следующие данные, касающиеся последней операции по загрузке данных из блока памяти на внешний носитель в режиме предприятия или калибровки:

- дата и время загрузки,
- номер карточки предприятия или мастерской, Договаривающаяся сторона, выдавшая карточку,
- название предприятия или мастерской.

12.15 Данные об особых ситуациях

105 a) Контрольное устройство должно регистрировать в своей памяти следующие данные, касающиеся особых ситуаций:

- дата и время ввода данных;
- тип особой ситуации.

105 b) Блок памяти данных должен быть способен хранить данные об особых ситуациях как минимум за 365 дней (при предположении, что в среднем ежедневно открывается и закрывается одна позиция, указывающая на особую ситуацию). Когда объем памяти заполнен, новые данные записываются на самые старые данные.

13. Считывание данных с карточки тахографа

106 Контрольное устройство должно быть способно считывать с карточек тахографа в соответствующих случаях необходимые данные в целях:

- идентификации типа карточки, держатель карточки, ранее использованного транспортного средства, даты и времени последнего извлечения карточки и вида деятельности, выбранного в тот момент;
- проверки правильности завершения последнего сеанса использования карточки;
- расчета непрерывного времени управления транспортным средством водителем, совокупное время перерывов и совокупное время управления за предыдущую и текущую неделю;
- вывод на печать требуемых данных, записанных на карточке водителя;
- загрузки данных с карточки водителя на внешний носитель.

107 В случае ошибки при считывании записывающее устройство должно произвести очередную попытку (максимум три раза) выполнения той же команды на считывание данных, после чего, если считать данные не удалось, сообщить, что карточка неисправна и недействительна.

14. Регистрация и хранение данных на карточках тахографа

- 108 Контрольное устройство должно записать "данные о сеансе использования карточки" в карточке водителя или мастерской сразу же после ее ввода.
- 109 Контрольное устройство должно обновлять данные, хранящиеся на действующей карточке водителя, мастерской и/или контролера, со всеми необходимыми данными, относящимися к периоду, в течение которого карточка была вставлена в устройство, и к держателю карточки. Данные, хранящиеся на этих карточках, указываются в главе IV.
- 109 а) Контрольное устройство должно обновлять данные о деятельности водителя и месте (как указано в пунктах 5.2.5 и 5.2.6 главы IV), хранящиеся на действующей карточке водителя и/или предприятия, с учетом данных о виде деятельности и месте, введенных держателем карточки вручную.
- 110 Порядок обновления данных в карточках тахографа должен быть таковым, чтобы в случае необходимости и с учетом фактического объема памяти хранения самые последние данные записывались на самые старые данные.
- 111 В случае ошибки при записи контрольное устройство должно сделать еще одну попытку (максимум три раза) выполнить ту же команду на запись, после чего, если считать данные не удалось, сообщить, что карточка неисправна и недействительна.
- 112 До высвобождения карточки водителя и после сохранения на ней всех соответствующих данных контрольное устройство должно установить "данные о сеансе использования карточки" в исходное состояние.

15. Индикация данных

- 113 Отображаемое сообщение должно включать не менее 20 знаков.
- 114 Минимальный размер знака должен быть 5 мм по высоте и 3,5 мм по ширине.
- 114 а) Дисплей должен поддерживать наборы латинских типа 1 и греческих знаков, определенных в частях 1 и 7 стандарта ISO 8859, как указано в главе 4 "Наборы знаков" подраздела 1. Для индикации данных могут использоваться упрощенные наборные знаки (например, ударные знаки могут отображаться без знака ударения или строчные буквы могут отображаться в виде прописных букв).

- 115 Дисплей должен быть оснащен надлежащей неослепляющей подсветкой.
- 116 Индикация должна быть видимой вне контрольного устройства.
- 117 Контрольное устройство должно быть способно выводить на дисплей:
- данные по умолчанию;
 - данные предупреждения;
 - данные о доступе к меню;
 - другие данные, запрашиваемые пользователем.

Контрольное устройство может выводить на дисплей дополнительную информацию при условии, что ее можно четко отличить от информации, требуемой выше.

- 118 Дисплей контрольного устройства должен использовать пиктограммы или комбинации пиктограмм, перечисленные в подразделе 3. На дисплей могут также выводиться дополнительные пиктограммы или комбинации пиктограмм при условии, что их можно четко отличить от пиктограмм или комбинаций пиктограмм, упомянутых выше.
- 119 Когда транспортное средство находится в процессе движения, дисплей должен быть всегда включен.
- 120 Контрольное устройство может быть оснащено ручной или автоматической функцией, позволяющей отключать дисплей, когда транспортное средство остановлено.

Формат отображения данных указан в подразделе 5.

15.1 Индикация данных по умолчанию

- 121 Когда иную информацию на дисплей выводить не требуется, контрольное устройство 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 его текущим видом деятельности является УПРАВЛЕНИЕ (DRIVING) - текущее время непрерывного управления и текущая продолжительность совокупных перерывов;
 - если его текущим видом деятельности не является УПРАВЛЕНИЕ (DRIVING) - продолжительность его текущей деятельности (с момента выбора этой функции) и совокупная продолжительность перерывов на данный момент;
 - информация, касающаяся второго водителя:
 - продолжительность его текущей деятельности (с момента выбора этой функции).
- 122 Индикация данных, относящихся к каждому водителю, должна быть четкой, полной и однозначной. В том случае, если информацию, относящуюся к водителю и второму водителю, нельзя вывести на дисплей одновременно, контрольное устройство должно отображать информацию, относящуюся к водителю, и давать пользователю возможность выводить на дисплей информацию, относящуюся ко второму водителю.
- 123 В том случае, если ширина дисплея не позволяет отображать по умолчанию режим работы, контрольное устройство должно выводить на дисплей кратковременное сообщение с указанием нового режима работы в момент его изменения.
- 124 Контрольное устройство должно выводить на дисплей кратковременное сообщение с указанием фамилии держателя карточки в момент ее ввода.
- 124a Когда открывается позиция "OUT OF SCOPE" (НЕПРИМЕНИМО), то в этом случае на дисплее должен отображаться по умолчанию с использованием соответствующей пиктограммы тот факт, что эта позиция открыта (при этом допускается, что текущий вид деятельности водителя может в это время не отображаться).

15.2 Предупреждающая индикация

- 125 Контрольное устройство должно выводить на дисплей предупреждающую информацию с использованием прежде всего пиктограмм, указанных в подразделе 3, дополненных, в случае необходимости, дополнительной информацией в виде числового кода. Кроме того, может быть включено текстовое описание предупреждения на языке, выбранном водителем.

15.3 Меню доступа

- 126 Контрольное устройство должно содержать необходимые команды, подаваемые с использованием соответствующего меню.

15.4 Индикация иных данных

- 127 По соответствующей команде можно выводить на дисплей на выборочной основе следующие данные:
- дата и время UTC,
 - режим работы (если он не указывается по умолчанию),
 - продолжительность управления и совокупное время перерывов водителя,
 - продолжительность управления и совокупное время управления вторым водителем,
 - совокупное время управления водителем за предыдущую и текущую неделю,
 - совокупное время управления второго водителя за предыдущую и текущую неделю,
 - содержание любой из шести распечаток в том же формате, что и сами распечатки.
- 128 Вывод 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.

16. Распечатка

129 Контрольное устройство должно быть способно выводить на печать информацию, содержащуюся в его памяти и/или в карточках тахографа, в виде следующих шести видов распечаток:

- ежедневная распечатка данных о деятельности водителя, записанных в карточке,
- ежедневная распечатка данных о деятельности водителя, записанных в бортовом устройстве,
- распечатка данных о событиях и ошибках, хранящихся на карточке,
- распечатка данных о событиях и неисправностях, записанных в бортовом устройстве,
- распечатка технических данных,
- распечатка данных о превышении скорости.

Детальный формат и содержание этих распечаток указываются в подразделе 4.

В конце распечаток могут содержаться дополнительные данные.

Дополнительные распечатки могут также выдаваться контрольным устройством, если они четко отличаются от шести распечаток, упомянутых выше.

130 "Ежедневная распечатка данных о деятельности водителя, записанных на карточке" (driver activities from card daily printout) и "распечатка данных о событиях и неисправностях, записанных на карточке" (Events and faults from card printout) выдается только в том случае, если в контрольное устройство вставлена карточка водителя или карточка мастерской. До выдачи распечатки контрольное устройство обновляет данные, содержащиеся в памяти соответствующей карточки.

131 Для того чтобы сделать "ежедневную распечатку данных о деятельности водителя, записанных на карточке" или "распечатку данных о событиях и неисправностях, записанных на карточке", контрольное устройство должно:

- либо автоматически выбрать карточку водителя или карточку мастерской, если в устройство вставлена только одна из этих карточек,

- либо предусматривать команду, позволяющую выбрать исходную карточку или выбрать карточку, вставленную в считывающее устройство водителя, если в контрольное устройство вставлены обе эти карточки.
- 132 Печатающее устройство должно быть способно печатать 24 знака на строке.
- 133 Минимальный размер знака должен составлять 2,1 мм по высоте и 1,5 мм по ширине.
- 133а Печатающее устройство должно поддерживать наборы латинских знаков типа 1 и греческих знаков, определенных в частях 1 и 7 стандарта ISO 8859, как указано в пункте "Наборы знаков" подраздела 1.
- 134 Печатающее устройство должно быть сконструировано таким образом, чтобы оно могло выдавать эти распечатки такой разрешающей способности, которая исключала бы всякое двоякое толкование при их чтении.
- 135 Распечатки должны сохранять свои размеры и содержащиеся на них данные в нормальных условиях влажности (10-90%) и температуры.
- 136 На бумаге, используемой контрольным устройством, должен быть нанесен соответствующий знак официального утверждения типа и указание типа (типов) контрольного устройства, на котором она используется. Распечатки должны оставаться легко читаемыми и распознаваемыми в обычных условиях хранения (интенсивность света, влажность и температура) в течение не менее одного года.
- 137 Кроме того, необходимо предусмотреть возможность включения в эти документы примечаний, написанных от руки, например подписи водителя.
- 138 В том случае, если во время распечатки закончилась бумага, контрольное устройство должно возобновить печатание после загрузки бумаги с начала распечатки или продолжить печатание с четкой ссылкой на ту часть, которая была выдана на печать ранее.

17. Предупреждения

- 139 Контрольное устройство должно предупреждать водителя в случае обнаружения любого события и/или неисправности.

- 140 Предупреждение о прекращении электропитания может подаваться с задержкой до тех пор, пока электропитание не будет восстановлено.
- 141 Контрольное устройство должно предупреждать водителя за 15 мин. до момента и в тот момент, когда непрерывное время управления превысило 4 час. 30 мин.
- 142 Предупреждения должны быть визуальными. В дополнение к визуальным предупреждениям могут также предусматриваться звуковые предупреждения.
- 143 Визуальные предупреждения должны быть четко распознаваемыми пользователем, располагаться в поле визуального восприятия водителя и быть удобочитаемыми как в дневное, так и в ночное время.
- 144 Система визуального предупреждения может быть встроена в контрольное устройство и/или вынесена за его пределы.
- 145 В последнем случае она должна обозначаться буквой "Т" и быть желтого или оранжевого цвета.
- 146 Предупреждения должны подаваться в течение как минимум 30 секунд, если только пользователь не нажимает на любую клавишу контрольного устройства в порядке подтверждения того, что он принял предупреждение к сведению. Это первое подтверждение не должно влечь за собой стирание выведенной на дисплей причины, указанной в следующем пункте.
- 147 Причина предупреждения должна выводиться на дисплей контрольного устройства и оставаться видимой до тех пор, пока пользователь не введет конкретный код или команду на контрольном устройстве.
- 148 Могут предусматриваться дополнительные предупреждения, если они не вводят водителей в заблуждение по поводу предупреждений, определенных выше.

18. Загрузка данных во внешние носители

- 149 Контрольное устройство должно быть способно загружать по команде данные из своей памяти или из карточки водителя на внешние носители через калибровочный/загрузочный разъем. До загрузки контрольное устройство должно обновить данные, сохраненные на соответствующей карточке.

150 В дополнение и в качестве факультативной функции контрольное устройство может загружать данные в базу данных предприятия, идентифицированного по этому каналу связи, через другой разъем. В таком случае к этой операции загрузки применяются права доступа к данным в режиме предприятия.

151 Загрузка не должна приводить к изменению или стиранию любых сохраненных данных.

Электрический интерфейс калибровочного/загрузочного разъема определяется в подразделе 6.

Протоколы загрузки определяются в подразделе 7.

19. Вывод данных на дополнительные внешние устройства

152 Когда в контрольном устройстве не предусмотрены функции вывода на дисплей показаний скорости и/или счетчика пробега, контрольное устройство должно генерировать выходной сигнал (сигналы), позволяющие выводить на дисплей скорость транспортного средства (показания спидометра) и/или общее расстояние, пройденное транспортным средством (счетчик пробега).

153 Бортовое устройство должно также быть способно выдавать следующие данные по соответствующему специально предназначенному для этой цели последовательному каналу, не зависящему от факультативного подсоединения к шине ЛСК (ISO 11898: Дорожные транспортные средства – Взаимообмен цифровой информацией – Локальная сеть контроллеров (ЛСК) для высокоскоростной передачи данных), в целях их обработки другими электронными устройствами, установленными на транспортном средстве:

- текущая дата и время UTC,
- скорость транспортного средства,
- общее расстояние, пройденное транспортным средством (счетчик пробега),
- текущий вид деятельности, выбранный водителем и вторым водителем,
- информация о том, вставлена ли в данный момент в считывающее устройство водителя и считывающее устройство второго водителя какая-либо карточка тахографа, и (в случае применимости) информация, касающаяся идентификации соответствующих карточек (номер карточки и выдавшая ее Договаривающая сторона).

В дополнение к этому минимальному перечню могут выводиться и иные данные.

Когда зажигание транспортного средства включено, эти данные должны передаваться постоянно. Когда зажигание транспортного средства выключено, должны передаваться как минимум данные об изменении вида деятельности водителя или второго водителя и/или о вводе или извлечении карточки тахографа. В том случае, если передача данных при выключенной системе зажигания транспортного средства приостанавливается, эти данные должны передаваться снова после включения зажигания транспортного средства.

20. Калибровка

154 Функция калибровки позволяет:

- автоматически подсоединять датчик движения к бортовому устройству,
- адаптировать в цифровом режиме постоянную контрольного устройства (k) к характеристическому коэффициенту транспортного средства (w) (транспортные средства с двумя передаточными числами моста или более должны оснащаться соответствующим устройством переключения, с помощью которого эти числа будут автоматически приводиться в соответствие с передаточным числом, на которое было отрегулировано устройство, установленное на транспортном средстве),
- корректировать (без ограничения) текущее время,
- корректировать текущие показания счетчика пробега,
- обновлять идентификационные данные датчика движения, записанные в блоке памяти,
- обновлять или подтверждать другие параметры, заложенные в контрольном устройстве: идентификация транспортного средства, показатели w и l, размер шин и регулировка устройства ограничения скорости (в случае применимости).

155 Подсоединение датчика движения к бортовому устройству заключается, как минимум в:

- обновлении данных установки счетчика движения, содержащихся в памяти датчика движения (при необходимости),
- копировании необходимых идентификационных данных датчика движения и блока памяти датчика движения в блок памяти бортового устройства.

156 Функция калибровки должна обеспечивать ввод необходимых данных с помощью калибровочного/загрузочного разъема в соответствии с протоколом калибровки, определенным в подразделе 8. Функция калибровки может также обеспечивать ввод необходимых данных с помощью других разъемов.

21. Корректировка времени

- 157 Функция корректировки времени должна позволять корректировать текущее время максимум в пределах 1 минуты с интервалами не менее 7 дней.
- 158 Функция корректировки времени должна обеспечивать корректировку текущего времени без каких бы то ни было ограничений в режиме калибровки.

22. Условия работы

- 159 Бортовое устройство должно быть полностью работоспособным в диапазоне температур от -20°C до 70°C , а датчик движения - в диапазоне температур от -40°C до 135°C . Содержание блока памяти должно сохраняться при температурах до -40°C .
- 160 Контрольное устройство должно быть полностью работоспособным в диапазоне мощности от 10% до 90%.
- 161 Контрольное устройство должно быть защищено от бросков напряжения, несоблюдения полярности источника питания и короткого замыкания.

162 Контрольное устройство должно соответствовать Правилам ЕЭК № 10⁹, касающимся электромагнитной совместимости, и должно быть защищено от электростатических разрядов и помех, вызванных переходными процессами.

23. Материалы

163 Все составные части контрольного устройства должны быть изготовлены из материалов, обладающих достаточной устойчивостью и механической прочностью и стабильными электромагнитными характеристиками.

164 В обычных условиях эксплуатации все внутренние компоненты оборудования должны быть защищены от действия влаги и пыли.

165 Бортовое устройство должно соответствовать требованиям уровня защиты IP 40, а датчик движения должен удовлетворять требованиям уровня защиты IP 64 в соответствии со стандартом IEC 529.

166 Контрольное устройство должно соответствовать применимым техническим спецификациям, регламентирующим параметры эргономичности.

167 Контрольное устройство должно быть защищено от случайного повреждения.

24. Маркировка

168 Если контрольное устройство выводит на дисплей показания счетчика пробега транспортного средства и спидометра, то на дисплее должны отображаться следующие символы:

- около цифры, указывающей пройденное расстояние, - единица измерения расстояния, обозначаемая с помощью сокращения "км",
- рядом с цифрой, указывающей скорость, - сокращение "км/ч".

⁹ Исходным текстом в ЕС является директива Комиссии 95/54/ЕС от 31 октября 1995 года, предусматривающая приведение директивы Совета 72/245/ЕЕС о сближении законодательства государств-членов, регламентирующего подавление радиопомех, производимых двигателями с искровым зажиганием, установленными на автотранспортных средствах, в соответствие с техническим прогрессом (OJ No. L 266, 08/11/1995).

Контрольное устройство может также переключаться в режим отображения скорости в милях в час; в этом случае единица измерения скорости указывается с помощью сокращения "mph" (м/ч).

- 169 К каждому отдельному компоненту контрольного устройства должна быть прикреплена табличка с указанием следующих данных:
- название и адрес изготовителя устройства,
 - номер детали, присвоенный изготовителем, и год изготовления устройства,
 - серийный номер устройства.
 - знак официального утверждения типа устройства.
- 170 Если место для указания вышеупомянутых данных на табличке недостаточно, на ней следует, как минимум, проставить название или логотип изготовителя и номер компонента устройства.

IV. ТРЕБОВАНИЯ К КОНСТРУКЦИИ И ФУНКЦИЯМ КАРТОЧЕК ТАХОГРАФА

1. Видимые данные

На первой странице должны быть указаны:

- 171 слова "Driver card" ("Карточка водителя") или "Control card" ("Карточка контролера" или "Workshop card" ("Карточка мастерской") или "Company card" ("Карточка предприятия"), напечатанные крупным шрифтом на официальном языке или языках Договаривающейся стороны, выдавшей карточку, в зависимости от типа карточки¹⁰;
- 172 те же слова, напечатанные на официальных языках ЕЭК ООН на фоне карточки (см. образцы в позиции 178):

EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTRÔLEUR	CARTE D'ATELIER	CARTE D'ENTREPRISE
RU	КАРТОЧКА ВОДИТЕЛЯ	КАРТОЧКА КОНТРОЛЕРА	КАРТОЧКА МАСТЕРСКОЙ	КАРТОЧКА ПРЕДПРИЯТИЯ

- 173 название Договаривающейся стороны, выдавшей карточку (факультативно);

- 174 отличительный знак Договаривающейся стороны, выдавшей карточку.

Официальные отличительные знаки Договаривающихся сторон соответствуют знакам, определенным в Венской конвенции о дорожном движении 1968 года или в Женевской конвенции о дорожном движении 1949 года. Отличительные знаки Договаривающихся сторон ЕСТР указаны ниже:

AL	Албания	GR	Греция	MD	Республика Молдова
AND	Андорра	H	Венгрия	RO	Румыния
A	Австрия	IR	Ирландия	SRB	Сербия
AM	Армения	I	Италия	SK	Словакия
AZ	Азербайджан	KZ	Казахстан	SLO	Словения
BY	Беларусь	LV	Латвия	E	Испания
B	Бельгия	FL	Лихтенштейн	S	Швеция
BIH	Босния и Герцеговина	LT	Литва	CH	Швейцария

¹⁰ Договаривающиеся стороны сообщат в секретариат ЕЭК ООН, какие слова они используют в этом случае на своем национальном языке.

BG	Болгария	L	Люксембург	МК	БЮР Македония
HR	Хорватия	M	Мальта	TR	Турция
CY	Кипр	MNE	Черногория	TM	Туркменистан
CZ	Чешская Республика	NL	Нидерланды	UK	Соединенное Королевство
DK	Дания	N	Норвегия	UA	Украина
EST	Эстония	PL	Польша	UZ	Узбекистан
FIN	Финляндия	P	Португалия		
F	Франция	RUS	Российская Федерация		
D	Германия	RSM	Сан-Марино		

175 конкретные данные, касающиеся выданной карточки, под следующими номерами:

	Карточка водителя	Карточка контроля	Карточка предприятия или мастерской
1.	фамилия водителя	название контрольного органа	название предприятия или мастерской
2.	имя (имена) водителя	фамилия контролера (в случае применимости)	фамилия держателя карточки (в случае применимости)
3.	дата рождения водителя	имя (имена) контролера (в случае применимости)	имя (имена) держателя карточки (в случае применимости)
4. (a)	дата начала срока действия карточки		
(b)	дата истечения срока действия карточки (в соответствующем случае)		
(c)	название компетентного органа, выдавшего карточку (может быть напечатано на стр. 2)		
(d)	номер, отличный от номера, указанного в позиции 5, для административных целей (факультативно)		
5. (a)	номер водительского удостоверения (на дату выдачи карточки водителя)	-	-
5. b)	номер карточки		
6.	фотография водителя	фотография контролера (факультативно)	-
7.	подпись водителя	подпись держателя (факультативно)	
8.	обычное место жительства или почтовый адрес держателя (факультативно)	почтовый адрес контрольного органа	почтовый адрес предприятия или мастерской

176 даты записываются в формате "дд/мм/гггг" или "дд.мм.гггг" (день, месяц, год).

На обратной стороне содержится:

177 разъяснение пронумерованных позиций, содержащихся на лицевой стороне карточки;

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

MODEL TACHOGRAPH CARDS

FRONT	REVERSE
<div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p style="text-align: center;">CP</p> <p>DRIVER CARD</p> <p>1. 2. 3. 4a. 4c. (4d.) 5a. 5b. 7. (8.)</p> </div> <div style="width: 60%;"> <p style="text-align: right;">CONTRACTING PARTY</p> <p style="text-align: right;">4b. Driver Card Carte de conducteur Карточка водителя</p> </div> </div>	<div style="display: flex; justify-content: space-between;"> <div style="width: 30%; text-align: center;"> <p>B</p> </div> <div style="width: 60%;"> <p>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;"><i>Please return to:</i></p> <p style="text-align: center; border: 1px solid black; padding: 2px;">NAME OF AUTHORITY AND ADDRESS</p> </div> <div style="width: 30%; text-align: center;"> <p>A</p> </div> </div>
<div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p style="text-align: center;">CP</p> <p>CONTROL CARD</p> <p>1. (2.) (3.) 4a. 4c. (4d.) 5b. (7.) 8.</p> </div> <div style="width: 60%;"> <p style="text-align: right;">CONTRACTING PARTY</p> <p style="text-align: right;">(4b.) Control Card Carte de contrôleur Карточка контролера</p> </div> </div>	<div style="display: flex; justify-content: space-between;"> <div style="width: 30%; text-align: center;"> <p>B</p> </div> <div style="width: 60%;"> <p>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;"><i>Please return to:</i></p> <p style="text-align: center; border: 1px solid black; padding: 2px;">NAME OF AUTHORITY AND ADDRESS</p> </div> <div style="width: 30%; text-align: center;"> <p>A</p> </div> </div>
<div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p style="text-align: center;">CP</p> <p>WORKSHOP CARD</p> <p>1. (2.) (3.) 4a. 4c. (4d.) 5b. (7.) 8.</p> </div> <div style="width: 60%;"> <p style="text-align: right;">CONTRACTING PARTY</p> <p style="text-align: right;">4b. Control Card Carte de contrôleur Карточка мастерской</p> </div> </div>	<div style="display: flex; justify-content: space-between;"> <div style="width: 30%; text-align: center;"> <p>B</p> </div> <div style="width: 60%;"> <p>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;"><i>Please return to:</i></p> <p style="text-align: center; border: 1px solid black; padding: 2px;">NAME OF AUTHORITY AND ADDRESS</p> </div> <div style="width: 30%; text-align: center;"> <p>A</p> </div> </div>
<div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p style="text-align: center;">CP</p> <p>COMPANY CARD</p> <p>1. (2.) (3.) 4a. 4c. (4d.) 5b. (7.) 8.</p> </div> <div style="width: 60%;"> <p style="text-align: right;">CONTRACTING PARTY</p> <p style="text-align: right;">4b. Company Card Carte d'entreprise Карточка предприятия</p> </div> </div>	<div style="display: flex; justify-content: space-between;"> <div style="width: 30%; text-align: center;"> <p>B</p> </div> <div style="width: 60%;"> <p>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;"><i>Please return to:</i></p> <p style="text-align: center; border: 1px solid black; padding: 2px;">NAME OF AUTHORITY AND ADDRESS</p> </div> <div style="width: 30%; text-align: center;"> <p>A</p> </div> </div>

(Перевод содержания вышеупомянутых образцов приводится ниже)

ОБРАЗЕЦ КАРТОЧЕК ТАХОГРАФА

ЛИЦЕВАЯ СТОРОНА

**Карточка
водителя**

Договаривающая
сторона:

ОБРАТНАЯ СТОРОНА

1. Фамилия 2. Имя (имена) 3. Дата рождения
- 4a. Дата начала действия карточки
- 4b. Дата истечения административного срока действия карточки
- 4c. Компетентный орган, выдавший карточку
- (4d) Не предназначена для административных целей на национальном уровне
- 5a. Номер водительского удостоверения 5b. Номер карточки
6. Фотография
7. Подпись (8.) Адрес

Просьба вернуть:

НАЗВАНИЕ И АДРЕС КОМПЕТЕНТНОГО ОРГАНА

**Карточка
водителя**

Договаривающая
сторона:

1. Контрольный орган 2. Фамилия 3. Имя (имена)
- 4a. Дата начала действия карточки
- 4b. Дата истечения административного срока действия карточки
- 4c. Компетентный орган, выдавший карточку
- (4d) Не предназначена для административных целей на национальном уровне
- 5b. Номер карточки
6. Фотография
7. Подпись; (8.) Адрес

Просьба вернуть:

НАЗВАНИЕ И АДРЕС КОМПЕТЕНТНОГО ОРГАНА

**Карточка
водителя**

Договаривающая
сторона:

1. Название мастерской 2. Фамилия 3. Имя (имена)
- 4a. Дата начала действия карточки
- 4b. Дата истечения административного срока действия карточки
- 4c. Компетентный орган, выдавший карточку
- (4d) Не предназначена для административных целей на национальном уровне
- 5b. Номер карточки
7. Подпись (8.) Адрес

Просьба вернуть:

НАЗВАНИЕ И АДРЕС КОМПЕТЕНТНОГО ОРГАНА

**Карточка
водителя**Договаривающая
сторона:

1. Название предприятия 2. Фамилия 3. Имя
(имена)
- 4а. Дата начала действия карточки
- 4б. Дата истечения административного срока действия
карточки
- 4с. Компетентный орган, выдавший карточку
- (4d) Не предназначена для административных целей на
национальном уровне
- 5б. Номер карточки
7. Подпись (8.) Адрес

*Просьба вернуть:***НАЗВАНИЕ И АДРЕС КОМПЕТЕНТНОГО ОРГАНА**

179 Текст карточек тахографа печатается на фоне следующего цвета:

- карточка водителя: белый,
- карточка контролера: голубой,
- карточка мастерской: красный,
- карточка предприятия: желтый.

180 Карточки тахографа должны содержать как минимум следующие элементы защиты карточки от подделки и фальсификации:

- защитный фон в виде тонкого и радужного узора из пересекающихся линий,
- в районе фотографии - накладка защитного фона на фотографию,
- как минимум одна двухцветная линия, нанесенная способом микропечати.

181 По согласованию с секретариатом ЕЭК ООН Договаривающиеся стороны могут включать цвета или маркировку, например национальные символы и элементы защиты без ущерба для других положений настоящего добавления.

2. Защита

Система защиты имеет целью предохранить целостность и аутентичность данных, передаваемых между карточками и контрольным устройством, предохранение целостности и аутентичности данных, загружаемых с карточки, предоставление возможности производить некоторые операции по записи данных на карточку только контрольным устройством, исключение любой возможности фальсификации

данных, хранящихся в карточках, предотвращение фальсификации и обнаружение любой попытки такого рода.

- 182 В целях обеспечения защиты системы карточки тахографа должны удовлетворять требованиям, предъявляемым к защите, которые предусмотрены общими контрольными показателями защиты карточки тахографа (подраздел 10).
- 183 Карточки тахографа должны считываться другими устройствами, например персональными компьютерами.

3. Стандарты

- 184 Карточки тахографа должны соответствовать следующим стандартам:
- ISO/IEC 7810: Карточки идентификационные - физические характеристики,
 - ISO/IEC 7816: Карточки идентификационные - карточки на интегральных схемах с контактами,
 - Часть 1: Физические характеристики,
 - Часть 2: Размеры и расположение контактов,
 - Часть 3: Электронные сигналы и протоколы передачи данных,
 - Часть 4: Межотраслевые команды обмена данными,
 - Часть 8: Межотраслевые команды обеспечения защиты,
 - ISO/IEC 10373: Карточки идентификационные - методы проверки.

4. Спецификации на окружающие условия и электромагнитную совместимость

- 185 Карточки тахографа должны быть способны правильно работать во всех климатических условиях, которые обычно встречаются на территории Договаривающихся сторон как минимум в диапазоне температур от -25°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 использования карточки.
- 186 Карточки тахографа должны быть способны работать нормально в условиях влажности в диапазоне от 10% до 90%.

- 187 Карточки тахографа должны быть способны правильно работать в течение пяти лет, если они используются с соблюдением указанных спецификаций на окружающие условия и электромагнитную совместимость.
- 188 В процессе работы карточки тахографа должны соответствовать Правилам ЕЭК № 10¹¹, касающимся электромагнитной совместимости, и должны быть защищены от электростатических разрядов.

5. Хранение данных

Для целей настоящего пункта

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

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

- 189 В настоящем пункте определяется минимальный объем памяти хранения различных файлов данных соответствующих приложений. Карточки тахографа должны быть способны передавать контрольному устройству данные о фактическом объеме памяти хранения данных этих файлов.

Любые дополнительные данные, которые могут храниться на карточках тахографа, связанные с иными приложениями, предусмотренными в соответствующих случаях карточкой, хранятся в соответствии с Европейскими положениями¹², касающимися

¹¹ Исходным текстом в ЕС является директива Комиссии 95/54/ЕС от 31 октября 1995 года, предусматривающая приведение директивы Совета 72/245/ЕС о сближении законодательства государств-членов, регламентирующего подавление радиопомех, производимых двигателями с искровым зажиганием, установленными на автотранспортных средствах, в соответствие с техническим прогрессом (ОJ No. L 266, 08/11/1995).

¹² Защита физических лиц в части обработки личных данных и беспрепятственной передачи таких данных соответствует положениям директивы Совета № 95/46/ЕС от 24 октября 1995 года с внесенными в них последними поправками (ОJ No. L 281, 23/11/1995).

защиты физических лиц в части обработки личных данных и беспрепятственной передачи таких данных.

5.1 Идентификация карточки и данные о защите

5.1.1 Идентификация приложений

190 Карточки тахографа должны быть способны хранить следующие идентификационные данные приложений:

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

5.1.2 Идентификация микропроцессора

191 Карточки тахографа должны быть способны хранить следующие идентификационные данные интегральной схемы (ИС):

- серийный номер ИС,
- исходные заводские данные ИС.

5.1.3 Идентификация карточки на интегральной схеме

192 Карточки тахографа должны быть способны хранить следующие идентификационные данные карточки на интегральной схеме:

- серийный номер карточки (включая исходные заводские данные),
- номер официального утверждения типа карточки,
- идентификатор учреждения, персонализирующего карточку (ИД),
- ИД монтажного предприятия,
- идентификатор ИС.

5.1.4 Элементы защиты

193 Карточки тахографа должны быть способны хранить следующие элементы данных, касающихся защиты:

- европейский открытый ключ,
- сертификат Договаривающейся стороны,

- сертификат карточки,
- закрытый ключ карточки.

5.2 Карточка водителя

5.2.1 Идентификация карточки

194 Карточка водителя должна быть способна хранить следующие идентификационные данные карточки:

- номер карточки,
- выдавшая Договаривающаяся сторона, название выдавшего компетентного органа, дата выдачи,
- дата начала действия карточки, дата истечения срока действия карточки.

5.2.2 Идентификация держателю карточки

195 Карточка водителя должна быть способна хранить следующие идентификационные данные держателя карточки:

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

5.2.3 Информация о водительском удостоверении

196 Карточка водителя должна быть способна хранить следующие данные о водительском удостоверении:

- выдавшая Договаривающаяся сторона, название выдавшего компетентного органа,
- номер водительского удостоверения (на дату выдачи карточки).

5.2.4 Данные об используемом транспортном средстве

197 Карточка водителя должна быть способна хранить за каждый календарный день, в течение которого используется эта 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) следующие данные:

- дата и время первого использования транспортного средства (т.е. первый ввод карточки за этот период использования транспортного средства или 00:00 часов, если в этот момент данный период использования продолжается),
- показание счетчика пробега транспортного средства в это время,
- дата и время последнего использования транспортного средства (т.е. последнее извлечение карточки в течение этого периода использования транспортного средства или 23 ч. 59 м., если в этот момент использование продолжается),
- показания счетчика пробега транспортного средства в это время,
- номер регистрации транспортного средства (VRN) и Договаривающаяся сторона регистрации данного транспортного средства.

198 Карточка водителя должна быть способна хранить как минимум 84 такие записи.

5.2.5 Данные о деятельности водителя

199 Карточка водителя должна быть способна хранить за каждый календарный день, в течение которого используется данная карточка или в течение которого водитель внес вручную данные о своей деятельности, следующие данные:

- дата,
- счетчик ежедневного присутствия (показания которого увеличиваются на одну единицу за каждый календарный день),
- общее расстояние, пройденное водителем на транспортном средстве в течение этого дня,
- статус водителя на 00:00 часов,
- во всех случаях когда водитель меняет вид деятельности и/или статус управления и/или вставляет или извлекает свою карточку:

- статус управления (CREW, SINGLE) (ЭКИПАЖ, ОДИН),
- считывающее устройство (DRIVER, CO-DRIVER) (ВОДИТЕЛЬ, ВТОРОЙ ВОДИТЕЛЬ),
- положение карточки (INSERTED, NOT INSERTED) (ВСТАВЛЕНА, НЕ ВСТАВЛЕНА),
- виды деятельности (DRIVING, AVAILABILITY, WORK, BREAK/REST) (УПРАВЛЕНИЕ, ГОТОВНОСТЬ, РАБОТА, ПЕРЕРЫВ/ОТДЫХ),
- время изменения.

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

201 Данные, перечисленные в позициях 197 и 199, должны храниться таким образом, чтобы данные о видах деятельности можно было извлечь из памяти в хронологическом порядке их ввода, даже в случае нестыковки времени.

5.2.6 Места, в которых начинаются и/или заканчиваются ежедневные периоды работы

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

- дата и время ввода (или дата/время, относящиеся к вводу этих данных, если этот ввод производится вручную),
- тип ввода (начало или конец, условия ввода),
- страна или район въезда,
- показания счетчика пробега транспортного средства.

203 Блок памяти карточки водителя должен быть способен хранить как минимум 42 пары таких записей.

5.2.7 Данные о событиях

Для целей настоящего подпункта данные о времени должны регистрироваться с точностью до одной секунды.

- 204 Карточка водителя должна быть способна хранить данные, касающиеся соответствующих событий, обнаруженных контрольным устройством со вставленной в него карточкой:
- нестыковка 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),
 - последний сеанс использования карточки, который был завершен неправильно (в тех случаях когда причиной этого события является данная карточка),
 - прекращение электропитания,
 - ошибка данных о движении,
 - попытки нарушения защиты.
- 205 Карточка водителя должна быть способна хранить следующие данные об этих событиях:
- код события,
 - дата и время начала события (или ввода карточки, если это событие в данный момент продолжается),
 - дата и время конца события (или извлечения карточки, если в данный момент это событие продолжается),
 - регистрационный номер транспортного средства (VRN) и Договаривающаяся сторона регистрации транспортного средства, к которому относится это событие.

Примечание: В случае события "Нестыковка времени":

- дата и время начала события должны соответствовать дате и времени извлечения карточки из предыдущего транспортного средства,
- дата и время завершения события должны соответствовать дате и времени ввода карточки в транспортное средство, используемое в данный момент,
- данные о транспортном средстве должны соответствовать используемому транспортному средству, к которому относится данное событие.

Примечание: В случае события "последний сеанс использования карточки завершен неправильно":

- дата и время начала события должны соответствовать дате и времени ввода карточки применительно к неправильно завершенному сеансу ее использования,
- дата и время завершения события должны соответствовать дате и времени ввода карточки, относящегося к сеансу ее использования, в ходе которого было обнаружено данное событие (текущий сеанс),
- данные о транспортном средстве должны соответствовать транспортному средству, на котором сеанс использования карточки был завершен неправильно.

206 Карточка водителя должна быть способна хранить данные о шести самых последних событиях каждого типа (т.е. 36 событий).

5.2.8 Данные о неисправностях

Для целей этого подпункта время регистрируется с точностью до одной секунды.

207 Карточка водителя должна быть способна хранить данные, касающиеся следующих неисправностей, обнаруженных устройством с введенной в него карточкой:

- сбой в работе карточки (в том случае если причиной события является карточка),

- сбой в работе контрольного устройства.

208 Карточка водителя должна быть способна хранить следующие данные об этих неисправностях:

- код неисправности,
- дата и время начала неисправности (или ввода карточки, если на данный момент времени неисправность сохраняется),
- дата и время прекращения неисправности (или извлечения карточки, если в данный момент времени неисправность сохраняется),
- регистрационный номер транспортного средства (VRN) и страна регистрации транспортного средства, на котором произошла данная неисправность.

209 Карточка водителя должна быть способна хранить данные о 12 самых последних неисправностях каждого типа (т.е. 24 неисправности).

5.2.9 Данные о проверочных операциях

210 Карточка водителя должна быть способна хранить следующие данные, касающиеся проверочных операций:

- дата и время проверки,
- номер контрольной карточки и название выдавшей ее Договаривающейся стороны,
- тип проверки (вывод на дисплей и/или на печать, и/или загрузка данных с бортового устройства, и/или загрузка данных с карточки (см. примечание)),
- период, за который загружаются данные, - в случае загрузки,
- регистрационный номер транспортного средства (VRN) и название Договаривающейся стороны регистрации транспортного средства, на котором производилась проверка.

Примечание: Требования, предъявляемые к защите, предполагают, что факт загрузки данных с карточки будет регистрироваться только в том случае, если он производится с помощью контрольного устройства.

211 Карточка водителя должна быть способна хранить одну такую запись.

5.2.10 Данные о сеансе использования карточки

212 Карточка водителя должна быть способна хранить данные, касающиеся транспортного средства, на котором был начат сеанс ее использования:

- дата и время начала сеанса (т.е. ввода карточки) с точностью до одной секунды,
- регистрационный номер транспортного средства (VRN) и название Договаривающейся стороны регистрации.

5.2.11 Данные об особых ситуациях

212a Карточка водителя должна быть способна хранить следующие данные, касающиеся особых ситуаций, введенных в то время, когда карточка была вставлена в контрольное устройство (независимо от считывающего устройства):

- дата и время начала ввода,
- тип особой ситуации.

212b Карточка водителя должна быть способна хранить 56 таких записей.

5.3 Карточка мастерской

5.3.1 Элементы защиты

213 Карточка мастерской должна быть способна хранить персональный идентификационный номер (PIN-код).

214 Карточка мастерской должна быть способна хранить криптографические ключи, необходимые для подсоединения датчиков движения к бортовым устройствам.

5.3.2 Идентификация карточки

215 Карточка мастерской должна быть способна хранить следующие идентификационные данные карточки:

- номер карточки,
- выдавшая ее Договаривающаяся сторона, название выдавшего ее компетентного органа, дата выдачи,
- дата начала действия карточки, дата истечения срока действия карточки.

5.3.3 Идентификация держателя карточки

216 Карточка мастерской должна быть способна хранить следующие идентификационные данные о держателе карточки:

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

5.3.4 Данные об используемом транспортном средстве

217 Карточка мастерской должна быть способна хранить записанные данные об используемых транспортных средствах таким же образом, как и карточка водителя.

218 Карточка мастерской должна быть способна хранить как минимум четыре таких записи.

5.3.5 Данные о деятельности водителя

219 Карточка мастерской должна быть способна хранить данные о деятельности водителя таким же образом, как и карточка водителя.

220 Карточка мастерской должна быть способна хранить данные о деятельности водителя как минимум за один день усредненной деятельности водителя.

5.3.6 Данные о начале и/или завершении ежедневных периодов работы

- 221 Карточка мастерской должна быть способна хранить записанные данные о начале и/или завершении ежедневных периодов работы таким же образом, как и карточка водителя.
- 222 Карточка мастерской должна быть способна хранить как минимум три пары таких записей.

5.3.7 Данные о событиях и неисправностях

- 223 Карточка мастерской должна быть способна хранить записанные данные о событиях и неисправностях таким же образом, как и карточка водителя.
- 224 Карточка мастерской должна быть способна хранить данные о трех самых последних событиях каждого типа (т.е. 18 событий) и о шести самых последних неисправностях каждого типа (т.е. 12 неисправностей).

5.3.8 Данные о проверочных операциях

- 225 Карточка мастерской должна быть способна хранить записанные данные о проверочных операциях таким же образом, как и карточка водителя.

5.3.9 Данные о калибровке и корректировке времени

- 226 Карточка мастерской должна быть способна хранить записанные данные о калибровке и/или корректировке времени, произведенной в то время, когда карточка была вставлена в контрольное устройство.
- 227 Каждая запись калибровки должна быть способна хранить следующие данные:
- цель калибровки (активация, первая установка, установка, периодическая инспекция),
 - идентификация транспортного средства,
 - обновленные или подтвержденные параметры (w, k, l, размер шин, регулировка устройства ограничения скорости, показания счетчика пробега (новые и прежние показания), дата и время (новые и прежние показания)),

- идентификация контрольного устройства (номер деталей бортового устройства (БУ), серийный номер бортового устройства (БУ), серийный номер датчика движения).

228 Карточка мастерской должна быть способна хранить как минимум 88 таких записей.

229 Карточка мастерской должна иметь счетчик, указывающий число калибровок, произведенных на карточке.

230 Карточка мастерской должна иметь счетчик, указывающий общее число калибровок, произведенных с момента последней загрузки данных.

5.3.10 Данные об особых ситуациях

230a Карточка мастерской должна быть способна хранить данные, касающиеся особых ситуаций, таким же образом, как и карточка водителя. Карточка мастерской должна быть способна хранить две такие записи.

5.4 Карточка контролера

5.4.1 Идентификация карточки

231 Карточка мастерской должна быть способна хранить следующие идентификационные данные карточки:

- номер карточки,
- выдавшая ее Договаривающаяся сторона, название выдавшего компетентного органа, дата выдачи,
- дата начала действия карточки, дата истечения срока действия карточки (в соответствующем случае).

5.4.2 Идентификация держателя карточки

232 Карточка контролера должна быть в состоянии хранить следующие идентификационные данные держателя карточки:

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

5.4.3 Данные о проверочных операциях

233 Карточка контролера должна быть способна хранить следующие данные о проверочных операциях:

- дата и время проверки,
- тип проверки (вывод на дисплей и/или на печать и/или загрузка данных с бортового устройства и/или загрузка с карточки),
- период, за который загружаются данные (в соответствующих случаях),
- регистрационный номер транспортного средства (VRN) компетентный орган Договаривающейся стороны, зарегистрировавший проверенное транспортное средство,
- номер проверенной карточки водителя и выдавшая ее Договаривающаяся сторона.

234 Карточка контролера должна быть способна хранить как минимум 230 таких записей.

5.5 Карточка предприятия

5.5.1 Идентификация карточки

235 Карточка предприятия должна быть способна хранить идентификационные данные карточки:

- номер карточки,
- выдавшая ее Договаривающаяся сторона, название выдавшего компетентного органа, дата выдачи,

- дата начала действия карточки, дата истечения срока действия карточки (в соответствующем случае).

5.5.2 Идентификация держателя карточки

236 Карточка предприятия должна быть способна хранить следующие идентификационные данные держателя карточки:

- название предприятия,
- адрес предприятия.

5.5.3 Данные о действиях предприятия

237 Карточка предприятия должна быть способна хранить следующие данные о действиях предприятия:

- дата и время соответствующего действия,
- тип действия (блокировка и/или разблокировка бортового устройства и/или загрузка данных с бортового устройства и/или загрузка данных с карточки),
- период, за который загружаются данные (в соответствующем случае),
- регистрационный номер транспортного средства (VRN) и компетентный орган Договаривающейся стороны, зарегистрировавшей транспортное средство,
- номер карточки и название выдавшей ее Договаривающейся стороны (в случае загрузки данных с карточки).

238 Карточка предприятия должна быть способна хранить как минимум 230 таких записей.

V. УСТАНОВКА КОНТРОЛЬНОГО УСТРОЙСТВА

1. Установка

- 239 Новые контрольные устройства поставляются механикам и изготовителям транспортного средства неактивированными со всеми параметрами калибровки, перечисленными в главе III.20, выставленными на соответствующие и действующие значения по умолчанию. В тех случаях, когда какое-либо конкретное значение не соответствует заданному, буквенные параметры отображаются в виде строк из вопросительных знаков "?", а числовые параметры устанавливаются на ноль "0".
- 240 До активации контрольное устройство должно обеспечивать доступ к функции калибровки, даже если в режим калибровки оно не установлено.
- 241 До активации контрольное устройство не должно ни регистрировать, ни хранить данные, указанные в пунктах III.12.3-III.12.9 и III.12.12-III.12.14, включительно.
- 242 В процессе установки изготовители транспортных средств предварительно устанавливают все известные параметры.
- 243 Изготовители транспортных средств или механики должны активировать установленное контрольное устройство до выезда транспортного средства из цеха, в котором производилась установка.
- 244 Активация контрольного устройства должна производиться автоматически в результате первого ввода карточки предприятия в любое из считывающих устройств карточки.
- 245 Конкретные операции по подсоединению датчика движения и бортового устройства, если таковые требуются, должны производиться автоматически до или во время активации.
- 246 После активации контрольное устройство должно полностью обеспечивать контроль за доступом к функциям и соответствующим данным.
- 247 Функции регистрации и хранения контрольного устройства после его активации должны быть полностью работоспособными.

248 После установки производится калибровка. Первая калибровка должна включать ввод регистрационного номера транспортного средства (VRN) и должна производиться не позже, чем через две недели после установки или присвоения регистрационного номера транспортного средства, в зависимости от того, какое из этих событий наступает позже.

248a Контрольное устройство должно быть установлено в транспортном средстве таким образом, чтобы водитель имел доступ ко всем необходимым функциям со своего места.

2. Установочная табличка

249 После проверки установленного контрольного устройства на него, внутри или сзади, должна устанавливаться четко видимая и легко доступная установочная табличка. После каждой инспекции, проведенной уполномоченным механиком или мастерской, на месте прежней таблички устанавливается новая.

250 На табличке должны содержаться как минимум следующие данные:

- название, адрес или фирменный знак уполномоченного механика или предприятия,
- характеристический коэффициент транспортного средства в форме " $w = \text{imp/km} \dots$ " (" $w = \dots$ имп./км"),
- постоянная контрольного устройства в форме " $k = \dots \text{imp/km}$ " (" $k = \text{имп./км}$ "),
- эффективная окружность шин колес в форме " $l = \dots \text{mm}$ " (" $l = \text{мм}$ "),
- размер шин,
- дата определения характеристического коэффициента транспортного средства и измерение эффективной окружности шин колес,
- опознавательный номер транспортного средства.

3. Наложение пломб

251 Пломбы накладываются на следующие детали:

- любое соединение, которое в случае его нарушения приведет к необнаруживаемым изменениям или к необнаруживаемой потере данных;
- установочную табличку, если только она не прикреплена таким образом, что ее нельзя снять, не повредив нанесенную на ней маркировку.

252 Указанные выше пломбы могут быть сняты:

- в случае аварийной ситуации,
- в целях установки, регулировки или ремонта устройства ограничения скорости или любого иного устройства обеспечения безопасности дорожного движения, при условии, что контрольное устройство продолжает функционировать надежно и правильно и пломбируется уполномоченным механиком или предприятием (в соответствии с главой VI) сразу же после установки устройства ограничения скорости или любого иного устройства обеспечения безопасности дорожного движения или в течение семи дней в других случаях.

253 Каждый случай нарушения этих пломб должен быть предметом письменного уведомления компетентного органа с указанием причин, по которым были произведены такие действия.

VI. ПРОВЕРКА, ИНСПЕКЦИЯ И РЕМОНТ

Требования, регламентирующие обстоятельства, в которых могут быть сняты пломбы, как указано в пункте 5 статьи 9 приложения к настоящему Соглашению, определяются в части 3 главы V настоящего добавления.

1. Утверждение механиков или мастерских

Договаривающаяся сторона утверждает, регулярно контролирует и аттестует организации, которым поручена:

- установка,
- проверка,
- инспекция,
- ремонт.

На основании пункта 1 статьи 9 приложения к настоящему Соглашению карточки мастерской выдаются только механикам и/или мастерским, которые уполномочены производить активацию и/или калибровку контрольного устройства в соответствии с настоящим добавлением и, за исключением должным образом обоснованных случаев:

- которые не имеют права на карточку предприятия,
- и иная профессиональная деятельность которых не может поставить под угрозу общую защиту системы, определенную в подразделе 10.

2. Проверка новых или отремонтированных приборов

254 Каждое отдельное устройство, будь то новое или отремонтированное, должно проверяться на предмет его надлежащего функционирования и точности его показаний и записей в пределах, изложенных в главе III.2.1 и III.2.2, посредством наложения пломб в соответствии с главой V.3 и в соответствии с параметрами калибровки.

3. Инспекция после установки

255 Во время установки на транспортное средство весь сборочный узел, включая контрольное устройство, должен соответствовать положениям, регламентирующим максимальные допуски, указанные в главе III.2.1 и III.2.2.

4. Периодические инспекции

256 Периодические инспекции оборудования, установленного на транспортных средствах, должны производиться 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 регистрационного номера транспортного средства (VRN) не реже одного раза в два года (24 месяца) после последней инспекции.

257 Эти инспекции включают следующие проверки, имеющие целью убедиться в том, что:

- контрольное устройство работает нормально, включая функцию хранения данных на карточках тахографа,
- положения главы III.2.1 и III.2.2 о максимальных допусках при установке соблюдаются должным образом,
- на контрольном устройстве проставлен знак официального утверждения типа,
- установочная табличка имеется,
- пломбы на устройстве и других частях оборудования не нарушены,
- размер шин и фактическая окружность шин колес соответствуют нормам.

258 Эти инспекции включают калибровку.

5. Измерение погрешностей

259 Измерение погрешностей в процессе установки и в ходе эксплуатации производится в следующих условиях, которые должны рассматриваться в качестве обычных условий испытания:

- транспортное средство в снаряженном состоянии без груза,
- давление в шинах соответствует инструкциям изготовителя,
- износ шин в пределах, допускаемых национальным законодательством,
- движение транспортного средства,
- транспортное средство движется вперед на своем двигателе по прямой линии по ровной дороге на скорости 50 ± 5 км/ч. Измеряемое расстояние должно составлять не менее 1 000 метров,

- для проведения этого испытания могут также использоваться альтернативные методы, например использование соответствующего испытательного стенда при условии обеспечения сопоставимой точности.

6. Ремонт

- 260 Мастерские должны иметь возможность загружать данные с контрольного устройства для их передачи соответствующему транспортному предприятию.
- 261 Утвержденные мастерские должны выдавать транспортным предприятиям свидетельство, подтверждающее невозможность загрузки данных в том случае, когда неисправность контрольного устройства не позволяет загрузить ранее записанные данные даже после ремонта, произведенного данной мастерской. Мастерские хранят копию каждого выданного свидетельства в течение как минимум одного года.

VII. ВЫДАЧА КАРТОЧЕК

Порядок выдачи карточек, установленный Договаривающимися сторонами, должен соответствовать следующим предписаниям.

- 262 В случае первой выдачи карточки тахографа соответствующему заявителю номер карточки должен иметь порядковый индекс (в случае применимости), индекс замены и индекс возобновления, установленные на "0".
- 263 В случае всех неиндивидуальных карточек тахографа, выданных одному контрольному органу или одной мастерской или одному транспортному предприятию, первые 13 цифр номеров карточек должны быть одинаковыми, но порядковый индекс должен быть иным.
- 264 Карточка тахографа, выданная в порядке замены существующей карточки тахографа, должна иметь тот же номер, что и номер замененной карточки, за исключением индекса замены, который увеличивается на 1 (в порядке 0, ..., 9, A, ..., Z).
- 265 Карточка тахографа, выданная в порядке замены существующей карточки тахографа, должна иметь ту же дату истечения срока действия, что и замененная карточка.
- 266 Карточка тахографа, выданная в порядке возобновления существующей карточки тахографа, должна иметь тот же номер карточки, что и возобновленная карточка, за исключением индекса замены, который устанавливается на "0", и индекса возобновления, который увеличивается на 1 (в порядке 0, ..., 9, A, ..., Z).
- 267 Обмен существующей карточки тахографа в целях изменения административной даты производится в соответствии с правилами возобновления, если это происходит в той же Договаривающейся стороне или в соответствии с правилами первой выдачи карточки, если это происходит в другой Договаривающейся стороне.
- 268 В случае неиндивидуальных карточек мастерской или контрольных карточек в позиции "card holder surname" (фамилия держателя карточки), проставляется название мастерской или контрольного органа.

VIII. ОФИЦИАЛЬНОЕ УТВЕРЖДЕНИЕ ТИПА КОНТРОЛЬНОГО УСТРОЙСТВА И КАРТОЧЕК ТАХОГРАФА

1. Общие положения

Для целей настоящей главы слова "control device" (контрольное устройство) означает контрольное устройство или его компоненты. Официальное утверждение типа электропроводки, связывающей датчик движения с бортовым устройством, не требуется. Бумага, используемая контрольным устройством, рассматривается в качестве одного из компонентов контрольного устройства.

- 269 Контрольное устройство представляется на официальное утверждение в сборе вместе со всеми комплектующими дополнительными устройствами.
- 270 Официальное утверждение типа контрольного устройства и карточек тахографа должна включать соответствующую проверку защиты, функциональную проверку и проверку на эксплуатационную совместимость. Положительные результаты каждой из этих проверок должны подтверждаться соответствующим сертификатом.
- 271 Компетентные органы Договаривающейся стороны, предоставляющие официальное утверждение типа, выдают свидетельство об официальном утверждении типа контрольного устройства или карточки тахографа, представленных на официальное утверждение типа, в соответствии со статьей 2 приложения к ЕСТР только при наличии:
- сертификата защиты,
 - сертификата функциональности,
 - сертификата эксплуатационной совместимости.
- 272 Любое изменение программного обеспечения или аппаратного оборудования или характера материалов, использованных для его изготовления, должно в предварительном порядке доводиться до сведения компетентного органа, который предоставил официальное утверждение оборудования по типу конструкции. Этот орган должен подтвердить изготовителю факт распространения официального утверждения данного типа или потребовать обновления или подтверждения соответствующего сертификата функциональности, сертификата защиты и/или сертификата эксплуатационной совместимости.
- 273 Процедуры совершенствования программного обеспечения контрольного устройства непосредственно на месте должны утверждаться компетентным органом, выдавшим

официальное утверждение типа контрольного устройства. Усовершенствованная версия программного обеспечения не должна приводить к изменению или стиранию любых данных о деятельности водителя, хранящихся в блоке памяти контрольного устройства. Усовершенствование программного обеспечения может производиться только под ответственность изготовителя данного устройства.

2. Сертификат защиты

274 Сертификат защиты выдается в соответствии с положениями подраздела 10 настоящего добавления.

3. Сертификат функциональности

275 Каждый претендент на получение официального утверждения типа направляет компетентному органу Договаривающейся стороны, предоставляющему официальное утверждение типа, все материалы и документацию, которые этот компетентный орган считают необходимыми.

276 Сертификат функциональности выдается изготовителю только по итогам всех требуемых успешно проведенных функциональных проверок, предусмотренных в подразделе 9.

277 Сертификат функциональности выдается компетентным органом, предоставляющим официальное утверждение типа. В этом сертификате должен содержаться, помимо названия его владельца и идентификационных данных модели, подробный перечень произведенных проверок и полученных результатов.

4. Сертификат эксплуатационной совместимости

278 Проверки на эксплуатационную совместимость проводятся одной и той же компетентной лабораторией, признанной на международном уровне.

279 Эта лаборатория регистрирует заявки на проведение проверок на эксплуатационную совместимость, представленные изготовителями, в хронологическом порядке их поступления.

280 Заявки официально регистрируются только в случае предоставления в распоряжение лаборатории:

- всего комплекта материалов и документов, необходимых для проведения таких проверок на предмет эксплуатационной совместимости,
- соответствующего сертификата защиты,
- соответствующего сертификата функциональности.

Дата регистрации заявки доводится до сведения изготовителя.

- 281 Проверки на эксплуатационную совместимость контрольного устройства или карточки тахографа, на которые не был выдан сертификат защиты или сертификат функциональности, лабораторией не проводятся.
- 282 Любой изготовитель, подавший заявку на проведение проверок на эксплуатационную совместимость, берет на себя обязательство передать на хранение лаборатории, уполномоченной проводить эти проверки, весь комплект материалов и документов, которые он предоставил для проведения этих проверок.
- 283 Проверки на эксплуатационную совместимость всех типов контрольных устройств или карточек тахографа:
- в случае которых официальное утверждение типа продолжает действовать или
 - в случае которых официальное утверждение типа находится на рассмотрении и на которые действующие сертификаты эксплуатационной совместимости не выданы, проводятся в соответствии с положениями пункта 5 подраздела 9 настоящего добавления.
- 284 Сертификат эксплуатационной совместимости выдается лабораторией изготовителю только по итогам всех требуемых успешно проведенных проверок на эксплуатационную совместимость.
- 285 Если одно или более контрольных устройств или карточек тахографа не прошли проверки на эксплуатационную совместимость, как это предусмотрено требованием 283, то сертификат эксплуатационной совместимости не выдается до тех пор, пока изготовитель, представивший заявку, не произведет необходимые изменения и не проведет успешные проверки на эксплуатационную совместимость. Лаборатория определяет причину проблемы с помощью изготовителей, которых касается данное несоответствие требованиям к эксплуатационной совместимости, и стремится оказать изготовителю, подавшему заявку, помощь в поиске соответствующего технического решения. В том случае, если изготовитель модифицировал свое изделие, он обязан удостовериться в соответствующих

компетентных органах в том, что сертификат защиты и сертификат функциональности продолжают действовать.

- 286 Сертификат об эксплуатационной совместимости действует в течение шести месяцев. Если изготовитель не получил соответствующее свидетельство об официальном утверждении типа, его срок действия в конце этого периода истекает. Он препровождается изготовителем компетентному органу Договаривающейся стороны, предоставляющему официальное утверждение типа, который выдал сертификат функциональности.
- 287 Любой элемент, который может явиться причиной несоответствия требованиям к эксплуатационной совместимости, не должен использоваться в целях получения какой бы то ни было выгоды или приводить к созданию доминирующего положения.

5. Свидетельство об официальном утверждении типа

- 288 Орган Договаривающейся стороны, предоставляющий официальное утверждение типа, может выдавать свидетельство об официальном утверждении типа после того, как он получает в свое распоряжение все три требуемых сертификата.
- 289 Копия свидетельства об официальном утверждении типа направляется компетентным органом, предоставляющим официальное утверждение типа, лаборатории, уполномоченной проводить проверки на эксплуатационную совместимость, в момент его выдачи изготовителю.
- 290 Лаборатория, уполномоченная проводить проверки на эксплуатационную совместимость, должна вести открытый вебсайт, на котором должен содержаться обновленный перечень образцов контрольных устройств или карточек тахографа:
- в отношении которых была зарегистрирована заявка на проведение проверок на эксплуатационную совместимость,
 - на которые был выдан сертификат эксплуатационной совместимости (даже временный),
 - на которые было выдано свидетельство об официальном утверждении типа.

6. Зарезервировано

Эта часть (Исключительная процедура: первый сертификат эксплуатационной совместимости) к ЕСТР не относится.

ПОДРАЗДЕЛ I
СЛОВАРЬ ДАННЫХ
СОДЕРЖАНИЕ

	Стр.
1. Введение.....	98
1.1 Метод определения типа данных.....	98
1.2 Источники	99
2. Определения типов данных.....	100
2.1 ActivityChangeInfo (данные об изменении вида деятельности).....	100
2.2 Address (адрес).....	102
2.3 BCDSString (строка BCD).....	102
2.4 CalibrationPurpose (цель калибровки).....	103
2.5 CardActivityDailyRecord (запись вида деятельности на карточке).....	103
2.6 CardActivityLengthRange (длина записи о деятельности на карточке)	104
2.7 CardApprovalNumber (номер официального утверждения карточки).....	104
2.8 CardCertificate (сертификат карточки)	104
2.9 CardChipIdentification (идентификация микропроцессора карточки)	105
2.10 CardConsecutiveIndex (порядковый индекс карточки).....	105
2.11 CardControlActivityDataRecord (запись данных о проведенных операциях).....	105
2.12 CardCurrentUse (текущее использование карточки)	106
2.13 CardDriverActivity (деятельность водителя).....	106
2.14 CardDrivingLicenceInformation (информация о водительском удостоверении)	107
2.15 CardEventData (данные о событиях).....	108
2.16 CardEventRecord (запись о событиях)	108
2.17 CardFaultData (данные о сбоях в работе карточки).....	109
2.18 CardFaultRecord (запись о сбоях в работе карточки)	109
2.19 CardIccIdentification (идентификация ИС карточки)	110
2.20 CardIdentification (идентификация карточки).....	110
2.21 CardNumber (номер карточки)	111
2.22 CardPlaceDailyWorkPeriod (ежедневный период работы и место).....	112
2.23 CardPrivateKey (закрытый ключ карточки)	113
2.24 CardPublicKey (открытый ключ карточки)	113
2.25 CardRenewalIndex (индекс возобновления карточки).....	113
2.26 CardReplacementIndex (индекс замены карточки).....	113
2.27 CardSlotNumber (номер считывающего устройства карточки).....	113
2.28 CardSlotsStatus (состояние считывающих устройств карточки).....	114
2.29 CardStructureVersion (вариант структуры карточки)	114
2.30 CardVehicleRecord (запись использования транспортного средства)	115
2.31 CardVehiclesUsed (использованное транспортное средство).....	116

СОДЕРЖАНИЕ (продолжение)

	Стр.
2.32 Certificate (сертификат)	116
2.33 CertificateContent (содержание сертификата)	117
2.34 CertificateHolderAuthorisation (разрешение держателя сертификата)	117
2.35 CertificateRequestID (запрос на идентификацию сертификата)	118
2.36 CertificationAuthorityKID (сертификационный орган KID).....	118
2.37 CompanyActivityData (данные об операциях с карточкой предприятия)	119
2.38 CompanyActivityType (тип операции, произведенной предприятием)	120
2.39 CompanyCardApplicationIdentification (идентификация приложения карточки предприятия)	120
2.40 CompanyCardHolderIdentification (идентификация держателя карточки предприятия)	121
2.41 ControlCardApplicationIdentification (идентификация приложения карточки контролера).....	121
2.42 ControlCardControlActivityData (данные о проверочных операциях на карточке контролера)	122
2.43 ControlCardHolderIdentification (идентификация держателя карточки контролера).....	123
2.44 ControlType (тип проверки)	123
2.45 CurrentDateTime (текущая дата/время).....	124
2.46 DailyPresenceCounter (счетчик ежедневного присутствия).....	125
2.47 Datef (формат даты).....	125
2.48 Distance (расстояние)	125
2.49 DriverCardApplicationIdentification (идентификация приложения карточки водителя).....	126
2.50 DriverCardHolderIdentification (идентификация держателя карточки водителя).....	127
2.51 EntryTypeDailyWorkPeriod (тип ввода данных о ежедневных периодах работы).....	127
2.52 EquipmentType (тип оборудования).....	128
2.53 EuropeanPublicKey (европейский открытый ключ).....	128
2.54 EventFaultType (тип неисправности)	128
2.55 EventFaultRecordPurpose (цель регистрации события или неисправности)..	130
2.56 ExtendedSerialNumber (расширенный номер серии).....	130
2.57 FullCardNumber (полный номер карточки).....	131
2.58 HighResOdometer (показания счетчика пробега).....	132
2.59 HighResTripDistance (расстояние, пройденное за рейс)	132
2.60 HolderName (фамилия держателя)	132
2.61 K-ConstantOfRecordingEquipment (постоянная K записывающего оборудования)	133
2.62 KeyIdentifier (идентификатор ключа).....	133

СОДЕРЖАНИЕ (продолжение)

	Стр.
2.63 L-TyreCircumference (окружность шины L)	133
2.64 Language (язык)	134
2.65 LastCardDownload (последняя дата загрузки с карточки)	134
2.66 ManualInputFlag (метка ручного ввода)	134
2.67 ManufacturerCode (код изготовителя).....	134
2.68 MemberStateCertificate (сертификат государства-члена).....	136
2.69 MemberStatePublicKey (открытый ключ государства-члена).....	136
2.70 Name (название).....	137
2.71 NationAlpha (буквенный код страны).....	137
2.72 NationNumeric (числовой код страны)	139
2.73 NoOfCalibrationRecords (число записей калибровки)	141
2.74 NoOfCalibrationsSinceDownload (число калибровок после загрузки)	141
2.75 NoOfCardPlaceRecords (число записей, касающихся мест, на карточке)	141
2.76 NoOfCardVehicleRecords (число записей, касающихся транспортных средств, на карточке).....	141
2.77 NoOfCompanyActivityRecords (число записей, касающихся операций предприятия).....	142
2.78 NoOfControlActivityRecords (число записей, касающихся проверочных операций).....	142
2.79 NoOfEventsPerType (число событий по типу)	142
2.80 NoOfFaultsPerType (число неисправностей по типу).....	142
2.81 OdometerValueMidnight (показания счетчика пробега в полночь).....	143
2.82 OdometerShort (показания счетчика)	143
2.83 OverspeedNumber (число превышений скорости)	143
2.84 PlaceRecord (запись, касающаяся места).....	143
2.85 PreviousVehicleInfo (информация о предыдущем транспортном средстве) ..	144
2.86 PublicKey (открытый ключ).....	144
2.87 RegionAlpha (буквенный код региона)	145
2.88 RegionNumeric (числовой код района)	145
2.89 RSAKeyModulus (модуль ключа RSA)	146
2.90 RSAKeyPrivateExponent (закрытая экспонента ключа RSA)	146
2.91 RSAKeyPublicExponent (открытая экспонента ключа RSA)	147
2.92 SensorApprovalNumber (номер официального утверждения датчика)	147
2.93 SensorIdentification (идентификация датчика)	147
2.94 SensorInstallation (установка датчика)	148
2.95 SensorInstallationSecData (данные о защите датчика)	148
2.96 SensorOSIdentifier (идентификатор датчика ОС)	149
2.97 SensorPaired (подсоединенный датчик)	149
2.98 SensorPairingDate (дата подсоединения датчика)	149
2.99 SensorSerialNumber (серийный номер датчика)	150
2.100 SensorSCIdentifier (идентификатор защиты датчика)	150
2.101 Signature (подпись)	150
2.102 SimilarEventsNumber (число аналогичных событий)	150

СОДЕРЖАНИЕ (продолжение)

	Стр.
2.103 SpecificConditionType (тип особой ситуации)	150
2.104 SpecificConditionRecord (запись особой ситуации)	151
2.105 Speed (скорость)	151
2.106 SpeedAuthorised (разрешенная скорость)	151
2.107 SpeedAverage (средняя скорость)	152
2.108 SpeedMax (максимальная скорость)	152
2.109 TDesSessionKey (ключ сеанса)	152
2.110 TimeReal (реальное время)	152
2.111 TyreSize (размер шин)	152
2.112 VehicleIdentificationNumber (идентификационный номер транспортного средства)	153
2.113 VehicleRegistrationIdentification (идентификация регистрации транспортного средства)	153
2.114 VehicleRegistrationNumber (номер регистрации транспортного средства)	153
2.115 VuActivityDailyData (данные об изменении деятельности в БУ)	154
2.116 VuApprovalNumber (номер официального утверждения БУ)	154
2.117 VuCalibrationData (дата калибровки БУ)	155
2.118 VuCalibrationRecord (запись калибровки БУ)	155
2.119 VuCardIWData (данные о вводе и извлечении карточки)	157
2.120 VuCardIWRecord (запись данных о вводе и извлечении карточки)	157
2.121 VuCertificate (сертификат БУ)	158
2.122 VuCompanyLocksData (дата блокировки БУ предприятием)	158
2.123 VuCompanyLocksRecord (запись блокировки БУ предприятием)	159
2.124 VuControlActivityData (дата операций по проверке БУ)	159
2.125 VuControlActivityRecord (запись операций по проверке БУ)	160
2.126 VuDataBlockCounter (счетчик блока данных БУ)	161
2.127 VuDetailedSpeedBlock (блок данных о скорости в БУ)	161
2.128 VuDetailedSpeedData (данные о скорости в БУ)	161
2.129 VuDownloadablePeriod (период загрузки данных в БУ)	162
2.130 VuDownloadActivityData (информация о загрузке данных в БУ)	162
2.131 VuEventData (данные о событиях в БУ)	163
2.132 VuEventRecord (записи событий в БУ)	163
2.133 VuFaultData (данные о неисправностях в БУ)	164
2.134 VuFaultRecord (записи о неисправностях в БУ)	164
2.135 VuIdentification (идентификация БУ)	165
2.136 VuManufacturerAddress (адрес изготовителя БУ)	166
2.137 VuManufacturerName (название изготовителя БУ)	166
2.138 VuManufacturingDate (дата изготовления БУ)	166
2.139 VuOverSpeedingControlData (данные о контроле за превышением скорости в БУ)	167
2.140 VuOverSpeedingEventData (данные о случаях превышения скорости в БУ)	167
2.141 VuOverSpeedingEventRecord (записи случаев превышения скорости в БУ)	168
2.142 VuPartNumber (номер детали БУ)	168

СОДЕРЖАНИЕ (продолжение)

	Стр.
2.143 VuPlaceDailyWorkPeriodData (данные о месте/ежедневном периоде работы в БУ)	169
2.144 VuPlaceDailyWorkPeriodRecord (записи о месте/ежедневном периоде работы в БУ)	169
2.145 VuPrivateKey (закрытый ключ БУ)	169
2.146 VuPublicKey (открытый ключ БУ)	170
2.147 VuSerialNumber (серийный номер БУ)	170
2.148 VuSoftInstallationDate (дата установки программы БУ)	170
2.149 VuSoftwareIdentification (идентификация программы БУ)	170
2.150 VuSoftwareVersion (версия программы БУ)	171
2.151 VuSpecificConditionData (данные об особых ситуациях в БУ)	171
2.152 VuTimeAdjustmentData (данные о корректировке времени в БУ)	171
2.153 VuTimeAdjustmentRecord (записи корректировки времени в БУ)	172
2.154 W-VehicleCharacteristicConstant (характеристическая постоянная W транспортного средства)	172
2.155 WorkshopCardApplicationIdentification (идентификация приложения карточки мастерской)	172
2.156 WorkshopCardCalibrationData (данные о калибровке на карточке мастерской)	173
2.157 WorkshopCardCalibrationRecord (записи калибровки на карточке мастерской)	174
2.158 WorkshopCardHolderIdentification (идентификация держателя карточки мастерской)	175
2.159 WorkshopCardPIN (PIN-код карточки мастерской)	176
3. Определения диапазонов значений и размеров	176
3.1 Определения для карточки водителя	176
3.2 Определения для карточки мастерской	177
3.3 Определения для карточки контролера	177
3.4 Определения для карточки предприятия	177
4. Наборы знаков	177
5. Кодирование	178

I. Введение

В настоящем подразделе уточняются форматы данных, элементы данных и структуры данных, подлежащие использованию в контрольных устройствах и карточках тахографа.

1.1 Метод определения типов данных

Для определения типов данных в настоящем подразделе используется абстрактное описание синтаксиса версии 1 (ASN.1). Он 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,
- в том случае, если какой-либо тип данных состоит из других типов данных, то 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 к названию 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 определен в качестве того или иного стандарта и если он подходит для использования в контрольном устройстве, то в этом подразделе будет определен и этот тип ASN.1.

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

1.2 Источники

В настоящем подразделе используются следующие источники:

- | | |
|----------------|---|
| ISO 639 | Код отображения названий языков. Издание первое: 1988 год. |
| EN 726-3 | Системы карточек идентификационных - Телекоммуникационные карточки и терминалы на интегральной схеме (интегральных схемах) - Часть 3: Требования, не зависящие от вида приложения, которым должны удовлетворять карточки. Декабрь 1994 года |
| ISO 3779 | Дорожные транспортные средства - Оповестительный номер транспортного средства (VIN) - Содержание и структура. Издание 3: 1083 год. |
| ISO/IEC 7816-5 | Информационные технологии - Карточки идентификационные - Карточки на интегральной схеме (интегральных схемах) с контактами - Часть 5: Система нумерации и процедура регистрации идентификаторов приложений. Издание первое: 1994 год плюс поправка 1: 1996 год. |
| ISO/IEC 8824-1 | Информационные технологии - Абстрактное описание синтаксиса версии 1 (ASN.1): Спецификация на базовое описание. Издание 2: 1998 год. |
| ISO/IEC 8825-2 | Информационные технологии - Правила кодирования ASN.1: Спецификация на правила кодирования в сжатом формате (PER). Издание 2: 1998 год. |
| ISO/IEC 8859-1 | Информационные технологии - 8-битовые однобайтовые наборы закодированных графических знаков - часть 1: Латинский алфавит № 1. Издание первое: 1998 год. |
| ISO/IEC 8859-7 | Информационные технологии - 8-битовые однобайтовые наборы закодированных графических знаков - часть 7: Латинский/греческий алфавит. Издание первое: 1987 год. |
| ISO 16844-3 | Дорожные транспортные средства - Системы тахографа - Интерфейс датчика движения. WD 3-20/05/99. |

2. Определения типов данных

В случае любого из следующих типов данных значение по умолчанию содержания "unknown" ("нет данных") или "not applicable" ("не применимо") определяется посредством заполнения соответствующего элемента данных с помощью байтов 'FF'.

2.1 ActivityChangeInfo (данные об изменении вида деятельности)

Этот тип данных позволяет кодировать с помощью слова из двух байтов состояние считывающего устройства в 00:00 часов и статус водителя в 00:00 часов и/или изменения вида деятельности и/или изменения статуса управления и/или изменения положения карточки водителя или второго водителя. Этот тип данных относится к требованиям 084, 109a, 199 и 219.

ActivityChangeInfo ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (2))

Присвоение значения - выровненный байт: 'sраatttttttt'В (16 бит)

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

- 's'В Считывающее устройство:
 - '0'В: DRIVER (ВОДИТЕЛЬ),
 - '1'В: CO-DRIVER (ВТОРОЙ ВОДИТЕЛЬ),

- 'с'В Статус управления:
 - '0'В: SINGLE (ОДИН),
 - '1'В: CREW (ЭКИПАЖ),

- 'р'В Положение карточки водителя (или мастерской) в соответствующем считывающем устройстве:
 - '0'В: INSERTED, карточка вставлена,
 - '1'В: NOT INSERTED, карточка не вставлена (или карточка извлечена),

- 'aa'В Вид деятельности:
 - '00'В: BREAK/REST (ПЕРЕРЫВ/ОТДЫХ),
 - '01'В: AVAILABILITY (ГОТОВНОСТЬ),
 - '10'В: WORK (РАБОТА),
 - '11'В: DRIVING (УПРАВЛЕНИЕ),

‘ttttttttt’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 (не применимо, если ‘p’ = 1, за исключением случая, указанного ниже):
‘0’В: DRIVER (ВОДИТЕЛЬ),
‘1’В: CO-DRIVER (ВТОРОЙ ВОДИТЕЛЬ),
- ‘c’В Статус управления (случай ‘p’ = 0) или Следующий вид деятельности (случай ‘p’ = 1):
‘0’В: SINGLE (ОДИН), ‘0’В: UNKNOWN (НЕТ ДАННЫХ)
‘1’В: CREW (ЭКИПАЖ), ‘1’В: KNOWN (ЕСТЬ ДАННЫЕ)
(= введено вручную)
- ‘p’В Положение карточки:
‘0’В: INSERTED, карточка вставлена в контрольное устройство,
‘1’В: NOT INSERTED, карточка не вставлена (или карточка извлечена),
- ‘aa’В Вид деятельности (неприменимо, если ‘p’=1 и ‘c’=0, за исключением случая, указанного ниже):
‘00’В: ПЕРЕРЫВ/ОТДЫХ,
‘01’В: ГОТОВНОСТЬ,
‘10’В: РАБОТА,
‘11’В: УПРАВЛЕНИЕ,
- ‘ttttttttt’В Время изменения: число минут, начиная с 00:00 часов на данный день.

Примечание в случае ‘извлечения карточки’:

Когда карточка извлечена:

- ‘s’ этот знак применим и указывает на считывающее устройство, из которого извлечена карточка,
- ‘c’ должно быть установлено на 0,
- ‘p’ должно быть установлено на 1,

- 'aa' должно кодировать текущий вид деятельности, выбранный в указанное время.

В результате ручного ввода биты 'с' и 'aa' в составе слова (хранящееся в памяти карточки) позднее могут быть стерты и на их место записаны другие данные, отражающие факт этого ввода.

2.2. Address (адрес)

Адрес.

```
Address ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    codePage                ЦЕЛОЕ ЧИСЛО (0..255),  
    address                  ОКТЕТНАЯ СТРОКА (РАЗМЕР (35))  
}
```

codePage указывает на часть стандарта ISO/IEC 8859, используемую для кодирования адреса,

address - закодированный адрес в соответствии с ISO/IEC 8859.

2.3 BCDString (строка BCD)

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 (тип строки знаков).

```
BCDString ::= ЗНАКОВАЯ СТРОКА (С КОМПОНЕНТАМИ {  
    идентификация (С КОМПОНЕНТАМИ {  
        устанавливает ПРИСУТСТВИЕ }) })
```

BCDString использует для описания строки нотацию 'hstring'. Крайняя левая шестнадцатиричная цифра представляет собой самый значимый полубайт первого байта. Для получения нескольких октетов после крайнего левого полуоктета первого октета включается соответствующее число нулевых полуоктетов.

Допустимые цифры: 0, 1, .. 9.

2.4 CalibrationPurpose (цель калибровки)

Данный код указывает причину регистрации набора параметров калибровки. Этот тип данных относится к требованиям 097 и 098.

CalibrationPurpose ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))

Присвоение значения:

'00' Н	зарезервированное значение
'01' Н	активация: регистрация известных параметров калибровки в момент включения БУ
'02' Н	первая установка: первая калибровка БУ после его активации
'03' Н	установка: первая калибровка БУ на данном транспортном средстве
'04' Н	периодическая инспекция.

2.5 CardActivityDailyRecord (запись вида деятельности на карточке)

Информация, которая хранится на карточке, относится к деятельности водителя за конкретный календарный день. Этот тип данных относится к требованиям 199 и 219.

```
CardActivityDailyRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
    activityPreviousRecordLength      ЦЕЛОЕ ЧИСЛО (0..CardActivityLengthRange),
    activityRecordLength              ЦЕЛОЕ ЧИСЛО (0..CardActivityLengthRange),
    activityRecordDate                Реальное время,
    activityDailyPresenceCounter      Счетчик ежедневного присутствия,
    activityDayDistance               Расстояние,
    activityChangeInfo                УСТАНОВЛЕННЫЙ РАЗМЕР (1..1440)
                                     ЭЛЕМЕНТА ДАННЫХ ActivityChangeInfo
}
```

activityPreviousRecordLength - общая длина предыдущей ежедневной записи в байтах. Максимальное значение определяется в виде длины ОКТЕТНОЙ СТРОКИ, содержащей эти записи (см. пункт 3: CardActivityLengthRange). Когда эта запись становится самой старой ежедневной записью, значение activityPreviousRecordLength должно устанавливаться на ноль.

activityRecordLength - общая длина данной записи в байтах. Максимальное значение определяется длиной ОКТЕТНОЙ СТРОКИ, содержащей эти записи.

activityRecordDate - дата записи.

activityDailyPresenceCounter - счетчик ежедневного наличия карточки на данный день.

activityDayDistance - общее расстояние, пройденное за данный день.

activityChangeInfo - набор данных типа 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.

2.6 CardActivityLengthRange (длина записи о деятельности на карточке)

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

CardActivityLengthRange ::= ЦЕЛОЕ ЧИСЛО (0..2¹⁶-1)

Присвоение значения: см. пункт 3.

2.7 CardApprovalNumber (номер официального утверждения карточки)

Эта позиция определяет номер официального утверждения типа карточки.

Card Approval Number:: = Строка IA5 (РАЗМЕР(8))

Присвоение значения: Не определено.

2.8 CardCertificate (сертификат карточки)

Сертификат открытого ключа карточки.

CardCertificate: = Сертификат

2.9 CardChipIdentification (идентификация микропроцессора карточки)

Информация, записанная на карточке, которая относится к идентификации интегральной схемы карточки (ИС) (требование 191).

```
CardChipIdentification: = ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    icSerialNumber          ОКТЕТНАЯ СТРОКА (РАЗМЕР (4)),  
    icManufacturingReferences ОКТЕТНАЯ СТРОКА (РАЗМЕР (4))  
}
```

icSerialNumber - серийный номер ИС, определенный в стандарте EN 726-3.

icManufacturingReferences - идентификатор изготовителя ИС и производственные данные, определенные в стандарте EN 726-3.

2.10 CardConsecutiveIndex (порядковый индекс карточки)

Порядковый индекс карточки (определение h)).

CardConsecutiveIndex: = строка IA5 (РАЗМЕР (1))

Присвоение значения: (см. главу VII настоящего добавления)

Порядок увеличения: '0 , ... , 9, A , ... , Z , a , ... , z'

2.11 CardControlActivityDataRecord (запись данных о проверочных операциях)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к последней проверке, которой подвергнулся водитель (требования 210 и 225).

```
CardControlActivityDataRecord: = ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    controlType          тип проверки,  
    controlTime          реальное время,  
    controlCardNumber    полный номер карточки,  
    controlVehicleRegistration идентификация регистрации транспортного средства,  
    controlDownloadPeriodBegin реальное время,  
    controlDownloadPeriodEnd реальное время  
}
```


activityPointerOldestDayRecord - указание на начало блока памяти (число байтов с начала строки) для хранения самой старой ежедневной записи в строке activityDailyRecords. Максимальное значение определяется длиной строки.

activityPointerNewestRecord - указание на начало блока памяти (число байтов с начала строки) для хранения самой последней ежедневной записи в строке activityDailyRecords. Максимальное значение определяется длиной строки.

activityDailyRecords - место, имеющееся для хранения данных о деятельности водителя (структура данных: CardActivityDailyRecord) за каждый календарный день, в течение которого использовалась карточка.

Присвоение значения: данная октетная строка периодически заполняется записями типа CardActivityDailyRecord. При первом использовании хранение данных производится с начала первого байта строки. Все новые записи включаются в конце предыдущей. Когда вся строка заполняется, процесс хранения продолжается с первого байта строки, независимо от наличия разрыва в том или ином элементе данных. До включения в строку данных о новом виде деятельности (посредством расширения текущей позиции activityDailyRecord или включения новой позиции activityDailyRecord), которые записываются вместо прежних данных о деятельности; указатель activityPointerOldestDayRecord должен быть обновлен с целью отразить новое место хранения самой старой полной ежедневной записи, а указатель activityPreviousRecordLength этой (новой) самой старой полной ежедневной записи должен быть установлен на ноль.

2.14 CardDrivingLicenceInformation (информация о водительском удостоверении)

Информация, записанная на карточке водителя, которая относится к данным о водительском удостоверении держателя карточки (требование 196).

```
CardDrivingLicenceInformation ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    drivingLicenceIssuingAuthority           название,  
    drivingLicenceIssuingNation             числовой код страны,  
    drivingLicenceNumber                    строка IA5 (РАЗМЕР (16))  
}
```

drivingLicenceIssuingAuthority - орган, ответственный за выдачу водительского удостоверения.

drivingLicenceIssuingNation - национальная принадлежность органа, выдавшего водительское удостоверение.

drivingLicenceNumber - номер водительского удостоверения.

2.15 CardEventData (данные о событиях)

Информация, записанная на карточке водителя или мастерской, которая относится к событиям, связанным с держателем карточки (требования 204 и 223).

```
CardEventData ::= РАЗМЕР ПОСЛЕДОВАТЕЛЬНОСТИ(6) {  
    cardEventRecords          УСТАНОВЛЕННЫЙ РАЗМЕР(NoOfEventsPerType)  
                                ЗАПИСИ CardEventRecord  
}
```

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

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

2.16 CardEventRecord (запись о событиях)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к данному событию, связанному с держателем карточки (требования 205 и 223).

```
CardEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    eventType                 тип события/неисправности,  
    eventBeginTime           реальное время,  
    eventEndTime             реальное время,  
    eventVehicleRegistration идентификация регистрации транспортного средства  
}
```

eventType - тип события.

eventBeginTime - дата и время начала события.

eventEndTime - дата и время завершения события.

eventVehicleRegistration - регистрационный номер транспортного средства (VRN) и название Договаривающейся стороны регистрации транспортного средства, в которой произошло данное событие.

2.17 CardFaultData (данные о сбоях в работе карточки)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к сбоям в работе, связанным с держателем карточки (требования 207 и 223).

```
CardFaultData ::= РАЗМЕР ПОСЛЕДОВАТЕЛЬНОСТИ(2) {  
    cardFaultRecords                УСТАНОВЛЕННЫЙ РАЗМЕР  
                                     (NoOfFaultsPerType) ЗАПИСИ CardFaultRecord  
}
```

CardFaultData - последовательность совокупности записей, отражающих неисправности контрольного устройства, за которой следует совокупность записей, отражающих сбой в работе карточек.

cardFaultRecords - совокупность записей о неисправностях, сгруппированных по данной категории неисправностей (контрольного устройства или карточки).

2.18 CardFaultRecord (запись о сбоях в работе карточки)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к сбою в работе, связанному с держателем карточки (требования 208 и 223).

```
CardFaultRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    faultType                тип события/сбоя в работе,  
    faultBeginTime           реальное время,  
    faultEndTime             реальное время,  
    VehicleRegistration       идентификация регистрации транспортного средства  
}
```

faultType - тип сбоя в работе.

faultBeginTime - дата и время начала сбоя в работе.

faultEndTime - дата и время конца сбоя в работе.

faultVehicleRegistration - VRN и название Договаривающейся стороны регистрации транспортного средства, в которой имел место сбой в работе.

2.19 CardIccIdentification (идентификация ИС карточки)

Информация, записанная на карточке, которая относится к идентификации интегральной схемы (ИС) карточки (требование 192).

```
CardIccIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    clockStop                ОКТЕТНАЯ СТРОКА (РАЗМЕР(1)),  
    CardApprovalNumber      расширенный номер серии,  
    cardApprovalNumber      номер официального утверждения карточки,  
    cardPersonaliserID      ОКТЕТНАЯ СТРОКА (РАЗМЕР(1)),  
    embedderIcAssemblerId   ОКТЕТНАЯ СТРОКА (РАЗМЕР(5)),  
    icIdentifier             ОКТЕТНАЯ СТРОКА (РАЗМЕР(2))  
}
```

clockStop - режим остановки часов, определенных в стандарте EN 726-3.

cardExtendedSerialNumber - серийный номер карточки на интегральной схеме и исходный заводской номер карточки на интегральной схеме, определенный в стандарте EN 726-3 и более точно определяемый типом данных ExtendedSerialNumber.

cardApprovalNumber - номер официального утверждения типа карточки.

cardPersonaliserID - идентификатор учреждения, персонализирующего карточку, определенный в стандарте EN 726-3.

embedderIcAssemblerId - идентификатор монтажного/сборочного предприятия, определенный в стандарте EN 726-3.

icIdentifier - идентификатор ИС карточки и изготовитель ИС, определенный в стандарте EN 726-3.

2.20 CardIdentification (идентификация карточки)

Информация, записанная на карточке, которая имеет отношение к идентификации карточки (требования 194, 215, 231, 235).

```
CardIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    CardIssuingMemberState    числовой код страны,  
    cardNumber                 номер карточки,  
    cardIssuingAuthorityName   название,  
    cardIssueDate              реальное время,  
    cardValidityBegin          реальное время,  
    cardExpiryDate             реальное время  
}
```

cardIssuingMemberState - код Договаривающейся стороны, выдавшей карточку.

cardNumber - номер карточки.

cardIssuingAuthorityName - название органа, выдавшего карточку.

cardIssueDate - дата выдачи карточки нынешнему держателю.

cardValidityBegin - первая дата действия карточки.

cardExpiryDate - дата истечения срока действия карточки.

2.21 CardNumber (номер карточки)

Номер карточки, содержащийся в определении (g).

```
CardNumber ::= ВЫБОР {  
    ПОСЛЕДОВАТЕЛЬНОСТЬ {  
        driverIdentification    строка IA5 (РАЗМЕР (14)),  
        cardReplacementIndex    индекс замены карточки  
        cardRenewalIndex         индекс обновления карточки  
    },  
  
    ПОСЛЕДОВАТЕЛЬНОСТЬ {  
        ownerIdentification     строка IA5 (РАЗМЕР (13)),  
        cardConsecutiveIndex     порядковый индекс карточки,  
        cardReplacementIndex     индекс замены карточки,  
        cardRenewalIndex         индекс обновления карточки  
    }  
}
```

driverIdentification - индивидуальная идентификация водителя Договаривающейся стороны.

ownerIdentification - индивидуальная идентификация предприятия или мастерской или контрольного органа в соответствующей Договаривающейся стороне.

cardConsecutiveIndex - порядковый индекс карточки.

cardReplacementIndex - индекс замены карточки.

cardRenewalIndex - индекс возобновления карточки.

Первая последовательность этого варианта позволяет кодировать номер карточки водителя, а вторая последовательность позволяет кодировать номера карточки мастерской, контролера и предприятия.

2.22 CardPlaceDailyWorkPeriod (ежедневный период работы и место)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к местам, в которых начинаются и/или заканчиваются ежедневные периоды работы (требования 202 и 221).

```
CardPlaceDailyWorkPeriod ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    placePointerNewestRecord    ЦЕЛОЕ ЧИСЛО (0 .. NoOfCardPlaceRecords-1),  
    placeRecords                УСТАНОВЛЕННЫЙ РАЗМЕР (NoOfCardPlaceRecords)  
                                ЗАПИСИ PlaceRecord  
}
```

placePointerNewestRecord - индекс последней обновленной 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 введенных названиях мест.

2.23 CardPrivateKey (закрытый ключ карточки)

Закрытый ключ карточки.

CardPrivateKey ::= закрытая экспонента ключа RSA

2.24 CardPublicKey (открытый ключ карточки)

Открытый ключ карточки.

CardPublicKey ::= открытый ключ

2.25 CardRenewalIndex (индекс возобновления карточки)

Индекс возобновления карточки (определение i)).

CardRenewalIndex ::= строка IA5 (РАЗМЕР (1))

Присвоение значения: (см. главу VII настоящего добавления).

‘0’ Первая выдача.

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

2.26 CardReplacementIndex (индекс замены карточки)

Индекс замены карточки (определение j)).

CardReplacementIndex ::= IA5Строка (РАЗМЕР (1))

Присвоение значения: (см. главу VII настоящего добавления).

‘0’ первая карточка.

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

2.27 CardSlotNumber (номер считывающего устройства карточки)

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

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

Присвоение значения: дополнительно не уточняется.

2.28 CardSlotsStatus (состояние считывающих устройств карточки)

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

CardSlotsStatus ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (1))

Присвоение значения – Выровненный октет: ‘ccccddd’В

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

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

со следующими идентификационными кодами:

‘0000’В карточка не вставлена,

‘0001’В не вставлена карточка водителя,

‘0010’В вставлена карточка мастерской,

‘0011’В вставлена карточка контролера,

‘0100’В вставлена карточка предприятия.

2.29 CardStructureVersion (вариант структуры карточки)

Код, указывающий вариант структуры, использованной на карточке тахографа.

CardStructureVersion ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (2))

Присвоение значения: ‘aabb’Н:

‘aa’Н индекс изменения структуры,

‘00h’ для данной версии

‘bb’H индекс изменений, касающийся использования элементов данных, определенных в структуре, заданной стартовым байтом, ‘00h’ для данного варианта.

2.30 CardVehicleRecord (запись использования транспортного средства)

Информация, записанная на карточке водителя или предприятия, которая имеет отношение к периоду использования транспортного средства в течение соответствующего календарного дня (требования 197 и 217).

```
CardVehicleRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    vehicleOdometerBegin          счетчик пробега,  
    vehicleOdometerEnd           счетчик пробега,  
    vehicleFirstUse              реальное время,  
    vehicleLastUse               реальное время,  
    vehicleRegistration          идентификация регистрации транспортного  
                                средства,  
    vuDataBlockCounter           счетчик массивов данных бортового  
                                устройства  
}
```

vehicleOdometerBegin - показания счетчика пробега транспортного средства на начало периода использования транспортного средства.

vehicleOdometerEnd - показания счетчика пробега транспортного средства на конец периода использования транспортного средства.

vehicleFirstUse - дата и время начала периода использования транспортного средства.

vehicleLastUse - дата и время завершения периода использования транспортного средства.

vehicleRegistration - VRN и Договаривающаяся сторона регистрации транспортного средства.

vuDataBlockCounter - показания счетчика блока данных бортового устройства на момент последнего извлечения данных, касающихся периода использования транспортного средства.

2.31 CardVehiclesUsed (использованное транспортное средство)

Информация, записанная на карточке водителя или мастерской, которая имеет отношение к транспортным средствам, используемым держателем карточки (требования 197 и 217).

```
CardVehiclesUsed := ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    vehiclePointerNewestRecord    ЦЕЛОЕ ЧИСЛО (0..NoOfCardVehicleRecords-1),  
    cardVehicleRecords           УСТАНОВЛЕННЫЙ РАЗМЕР  
                                (NoOfCardVehicleRecords) ЗАПИСИ  
                                CardVehicleRecord  
}
```

vehiclePointerNewestRecord - индекс последней обновленной записи, касающейся транспортного средства.

Присвоение значения: число, соответствующее числовому показателю записи, касающейся транспортного средства, которое начинается с '0' в случае первой регистрации записей, касающихся транспортного средства, в данной структуре.

cardVehicleRecords - совокупность записей, содержащих информацию об использованных транспортных средствах.

2.32 Certificate (сертификат)

Сертификат открытого ключа, выданный сертификационным органом.

```
Certificate ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (194))
```

Присвоение значения: цифровая подпись с частичным восстановлением содержания сертификата в соответствии с подразделом 11 (общие механизмы защиты): подпись (128 байтов) || оставшая часть открытого ключа (58 байтов) || исходные данные сертификационного органа (8 байтов).

2.33 CertificateContent (содержание сертификата)

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

```
CertificateContent ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    certificateProfileIdentifier          ЦЕЛОЕ ЧИСЛО (0..255),  
    certificationAuthorityReference      Идентификатор ключа,  
    certificateHolderAuthorisation      Разрешение владельца сертификата,  
    certificateEndOfValidity            Реальное время,  
    certificateHolderReference          Идентификатор ключа,  
    publicKey                           Открытый ключ  
}
```

certificateProfileIdentifier - версия соответствующего сертификата.

Присвоение значения: '01h' для данного варианта.

certificationAuthorityReference - идентификатор сертификационного органа, выдавшего сертификат. Он также включает ссылку на открытый ключ данного сертификационного органа.

certificateHolderAuthorisation - идентификатор прав держателя сертификата.

certificateEndOfValidity - дата, когда истекает срок административного действия сертификата.

certificateHolderReference - идентификатор держателя сертификата. Он также включает ссылку на его открытый ключ.

publicKey - открытый ключ, подтверждающий данный сертификат.

2.34 CertificateHolderAuthorisation (разрешение держателя сертификата)

Идентификация прав держателя сертификата.

```
CertificateHolderAuthorisation ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    tachographApplicationID            ОКТЕТНАЯ СТРОКА (РАЗМЕР (6) )  
    equipmentType                      Тип оборудования  
}
```

tachographApplicationID - идентификатор приложения для прикладной программы тахографа.

Присвоение значения: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Этот идентификатор является фирменным незарегистрированным идентификатором приложения в соответствии со стандартом ISO/IEC 7816-5.

equipmentType - идентификация типа оборудования, для которого предназначен этот сертификат.

Присвоение значения: в соответствии с типом данных EquipmentType . **0**, если сертификат выдан какой-либо Договаривающейся стороной.

2.35 CertificateRequestID (запрос на идентификацию сертификата)

Индивидуальная идентификация запроса сертификата. Она также может использоваться в качестве идентификатора открытого ключа бортового устройства, если серийный номер бортового устройства, для которого предназначен данный ключ, в момент создания сертификата не был известен.

```
CertificateRequestID ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    requestSerialNumber          ЦЕЛОЕ ЧИСЛО (0..232-1)  
    requestMonthYear            VCDString(РАЗМЕР (2))  
    crIdentifier                 ОКТЕТНАЯ СТРОКА (РАЗМЕР (1))  
    manufacturerCode           Код изготовителя  
}
```

requestSerialNumber - порядковый номер запроса на сертификат, индивидуальный для данного изготовителя и относящийся к месяцу, указанному ниже.

requestMonthYear - идентификация месяца и года запроса на сертификат.

Присвоение значения: Код VCD месяца (две цифры) и года (две последние цифры).

crIdentifier: идентификатор, позволяющий проводить различие между запросом на сертификат и расширенным порядковым номером.

Присвоение значения: 'FFh'.

Код завода-изготовителя: цифровой код изготовителя, запрашивающего сертификат.

2.36 CertificationAuthorityKID (Сертификационный орган KID)

Идентификатор открытого ключа Сертификационного органа (Договаривающейся стороны или Европейского сертификационного органа)

```
CertificationAuthorityKID ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    nationNumeric              Числовой код страны  
    nationAlpha               Буквенный код страны  
    keySerialNumber          ЦЕЛОЕ ЧИСЛО (0..255)  
    additionalInfo           ОКТЕТНАЯ СТРОКА (РАЗМЕР (2))  
    caIdentifier              ОКТЕТНАЯ СТРОКА (РАЗМЕР (1))  
}
```

nationNumeric - числовой код страны сертификационного органа.

nationAlpha - буквенно-числовой код страны сертификационного органа.

keySerialNumber - порядковый номер, позволяющий проводить различие между различными ключами сертификационного органа в случае изменения ключей.

additionalInfo - двухбайтовое поле для дополнительного кодирования (специфичное для сертификационного органа).

caIdentifier - идентификатор, позволяющий проводить различие между идентификатор ключа сертификационного органа и другими идентификаторами ключа.

Присвоение значения: '01h'.

2.37 CompanyActivityData (данные об операциях с карточкой предприятия)

Информация, записанная на карточке предприятия, которая имеет отношение к операциям, произведенным с карточкой (требование 237).

```
CompanyActivityData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
  companyPointerNewestRecord ЦЕЛОЕ ЧИСЛО (0..NoOfCompanyActivityRecords-1),  
  companyActivityRecords    УСТАНОВЛЕННЫЙ РАЗМЕР  
                             (NoOfCompanyActivityRecords)  
                             ПОСЛЕДОВАТЕЛЬНОСТИ {  
   companyActivityRecord    тип операций с карточкой предприятия  
   companyActivityType      реальное время,  
   companyActivityTime      полный номер карточки,  
   cardNumberInformation    идентификация регистрации транспортного  
   vehicleRegistrationInformation средства,  
   downloadPeriodBegin     реальное время,  
   downloadPeriodEnd       реальное время  
 }  
}
```

companyPointerNewestRecord - индекс последней обновленной записи операции с карточкой предприятия.

Присвоение значения: число, соответствующее числовому идентификатору записи операций с карточкой предприятия, начинающееся с '0' в случае первой записи операции, произведенной предприятием в данной структуре.

companyActivityRecords - совокупность всех записей операций, произведенных предприятием.

companyActivityRecord - последовательность информации, относящейся к одной операции, произведенной предприятием.

companyActivityType - тип операции, произведенной предприятием.

companyActivityTime - дата и время операции, произведенной предприятием.

cardNumberInformation - номер карточки и, в соответствующих случаях, название Договаривающейся стороны, выдавшей карточку с загруженными с нее данными.

vehicleRegistrationInformation - VRN и страна регистрации транспортного средства, с которого были загружены данные или на которое была поставлена или снята блокировка.

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

2.38 CompanyActivityType (тип операции, произведенной предприятием)

Код указывающей операции, произведенной предприятием с использованием карточки предприятия.

```
CompanyActivityType:= ЦЕЛОЕ ЧИСЛО {
    загрузка данных с карточки          (1),
    загрузка с БУ                        (2),
    блокировка БУ                        (3),
    снятие блокировки с БУ              (4)
}
```

2.39 CompanyCardApplicationIdentification (идентификация приложения карточки предприятия)

Информация, записанная на карточке предприятия, которая имеет отношение к идентификации приложения карточки (требование 190).

```
CompanyCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
    typeOfTachographCardId             тип оборудования,
    cardStructureVersion                 вариант структуры карточки,
    noOfCompanyActivityRecords           число записей операций, произведенных
                                         компанией
}
```

typeOfTachographCardId - элемент данных, указывающий на применяемый тип карточки.

cardStructureVersion - элемент данных, указывающий на версию структуры, которая используется в карточке.

noOfCompanyActivityRecords - число записей операций, произведенных предприятием, которые могут храниться на карточке.

2.40 **CompanyCardHolderIdentification** (идентификация держателя карточки предприятия)

Информация, записанная на карточке предприятия, которая относится к идентификации держателя карточки (требование 236).

```
CompanyCardHolderIdentification ::=      ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    companyName                          название,  
    companyAddress                       адрес,  
    cardHolderPreferredLanguage          язык  
}
```

companyName - название предприятия-держателя.

companyAddress - адрес предприятия-держателя а.

cardHolderPreferredLanguage - предпочитаемый язык держателя карточки.

2.41 **ControlCardApplicationIdentification** (идентификация приложения карточки контролера)

Информация, записанная на карточке контролера, которая имеет отношение к идентификации приложения карточки (требование 190).

```
ControlCardApplicationIdentification ::=  ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    typeOfTachographCardId              тип оборудования,  
    cardStructureVersion                 версия структуры карточки,  
    noOfControlActivityRecords           число записей проверочных операций  
}
```

typeOfTachographCardId - элемент данных, указывающий на используемый тип карточки.

cardStructureVersion - элемент данных, указывающий вариант структуры, применяемой на карточке.

noOfControlActivityRecords - число записей проверочных операций, которые могут храниться на карточке.

2.42 ControlCardControlActivityData (данные о проверочных операциях на карточке контролера)

Информация, записанная на карточке контролера, которая имеет отношение к проверочной операции, произведенной с карточкой (требование 233).

```
ControlCardControlActivityData ::=      ПОСЛЕДОВАТЕЛЬНОСТЬ {
  controlPointerNewestRecord            ЦЕЛОЕ ЧИСЛО (0.. NoOfControlActivityRecords-1),
  controlActivityRecords                УСТАНОВЛЕННЫЙ РАЗМЕР
                                        (NoOfControlActivityRecords)
  controlActivityRecord                 ПОСЛЕДОВАТЕЛЬНОСТИ {
  controlType                           тип проверки,
  controlTime                           реальное время,
  controlledCardNumber                  полное время карточки,
  controlledVehicleRegistration          идентификация регистрации транспортного
                                        средства,
  controlDownloadPeriodBegin            реальное время,
  controlDownloadPeriodEnd              реальное время
  }
}
```

controlPointerNewestRecord - индекс последней обновленной записи проверочной операции.

Присвоение значения: число, соответствующее числовому показателю записи проверочной операции, которая начинается с '0' в случае первой записи проверочной операции в данной структуре.

controlActivityRecords - совокупность всех записей проверочных операций.

controlActivityRecord - последовательность информации, связанной с одной проверкой.

controlType - тип проверки.

controlTime - дата и время проверки.

controlledCardNumber - номер карточки и название Договаривающейся Стороны, выдавшей карточку, которая подвергалась проверке.

controlledVehicleRegistration - VRN и название Договаривающейся Стороны регистрации транспортного средства, в которой производилась проверка.

controlDownloadPeriodBegin и **controlDownloadPeriodEnd** - период, за который в соответствующих случаях загружались данные.

2.43 ControlCardHolderIdentification (идентификация держателя карточки контролера)

Информация, записанная на карточке контролера, которая имеет отношение к идентификации держателя карточки (требование 232).

ControlCardHolderIdentification ::=	ПОСЛЕДОВАТЕЛЬНОСТЬ {
controlBodyName	название,
controlBodyAddress	адрес,
cardHolderName	фамилия держателя,
cardHolderPreferredLanguage	язык
}	

controlBodyName - название контрольного органа держателя карточки.

controlBodyAddress - адрес контрольного органа держателя карточки.

cardHolderName - фамилия и имя (имена) держателя контрольной карточки.

cardHolderPreferredLanguage - предпочитаемый язык держателя карточки.

2.44 ControlType (тип проверки)

Код, указывающий на операции, проведенные в ходе проверки. Этот тип данных имеет отношение к требованиям 102, 210 и 225.

ControlType ::= ОКТЕТНАЯ (РАЗМЕР (1))

Присвоение значения - выровненный октет: 'c'В (8 битов)

'с'В загрузка данных с карточки:

'0'В: во время данной проверочной операции загрузка данных с карточки не была произведена,

'1'В: во время данной операции загрузка данных с карточки была произведена.

'v'В загрузка данных с БУ:

'0'В: во время данной проверочной операции загрузка данных с БУ не была произведена,

'1'В: во время данной проверочной операции загрузка данных с БУ была произведена

'р'В вывод на печать:

'0'В: во время данной проверочной операции вывод данных на печать произведен не был,

'1'В: во время данной проверочной операции вывод данных на печать был произведен

'd'В вывод на дисплей:

'0'В: во время данной проверочной операции вывод на дисплей не использовался,

'1'В: во время данной проверочной операции использовался вывод на дисплей

'xxxx'В - не использовался.

2.45 CurrentDateTime (текущая дата/время)

Текущая дата и время, отображаемые на контрольном устройстве.

CurrentDateTime ::= реальное время

Присвоение значения: дополнительно не указывается.

2.46 DailyPresenceCounter (счетчик ежедневного присутствия)

Показания счетчика, записанные на карточке водителя или предприятия, которые увеличиваются на единицу за каждый календарный день, в течение которого в БУ была вставлена карточка. Этот тип данных имеет отношение к требованиям 199 и 219.

DailyPresenceCounter ::= строка BCD (РАЗМЕР(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.

2.47 Datef (формат даты)

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

Datef ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

год	строка BCD (РАЗМЕР(2)),
месяц	строка BCD (РАЗМЕР(1)),
день	строка BCD (РАЗМЕР(1))

}

Присвоение значения:

гггг	год
мм	месяц
дд	день

'00000000'Н четкое указание на отсутствие даты.

2.48 Distance (расстояние)

Пройденное расстояние (результат расчета разницы между двумя показаниями счетчика пробега транспортного средства в километрах).

Distance ::= ЦЕЛОЕ ЧИСЛО ($0..2^{16}-1$)

Присвоение значения: двоичный код без знака. Значение в км в рабочем диапазоне от 0 до 9 999 км.

2.49 **DriverCardApplicationIdentification** (идентификация приложения карточки водителя)

Информация, записанная на карточке водителя, которая имеет отношение к идентификации приложения карточки (требование 190).

```
DriverCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    typeOfTachographCardId      тип оборудования,  
    cardStructureVersion         вариант структуры карточки,  
    noOfEventsPerType           число событий по типу,  
    noOfFaultsPerType           число неисправностей по типу,  
    activityStructureLength      диапазон длины записи вида деятельности  
                                на карточку,  
    noOfCardVehicleRecords      число записей на карточке, относящихся к  
                                транспортному средству,  
    noOfCardPlaceRecords        число записей на карточке, относящихся к месту  
}
```

typeOfTachographCardId - элемент данных, указывающий тип используемой карточки.

cardStructureVersion - элемент данных, указывающий вариант структуры, использованной в 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 - элемент данных, указывающий число байтов, которые могут быть использованы для хранения записей, относящихся к виду деятельности.

noOfCardVehicleRecords - число записей, относящихся к транспортному средству, которое может быть записано на карточку.

noOfCardPlaceRecords - число мест, которое может быть записано на карточку.

2.50 DriverCardHolderIdentification (идентификация держателя карточки водителя)

Информация, записанная на карточке водителя, которая имеет отношение к идентификации держателя карточки (требование 195).

```
DriverCardHolderIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    cardHolderName           фамилия держателя,  
    cardHolderBirthDate      формат даты,  
    cardHolderPreferredLanguage язык  
}
```

cardHolderName - фамилия и имя (имена) держателя карточки водителя.

cardHolderBirthDate - дата рождения держателя карточки водителя.

cardHolderPreferredLanguage - предпочитаемый язык держателя карточки.

2.51 EntryTypeDailyWorkPeriod (тип ввода данных о ежедневных периодах работы)

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

```
EntryTypeDailyWorkPeriod ::= ЦЕЛОЕ ЧИСЛО {  
    начало, относительное время = время ввода карточки или время ввода данных (0),  
    конец, относительное время = время извлечения карточки или время  
    ввода данных (1),  
    начало, относительное время ручного ввода данных (время начала работы) (2),  
    конец, относительное время ручного ввода данных (конец рабочего периода) (3),  
    начало, относительное время, зафиксированное БУ (4),  
    конец, относительное время, зафиксированное БУ (5)  
}
```

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

2.52 EquipmentType (тип оборудования)

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

EquipmentType ::= ЦЕЛОЕ ЧИСЛО (0..255)

-- зарезервировано	(0),
-- карточка водителя	(1),
-- карточка мастерской	(2),
-- карточка контролера	(3),
-- карточка предприятия	(4),
-- карточка завода-изготовителя	(5),
-- бортовое устройство	(6),
-- датчик движения	(7),
-- RFU (зарезервировано для будущего использования)	(8..255)

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

Значение 0 зарезервировано для целей указания Договаривающейся стороны или Европы в поле данных СНА сертификатов.

2.53 EuropeanPublicKey (европейский открытый ключ)

Европейский открытый ключ.

EuropeanPublicKey ::= открытый ключ

2.54 EventFaultType (тип неисправности)

Код, отображающий события или неисправность.

EventFaultType ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (1))

Присвоение значений:

'0x'H	общие события,
'00'H	дополнительно не уточняется,
'01'H	ввод недействительной карточки,
'02'H	несовместимость карточек,

'03'H	несстыковка времени,
'04'H	управление без соответствующей карточки,
'05'H	ввод карточки в процессе управления,
'06'H	последний сеанс использования карточки завершен неправильно,
'07'H	превышение скорости,
'08'H	прекращение электропитания,
'09'H	ошибка данных о движении,
'0A'H to '0F'H	RFU,
'1x'H	события, связанные с попыткой нарушения защиты бортового устройства,
'10'H	дополнительно не уточняется,
'11'H	сбой в аутентификации датчика движения,
'12'H	сбой в аутентификации карточки тахографа,
'13'H	несанкционированная замена датчика движения,
'14'H	ошибка, указывающая на нарушение целостности при вводе данных на карточку
'15'H	ошибка, указывающая на нарушение целостности данных пользователя, записанных в блоке памяти,
'16'H	внутренняя ошибка при передаче данных,
'17'H	несанкционированное вскрытие корпуса,
'18'H	нарушение целостности аппаратного оборудования,
'19'H to '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, указывающая на нарушение целостности сохраненных данных,
'23'H	внутренняя ошибка при передаче данных,
'24'H	несанкционированное вскрытие корпуса,
'25'H	нарушение целостности аппаратного оборудования,
'26'H to '2F'H	RFU,
'3x'H	неисправность контрольного устройства,
'30'H	дополнительно не уточняется,
'31'H	внутренняя неисправность БУ,
'32'H	неисправность принтера,
'33'H	неисправность дисплея,

'34'H	ошибка при загрузке,
'35'H	неисправность датчика,
'36'H to '3F'H	RFU,
'4x'H	сбой в работе карточки,
'40'H	дополнительно не уточняется,
'41'H to '4F'H	RFU,
'50'H to '7F'H	RFU,
'80'H to 'FF'H	по усмотрению изготовителя.

2.55 EventFaultRecordPurpose (цель регистрации события или неисправности)

Код, указывающий на причину регистрации события или неисправности.

EventFaultRecordPurpose: = ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))

Присвоение значений:

'00'H	одно из 10 самых последних (недавних) событий или неисправностей
'01'H	самое длинное событие, произошедшее в один из последних 10 дней
'02'H	одно из пяти наиболее продолжительных событий, произошедших за последние 365 дней
'03'H	последнее событие за один из последних 10 дней
'04'H	самое серьезное событие за один из последних 10 дней
'05'H	одно из пяти самых серьезных событий, произошедших за последние 365 дней
'06'H	первое событие или первая неисправность, имевшие место после последней калибровки
'07'H	текущее/продолжающееся событие или неисправность
'08'H - '7F'H	RFU
'80'H - 'FF'H	по усмотрению изготовителя

2.56 ExtendedSerialNumber (расширенный номер серии)

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

```
ExtendedSerialNumber: = ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    serialNumber          ЦЕЛОЕ ЧИСЛО (0..232-1)  
    monthYear             строка VCD (РАЗМЕР(2))  
    type                  ОКТЕТНАЯ СТРОКА (РАЗМЕР(1))  
    manufacturerCode      код изготовителя  
}
```

serialNumber - серийный номер оборудования, индивидуальный для данного изготовителя, типа оборудования и месяца, указанного ниже.

monthYear - идентификация месяца и года изготовления (или присвоение порядкового номера).

Присвоение значения: кодирование VCD месяца (две цифры) и года (две последние цифры).

type - идентификатор типа оборудования.

Присвоение значения: по усмотрению изготовителя с зарезервированным значением 'FFh'.

manufacturerCode: числовой код изготовителя оборудования.

2.57 FullCardNumber (полный номер карточки)

Код, полностью идентифицирующий карточку тахографа.

```
FullCardNumber: = ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    cardType              тип оборудования,  
    cardIssuingMemberState  числовой код страны,  
    cardNumber            номер карточки  
}
```

cardType - тип карточки тахографа.

cardIssuingMemberState - код Договаривающейся стороны, выдавшей карточку.

cardNumber - номер карточки.

2.58 HighResOdometer (показания счетчика пробега)

Показания счетчика пробега транспортного средства: общее расстояние, пройденное транспортным средством за период его эксплуатации.

HighResOdometer: = ЦЕЛОЕ ЧИСЛО ($0..2^{32}-1$)

Присвоение значения: двоичный код без знака. Значение с точностью до 1/200 км в рабочем диапазоне от 0 до 21 055 406 км.

2.59 HighResTripDistance (расстояние, пройденное за рейс)

Расстояние, пройденное за весь или часть рейса.

HighResTripDistance: = ЦЕЛОЕ ЧИСЛО ($0..2^{32}-1$)

Присвоение значения: двоичный код без знака. Значение с точностью до 1/200 км в рабочем диапазоне от 0 до 21 055 406 км.

2.60 HolderName (фамилия держателя)

Фамилия и имя (имена) держателя карточки.

HolderName: = ПОСЛЕДОВАТЕЛЬНОСТЬ {
holderSurname фамилия,
holderFirstNames имя
}

holderSurname - фамилия держателя. Эта фамилия не включает никаких дополнительных указаний.

Присвоение значения: когда карточка не именная, позиция holderSurname содержит ту же информацию, что и companyName (название предприятия), или workshopName (название мастерской) или controlBodyName (название контрольного органа).

holderFirstNames - имя (имена) и инициалы держателя.

2.61 K-ConstantOfRecordingEquipment (постоянная К записывающего оборудования)

Постоянная контрольного устройства (определение m)).

K-ConstantOfRecordingEquipment: = ЦЕЛОЕ ЧИСЛО ($0..2^{16}-1$)

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

2.62 KeyIdentifier (идентификатор ключа)

Индивидуальный идентификатор открытого ключа, используемого для назначения и выбора ключа. Он также определяет держателя ключа.

KeyIdentifier: = ВЫБОР {
 extendedSerialNumber расширенный номер серии,
 certificateRequestID идентификатор запроса на сертификат,
 certificationAuthorityKID сертификационный орган KID
}

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

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

Третий вариант выбора позволяет назначить открытый ключ Договаривающейся стороны.

2.63 L-TyreCircumference (окружность шины L)

Эффективная окружность шин колес (определение u)).

L-TyreCircumference: = ЦЕЛОЕ ЧИСЛО ($0..2^{16}-1$)

Присвоение значения: двоичный код без знака, значение с точностью 1/8 мм в рабочем диапазоне от 0 до 8 031 мм.

2.64 Language (язык)

Код, идентифицирующий язык.

Language: = Строка IA5 (РАЗМЕР (2))

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

2.65 LastCardDownload (последняя дата загрузки с карточки)

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

LastCardDownload: = Реальное время

Присвоение значения: дополнительно не уточняется.

2.66 ManualInputFlag (метка ручного ввода)

Код, позволяющий определить, ввел ли держателя карточки данные о деятельности водителя вручную в момент ввода карточки или нет (требование 081).

ManualInputFlag: = ЦЕЛОЕ ЧИСЛО {
 noEntry (0)
 manualEntries (1)
}

Присвоение значения: дополнительно не уточняется.

2.67 ManufacturerCode (код изготовителя)

Код, идентифицирующий изготовителя¹³.

¹³ Обновленный список кодов, позволяющих идентифицировать заводы-изготовители, размещен на вебсайте Европейского сертификационного органа по адресу:
<http://dtc.jrc.ec.europa.eu/text/cm.html>.

ManufacturerCode: = ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения :

'00'Н	Информации нет
'01'Н	Значение зарезервировано
'02'Н .. '0F'Н	Зарезервировано для будущего использования
'10'Н	АСТИА
'11'Н .. '17'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'А'
'18'Н .. '1F'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'В'
'20'Н .. '27'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'С'
'28'Н .. '2F'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'D'
'30'Н .. '37'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'Е'
'38'Н .. '3F'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'F'
'40'Н	Giesecke & Devrient GmbH
'41'Н	GEM plus
'42'Н .. '47'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'G'
'48'Н .. '4F'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'H'
'50'Н .. '57'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'I'
'58'Н .. '5F'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'J'
'60'Н .. '67'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'K'
'68'Н .. '6F'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'L'
'70'Н .. '77'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'M'
'78'Н .. '7F'Н	Зарезервировано для изготовителей, название которых начинается с буквы 'N'
'80'Н	OSCARD

'81'H .. '87'H	Зарезервировано для изготовителей, название которых начинается с буквы 'O'
'88'H .. '8F'H	Зарезервировано для изготовителей, название которых начинается с буквы 'P'
'90'H .. '97'H	Зарезервировано для изготовителей, название которых начинается с буквы 'Q'
'98'H .. '9F'H	Зарезервировано для изготовителей, название которых начинается с буквы 'R'
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H.. 'A7'H	Зарезервировано для изготовителей, название которых начинается с буквы 'S'
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	Зарезервировано для изготовителей, название которых начинается с буквы 'T'
'B0'H .. 'B7'H	Зарезервировано для изготовителей, название которых начинается с буквы 'U'
'B8'H .. 'BF'H	Зарезервировано для изготовителей, название которых начинается с буквы 'V'
'C0'H .. 'C7'H	Зарезервировано для изготовителей, название которых начинается с буквы 'W'
'C8'H .. 'CF'H	Зарезервировано для изготовителей, название которых начинается с буквы 'X'
'D0'H .. 'D7'H	Зарезервировано для заводов-изготовителей, название которых начинается с буквы 'Y'
'D8'H .. 'DF'H	Зарезервировано для изготовителей, название которых начинается с буквы 'Z'

2.68 MemberStateCertificate (сертификат государства-члена)

Сертификат открытого ключа Договаривающейся стороны, выданный Европейским сертификационным органом.

MemberStateCertificate: = Сертификат

2.69 MemberStatePublicKey (открытый ключ государства-члена)

Открытый ключ Договаривающейся стороны.

MemberStatePublicKey: = Открытый ключ

2.70 Name (название)

Название.

Название := ПОСЛЕДОВАТЕЛЬНОСТЬ {
codePage ЦЕЛОЕ ЧИСЛО (0..255),
name ОКТЕТНАЯ СТРОКА (РАЗМЕР(35))
}

codePage - элемент данных, указывающий на раздел стандарта ISO/IEC 8859, использованный для кодирования названия,

name - название, закодированное в соответствии со стандартом ISO/IEC 8859-codePage.

2.71 NationAlpha (буквенный код страны)

Буквенное обозначение страны в соответствии с обычным принципом кодирования стран (отличительные знаки), которое наносится на заднюю часть транспортных средств (либо отдельно от номерного знака, либо включенного в номерной знак) и/или упомянутое в зеленых карточках, выдаваемых страховыми компаниями.

NationAlpha ::= строка IA5 (РАЗМЕР(3))

Присвоение значения:

' '	Информации нет,
'A'	Австрия,
'AL'	Албания,
'AND'	Андорра,
'ARM'	Армения,
'AZ'	Азербайджан,
'B'	Бельгия,
'BG'	Болгария,
'BH'	Босния и Герцеговина,
'BY'	Беларусь,

'CH'	Швейцария,
'CY'	Кипр,
'CZ'	Чешская Республика,
'D'	Германия,
'DK'	Дания,
'E'	Испания,
'EST'	Эстония,
'F'	Франция,
'FIN'	Финляндия,
'FL'	Лихтенштейн,
'FR'	Фарерские Острова
'UK'	Соединенное Королевство, Олдерни, Гернси, Джерси, Остров Мэн, Гибралтар,
'GE'	Грузия,
'GR'	Греция,
'H'	Венгрия,
'HR'	Хорватия,
'I'	Италия,
'IRL'	Ирландия,
'IS'	Исландия,
'KZ'	Казахстан,
'L'	Люксембург,
'LT'	Литва,
'LV'	Латвия,
'M'	Мальта,
'MC'	Монако,
'MD'	Республика Молдова,
'MK'	Бывшая югославская Республика Македония,
'N'	Норвегия,
'NL'	Нидерланды,
'P'	Португалия,
'PL'	Польша,
'RO'	Румыния,
'RSM'	Сан-Марино,
'RUS'	Российская Федерация,
'S'	Швеция,
'SK'	Словакия,
'SLO'	Словения,
'SRB'	Сербия,

'TM '	Туркменистан
'TR '	Турция,
'UA '	Украина,
'V '	Ватикан,
'UNK'	Нет данных,
'EC '	Европейское сообщество,
'EUR'	Остальная часть Европы,
'WLD'	Остальная часть мира.

2.72 NationNumeric (числовой код страны)

Числовое обозначение страны.

NationNumeric ::= ЦЕЛОЕ ЧИСЛО (0 .. 255)

Присвоение значения:

-- Информации нет	(00)Н,
-- Австрия	(01)Н,
-- Албания	(02)Н,
-- Андорра	(03)Н,
-- Армения	(04)Н,
-- Азербайджан	(05)Н,
-- Бельгия	(06)Н,
-- Болгария	(07)Н,
-- Босния и Герцеговина	(08)Н,
-- Беларусь	(09)Н,
-- Швейцария	(0A)Н,
-- Кипр	(0B)Н,
-- Чешская Республика	(0C)Н,
-- Германия	(0D)Н,
-- Дания	(0E)Н,
-- Испания	(0F)Н,
-- Эстония	(10)Н,
-- Франция	(11)Н,
-- Финляндия	(12)Н,
-- Лихтенштейн	(13)Н,
-- Фарерские Острова	(14)Н,
-- Соединенное Королевство	(15)Н,

-- Грузия	(16)Н,
-- Греция	(17)Н,
-- Венгрия	(18)Н,
-- Хорватия	(19)Н,
-- Италия	(1A)Н,
-- Ирландия	(1B)Н,
-- Исландия	(1C)Н,
-- Казахстан	(1D)Н,
-- Люксембург	(1E)Н,
-- Литва	(1F)Н,
-- Латвия	(20)Н,
-- Мальта	(21)Н,
-- Монако	(22)Н,
-- Республика Молдова	(23)Н,
-- Бывшая югославская Республика Македония	(24)Н,
-- Норвегия	(25)Н,
-- Нидерланды	(26)Н,
-- Португалия	(27)Н,
-- Польша	(28)Н,
-- Румыния	(29)Н,
-- Сан-Марино	(2A)Н,
-- Российская Федерация	(2B)Н,
-- Швеция	(2C)Н,
-- Словакия	(2D)Н,
-- Словения	(2E)Н,
-- Туркменистан	(2F)Н,
-- Турция	(30)Н,
-- Украина	(31)Н,
-- Ватикан	(32)Н,
-- Сербия	(33)Н,
-- RFU (зарезервировано для будущего использования)	(34 .. FC)Н,
-- Европейское сообщество	(FD)Н,
-- Остальная часть Европы	(FE)Н,
-- Остальная часть мира	(FF)Н

2.73 NoOfCalibrationRecords (число записей калибровки)

Число записей калибровки, которое может храниться на карточке.

NoOfCalibrationRecords: = ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения: см. пункт 3.

2.74 NoOfCalibrationsSinceDownload (число калибровок после загрузки)

Счетчик, указывающий число калибровок, произведенных с карточкой мастерской после последней загрузки данных с этой карточки (требование 230).

NoOfCalibrationsSinceDownload ::= ЦЕЛОЕ ЧИСЛО (0..2¹⁶-1),

Присвоение значения: Дополнительно не уточняется.

2.75 NoOfCardPlaceRecords (число записей, касающихся мест, мест на карточке)

Число записей с указанием мест, которое может храниться на карточке водителя или мастерской.

NoOfCardPlaceRecords ::= ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения: см. пункт 3.

2.76 NoOfCardVehicleRecords (число записей, касающихся транспортных средств на карточке)

Число записей с указанием использованных транспортных средств, которое может храниться на карточке водителя или мастерской.

NoOfCardVehicleRecords: = ЦЕЛОЕ ЧИСЛО (0.. 2¹⁶-1)

Присвоение значения: см. пункт 3.

2.77 NoOfCompanyActivityRecords (число записей, касающихся операций предприятия)

Число записей, касающихся операций предприятия, которое может храниться на карточке предприятия.

NoOfCompanyActivityRecords ::= ЦЕЛОЕ ЧИСЛО (0.. $2^{16}-1$)

Присвоение значения: см. пункт 3.

2.78 NoOfControlActivityRecords (число записей, касающихся проверочных операций)

Число, касающихся проверочных операций, которое может храниться на карточке контролера.

NoOfControlActivityRecords ::= ЦЕЛОЕ ЧИСЛО (0.. $2^{16}-1$)

Присвоение значения: см. пункт 3.

2.79 NoOfEventsPerType (число событий по типу)

Число событий по типу события, которое может храниться на карточке.

NoOfEventsPerType ::= ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения: см. пункт 3.

2.80 NoOfFaultsPerType (число неисправностей по типу)

Число неисправностей по типу неисправности, которое может храниться на карточке.

NoOfFaultsPerType ::= ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения: см. пункт 3.

dailyWorkPeriodRegion	числовой код региона,
vehicleOdometerValue	показания счетчика пробега
}	

entryTime - дата и время ввода данных.

entryTypeDailyWorkPeriod - тип ввода.

dailyWorkPeriodCountry - страна въезда.

dailyWorkPeriodRegion - район въезда.

vehicleOdometerValue - показания счетчика пробега в момент ввода данных о месте въезда.

2.85 PreviousVehicleInfo (информация о предыдущем транспортном средстве)

Информация, касающаяся транспортного средства, использованного водителем ранее, в момент ввода его карточки в бортовое устройство (требование 081).

```
PreviousVehicleInfo ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    vehicleRegistrationIdentification    идентификация регистрации транспортного  
                                         средства,  
    cardWithdrawalTime                  реальное время  
}
```

vehicleRegistrationIdentification - VRN и Договаривающаяся сторона регистрации транспортного средства.

cardWithdrawalTime - дата и время извлечения карточки.

2.86 PublicKey (открытый ключ)

Открытый ключ RSA.

```
PublicKey ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    rsaKeyModulus                        модуль ключа RSA,  
    rsaKeyPublicExponent                 открытая экспонента ключа RSA  
}
```


rsaKeyModulus - модуль парного ключа.

rsaKeyPublicExponent - открытая экспонента парного ключа.

2.87 RegionAlpha (буквенный код региона)

Буквенное обозначение региона в конкретной стране.

RegionAlpha ::= СТРОКА IA5 (РАЗМЕР (3))

Присвоение значения:

' '	информации нет,
Испания:	
'AN '	Андалусия,
'AR '	Арагон,
'AST'	Астурия,
'C '	Кантабрия,
'CAT'	Каталония,
'CL '	Кастилия-Леон,
'CM '	Кастилия-ла-Манча,
'CV'	Валенсия,
'EXT'	Эстремадура,
'G '	Галисия,
'IB '	Балеарские острова,
'IC '	Канарские острова,
'LR '	Ла-Риоха,
'M '	Мадрид,
'MU '	Мурсия,
'NA '	Наварра,
'PV '	Страна Басков

2.88 RegionNumeric (числовой код района)

Числовое обозначение района в конкретной стране.

RegionNumeric ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (1))

Присвоение значения:

'00'Н	данных нет,
Испания:	
'01'Н	Андалусия,
'02'Н	Арагон,
'03'Н	Астурия,
'04'Н	Кантабрия,
'05'Н	Каталония,
'06'Н	Кастилия-Леон,
'07'Н	Кастилия-ла-Манча,
'08'Н	Валенсия,
'09'Н	Эстремадура,
'0A'Н	Галисия,
'0B'Н	Балеарские острова,
'0C'Н	Канарские острова,
'0D'Н	Ла-Риоха,
'0E'Н	Мадрид,
'0F'Н	Мурсия,
'10'Н	Наварра,
'11'Н	Страна Басков

2.89 RSAKeyModulus (модуль ключа RSA)

Модуль парного ключа RSA.

`RSAKeyModulus ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (128))`

Присвоение значения: не определено.

2.90 RSAKeyPrivateExponent (закрытая экспонента ключа RSA)

(закрытая экспонента парного ключа RSA.

`RSAKeyPrivateExponent ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (128))`

Присвоение значения: не определено.

2.91 RSA KeyPrivateExponent (открытая экспонента ключа RSA)

Открытая экспонента ключа RSA.

RSAKeyPublicExponent ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР (8))

Присвоение значения: не определено.

2.92 SensorApprovalNumber (номер официального утверждения датчика)

Номер официального утверждения типа датчика.

SensorApprovalNumber ::= строка IA5 (РАЗМЕР(8))

Присвоение значения: не определено.

2.93 SensorIdentification (идентификация датчика)

Информация, записанная в датчике движения, которая имеет отношение к идентификации датчика движения (требование 077).

SensorIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
 sensorSerialNumber серийный номер датчика,
 sensorApprovalNumber номер официального утверждения датчика,
 sensorSCIdentifier идентификатор компонента защиты датчика,
 sensorOSIdentifier идентификатор операционной системы датчика
}

sensorSerialNumber - расширенный серийный номер датчика движения (включая номера деталей и код изготовителя).

sensorApprovalNumber - номер официального утверждения датчика движения.

sensorSCIdentifier - идентификатор компонента защиты датчика движения.

sensorOSIdentifier - идентификатор операционной системы датчика движения.

2.94 SensorInstallation (установка датчика)

Информация, записанная в датчике движения, которая имеет отношение к установке датчика движения (требование 099).

```
SensorInstallation ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    sensorPairingDateFirst           дата подсоединения датчика,  
    firstVuApprovalNumber           номер официального утверждения БУ,  
    firstVuSerialNumber             серийный номер БУ,  
    sensorPairingDateCurrent        дата подсоединения датчика,  
    currentVuApprovalNumber         номер официального утверждения БУ,  
    currentVUSerialNumber           серийный номер БУ  
}
```

sensorPairingDateFirst - дата первого подсоединения датчика движения к бортовому устройству.

firstVuApprovalNumber - номер официального утверждения первого бортового устройства, подсоединенного к датчику движения.

firstVuSerialNumber - серийный номер первого бортового устройства, подсоединенного к датчику движения.

sensorPairingDateCurrent - дата текущего подсоединения датчика движения к бортовому устройству.

currentVuApprovalNumber - официальный номер бортового устройства, подсоединенного в данный момент к датчику движения.

currentVUSerialNumber - серийный номер бортового устройства, подсоединенного в данный момент к датчику движения.

2.95 SensorInstallationSecData (данные о защите датчика)

Информация, записанная на карточке мастерской, которая имеет отношение к данным о защите, необходимым для подсоединения датчиков движения к бортовым устройствам (требование 214).

SensorInstallationSecData ::= сеанс трехкратного шифрования ключа по системе DES

Присвоение значения: в соответствии со стандартом ISO 16844-3.

2.96 SensorOSIdentifier (идентификатор датчика ОС)

Идентификатор операционной системы датчика движения.

SensorOSIdentifier ::= Строка IA5 (РАЗМЕР (2))

Присвоение значения: по усмотрению изготовителя.

2.97 SensorPaired (подсоединенный датчик)

Информация, записанная в бортовом устройстве, которая имеет отношение к идентификации датчика движения, подсоединенного к бортовому устройству (требование 079).

SensorPaired ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
 sensorSerialNumber серийный номер датчика,
 sensorApprovalNumber номер официального утверждения датчика,
 sensorPairingDateFirst дата подсоединения датчика
}

sensorSerialNumber - серийный номер датчика движения, подсоединенного в данный момент к бортовому устройству.

sensorApprovalNumber - номер официального утверждения датчика движения, подсоединенного в данный момент к бортовому устройству.

sensorPairingDateFirst - дата первого подсоединения к бортовому устройству датчика движения, подсоединенного к бортовому устройству в данный момент.

2.98 SensorPairingDate (дата подсоединения датчика)

Дата подсоединения датчика движения к бортовому устройству.

SensorPairingDate ::= Реальное время.

Присвоение значения: не определено.

2.99 SensorSerialNumber (серийный номер датчика)

Серийный номер датчика движения.

SensorSerialNumber ::= Расширенный серийный номер

2.100 SensorSCIdentifier (идентификатор защиты датчика)

Идентификатор компонента защиты датчика движения.

SensorSCIdentifier ::= Страна IA5 (РАЗМЕР (8))

Присвоение значения: по усмотрению изготовителя компонента.

2.101 Signature (подпись)

Цифровая подпись.

Signature ::= ОКТЕТНАЯ СТРОКА (РАЗМЕР(128))

Присвоение значения: в соответствии с общими механизмами защиты, определенными в подразделе 11.

2.102 SimilarEventsNumber (число аналогичных событий)

Число аналогичных событий за один конкретный день (требование 094).

SimilarEventsNumber ::= ЦЕЛОЕ ЧИСЛО (0..255)

Присвоение значения: 0 не используется, 1 означает, что в данный день имело место и было зарегистрировано только одно событие этого типа, 2 означает, что в этот день имели место 2 события (из которых было зарегистрировано только одно), ...255 означает, что в данный день произошло 255 или более событий этого типа.

2.103 SpecificConditionType (тип особой ситуации)

Код, позволяющий идентифицировать ту или иную особую ситуацию (требования 050b, 105a, 212a и 230a).

2.107 SpeedAverage (средняя скорость)

Средняя скорость за предварительно определенный промежуток времени (км/ч).

SpeedAverage ::= Скорость

2.108 SpeedMax (максимальная скорость)

Максимальная скорость за предварительно определенный промежуток времени.

SpeedMax ::= Скорость

2.109 TDesSessionKey (ключ сеанса)

Трехкратное шифрование ключа сеанса в системе DES.

TDesSessionKey ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
 tDesKeyA ОКТЕТНАЯ СТРОКА (РАЗМЕР (8))
 tDesKeyB ОКТЕТНАЯ СТРОКА (РАЗМЕР (8))
}

Присвоение значения: дополнительно не уточняется.

2.110 TimeReal (реальное время)

Код совмещенного поля данных даты и времени, в котором дата и время выражаются в секундах, начиная с 00 ч. 00 м. 00 с. 1 января 1970 года (среднее время по Гринвичу).

TimeReal{INTEGER:TimeRealRange} ::= ЦЕЛОЕ ЧИСЛО (0..TimeRealRange)

Присвоение значения – Выровненный байт: число секунд начиная с полночи 1 января 1970 года (среднее время по Гринвичу).

Максимально возможное отображение даты/времени - 2106 год.

2.111 TyreSize (размер шин)

Обозначение размера шин.

TyreSize ::= Сторона IA5 (РАЗМЕР (15))

Присвоение значения: в соответствии с Правилами ЕЭК №54¹⁴.

2.112 VehicleIdentificationNumber (идентификационный номер транспортного средства)

Идентификационный номер транспортного средства (VIN), указывающий на транспортное средство в целом; обычно это серийный номер шасси или номер рамы.

VehicleIdentificationNumber ::= Сторона IA5 (РАЗМЕР (17))

Присвоение значения: в соответствии с определением в стандарте ИСО 3779.

2.113 VehicleRegistrationIdentification (идентификация регистрации транспортного средства)

Идентификация транспортного средства, индивидуальная для Европы (VRN и Договаривающаяся сторона)

VehicleRegistrationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
 vehicleRegistrationNation числовой код страны,
 vehicleRegistrationNumber номер регистрации транспортного средства
}

vehicleRegistrationNation - страна, в которой зарегистрировано транспортное средство.

vehicleRegistrationNumber - номер регистрации транспортного средства (VRN).

2.114 VehicleRegistrationNumber (номер регистрации транспортного средства)

Номер регистрации транспортного средства (VRN). Номер регистрации присваивается компетентным органом, регистрирующим транспортное средство.

¹⁴ Исходным текстом является директива ЕС 92/23/ЕЕС, касающаяся шин автотранспортных средств и их прицепов и их установки, от 31 марта 1992 года (OJ No L 129, 14/05/1992).

```
VehicleRegistrationNumber ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
  codePage                ЦЕЛОЕ ЧИСЛО (0,255),  
  vehicleRegNumber        ОКТЕТНАЯ СТРОКА (РАЗМЕР(13))  
}
```

codePage - элемент данных, указывающих на раздел стандарта ISO/IEC 8859, использованный для кодирования регистрационного номера транспортного средства,

vehicleRegNumber - VRN, закодированный в соответствии со стандартом ISO/IEC 8859-codePage.

Присвоение значения: по усмотрению страны.

2.115 VuActivityDailyData (данные об изменении деятельности в БУ)

Информация, записанная в БУ, которая имеет отношение к изменению деятельности и/или изменению статуса управления и/или изменению состояния карточки за данный календарный день (требование 084) и к состоянию считывающих устройств на 00:00 часов в указанный день.

```
VuActivityDailyData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
  noOfActivityChanges      ЦЕЛОЕ ЧИСЛО (0.1440),  
  activityChangeInfos      УСТАНОВЛЕННЫЙ РАЗМЕР  
                           (noOfActivityChanges) ПАРАМЕТРА  
                           ActivityChangeInfo  
}
```

noOfActivityChanges - число слов позиции ActivityChangeInfo в совокупности данных activityChangeInfos.

activityChangeInfos - совокупность слов позиции ActivityChangeInfo, записанных в БУ за данный день. Она всегда включает два слова ActivityChangeInfo, указывающих на состояние считывающих устройств в 00:00 часов в указанный день.

2.116 VuApprovalNumber (номер официального утверждения БУ)

Номер официального утверждения типа бортового устройства

```
VuApprovalNumber ::= Сторона IA5 (РАЗМЕР (8))
```

Присвоенное значение: не определено.

2.117 **VuCalibrationData** (дата калибровки БУ)

Информация, записанная в бортовом устройстве, которая имеет отношение к калибровке контрольного устройства (требование 098).

```
VuCalibrationData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    noOfVuCalibrationRecords          ЦЕЛОЕ ЧИСЛО (0,255),  
    vuCalibrationRecords              УСТАНОВЛЕННЫЙ РАЗМЕР  
                                     (noOfVuCalibrationRecords) ПАРАМЕТРА  
                                     VuCalibrationRecord  
}
```

noOfVuCalibrationRecords - число записей, содержащееся в совокупности vuCalibrationRecords.

vuCalibrationRecords - совокупность записей калибровки.

2.118 **VuCalibrationRecord** (запись калибровки БУ)

Информация, записанная в бортовом устройстве, которая имеет отношение к калибровке контрольного устройства (требование 098).

```
VuCalibrationRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    calibrationPurpose                цель калибровки,  
    workshopName                      название,  
    workshopAddress                   адрес,  
    workshopCardNumber                полный номер карточки,  
    workshopCardExpiryDate            реальное время,  
    vehicleIdentificationNumber        идентификационный номер транспортного  
                                       средства,  
    vehicleRegistrationIdentification  идентификация регистрации транспортного  
                                       средства,  
    wVehicleCharacteristicConstant    характеристическая постоянная  
                                       транспортного средства W,  
    kConstantOfRecordingEquipment     постоянная записывающего оборудования K,  
    lTyreCircumference                 окружность шины L,
```

tyreSize	размер шины,
authorisedSpeed	разрешенная скорость,
oldOdometerValue	показания счетчика пробега,
newOdometerValue	показания счетчика пробега,
oldTimeValue	реальное время,
newTimeValue	реальное время,
nextCalibrationDate	реальное время
}	

calibrationPurpose - цель калибровки.

workshopName, workshopAddress - название и адрес мастерской.

workshopCardNumber - идентификатор карточки мастерской, использованной во время калибровки.

workshopCardExpiryDate - дата истечения срока действия карточки.

vehicleIdentificationNumber - VIN (опознавательный номер транспортного средства).

vehicleRegistrationIdentification - VRN (регистрационный номер транспортного средства) и Договаривающаяся сторона регистрации.

wVehicleCharacteristicConstant - характеристический коэффициент транспортного средства.

kConstantOfRecordingEquipment - постоянная контрольного устройства.

ITyreCircumference - эффективная окружность шин колес.

tyreSize - обозначение размера шин, установленных на транспортном средстве.

authorisedSpeed - разрешенная скорость транспортного средства.

oldOdometerValue, newOdometerValue - прежние и новые показания счетчика пробега.

oldTimeValue, newTimeValue - прежние и новые значения даты и времени.

nextCalibrationDate - дата следующей калибровки типа, указанной в позиции CalibrationPurpose, которая должна быть произведена уполномоченным инспекционным органом.

2.119 VuCardIWData (данные о вводе и извлечении карточки)

Информация, записанная в бортовом устройстве, которая имеет отношение к циклам ввода карточек водителя или карточек мастерской в бортовое устройство и их извлечения (требование 081).

```
VuCardIWData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    noOfIWRecords          ЦЕЛОЕ ЧИСЛО(0..216-1),  
    vuCardIWRecords       УСТАНОВЛЕННЫЙ РАЗМЕР(noOfIWRecords)  
                           ПАРАМЕТРА VuCardIWRecord  
}
```

noOfIWRecords - число записей в совокупности vuCardIWRecords.

vuCardIWRecords - совокупность записей, относящихся к циклам ввода и извлечения карточек.

2.120 VuCardIWRecord (запись данных о вводе и извлечении карточки)

Информация, записанная в бортовом устройстве, которая имеет отношение к циклу ввода карточки водителя или карточки мастерской в бортовое устройство и их извлечения (требование 081).

```
VuCardIWRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    cardHolderName         фамилия держателя,  
    fullCardNumber        полный номер карточки,  
    cardExpiryDate        реальное время,  
    cardInsertionTime     реальное время,  
    vehicleOdometerValueAtInsertion  показания счетчика пробега,  
    cardSlotNumber        номер считывающего устройства,  
    cardWithdrawalTime    реальное время,  
    vehicleOdometerValueAtWithdrawal  показания счетчика пробега,  
    previousVehicleInfo   информация о предыдущем транспортном  
                           средстве  
    manualInputFlag       отметка, указывающая на ручной ввод данных  
}
```

cardHolderName - фамилия и имя держателя карточки водителя или мастерской, записанные в карточке.

fullCardNumber - тип карточки, выдавшая ее Договаривающаяся сторона и номер карточки, записанные в карточке.

cardExpiryDate - дата истечения срока действия карточки, записанная в карточке.

cardInsertionTime - дата и время ввода карточки.

vehicleOdometerValueAtInsertion - показания счетчика пробега транспортного средства в момент ввода карточки.

cardSlotNumber - считывающее устройство, в которое вставлена карточка.

cardWithdrawalTime - дата и время извлечения карточки.

vehicleOdometerValueAtWithdrawal - показания счетчика пробега транспортного средства в момент извлечения карточки.

previousVehicleInfo - информация о предыдущем транспортном средстве, использованном водителем, записанная в карточке.

manualInputFlag - метка, позволяющая определить, ввел ли держатель карточки в момент ее ввода данные о деятельности водителя вручную.

2.121 VuCertificate (сертификат БУ)

Сертификат открытого ключа бортового устройства.

VuCertificate ::= сертификат

2.122 VuCompanyLocksData (дата блокировки БУ предприятием)

Информация, записанная в бортовом устройстве, которая относится к блокировкам, установленным предприятием (требование 104).

```
VuCompanyLocksData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    noOfLocks                ЦЕЛОЕ ЧИСЛО(0..20),  
    vuCompanyLocksRecords    УСТАНОВЛЕННЫЙ РАЗМЕР(noOfLocks)  
                             ПАРАМЕТРА VuCompanyLocksRecord  
}
```

noOfLocks - число блокировок, перечисленных в файле vuCompanyLocksRecords.

vuCompanyLocksRecords - совокупность записей о блокировках, установленных предприятием.

2.123 VuCompanyLocksRecord (запись блокировки БУ предприятием)

Информация, записанная в бортовом устройстве, которая относится к одной блокировке, произведенной предприятием (требование 104).

```
VuCompanyLocksRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    lockInTime                реальное время,  
    lockOutTime              реальное время,  
    companyName              название,  
    companyAddress           адрес,  
    companyCardNumber        полный номер карточки  
}
```

lockInTime, lockOutTime - дата и время блокировки и снятия блокировки.

companyName, companyAddress - название и адрес предприятия, которое произвело блокировку.

companyCardNumber - номер, идентифицирующий карточку, использованную для блокировки.

2.124 VuControlActivityData (дата операций по проверке БУ)

Информация, записанная в бортовом устройстве, которая имеет отношение к проверкам данного БУ (требование 102).

```
VuControlActivityData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    noOfControls                ЦЕЛОЕ ЧИСЛО(0..20),  
    vuControlActivityRecords    УСТАНОВЛЕННЫЙ РАЗМЕР(noOfControls)  
                                ПАРАМЕТРА VuControlActivityRecord  
}
```

noOfControls - число проверок, перечисленных в файле vuControlActivityRecords.

vuControlActivityRecords - совокупность записей о проверочных операциях.

2.125 VuControlActivityRecord (запись операций по проверке БУ)

Информация, записанная в бортовом устройстве, которая имеет отношение к проверке данного БУ (требование 102).

```
VuControlActivityRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    controlType                тип проверки,  
    controlTime                реальное время,  
    controlCardNumber          полный номер карточки,  
    downloadPeriodBeginTime    реальное время,  
    downloadPeriodEndTime      реальное время  
}
```

controlType - тип проверки.

controlTime - дата и время проверки.

controlCardNumber - идентификатор карточки контролера, использованной для проверки.

downloadPeriodBeginTime - время начала периода, за который загружаются данные (в случае загрузки).

downloadPeriodEndTime - время конца периода, за который загружаются данные (в случае загрузки).

noOfSpeedBlocks - число блоков скорости в совокупности **vuDetailedSpeedBlocks**.

vuDetailedSpeedBlocks - совокупность блоков данных об изменении скорости.

2.129 **VuDownloadablePeriod** (период загрузки данных в БУ)

Самая ранняя и самая последняя дата, на которую хранятся в бортовом устройстве данные о деятельности водителя (требования 081, 084 или 087).

```
VuDownloadablePeriod ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    minDownloadableTime  
    maxDownloadableTime          реальное время  
}
```

minDownloadableTime - самая ранняя дата и время ввода карточки, въезда на данную территорию или изменения вида деятельности, которые хранятся в блоке памяти бортового устройства.

maxDownloadableTime - самая последняя дата и время извлечения карточки, въезда на данную территорию или изменения вида деятельности, которые хранятся в блоке памяти бортового устройства.

2.130 **VuDownloadActivityData** (информация о загрузке данных в БУ)

Информация, записанная в бортовом устройстве, которая указывает на время последней загрузки (требование 105).

```
VuDownloadActivityData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    downloadingTime          реальное время,  
    fullCardNumber          полный номер карточки,  
    companyOrWorkshopName    название  
}
```

downloadingTime - дата и время загрузки.

fullCardNumber - идентификатор использованной карточки, разрешающий загрузку.

companyOrWorkshopName - название предприятия или мастерской.

2.131 VuEventData (данные о событиях в БУ)

Информация, записанная в бортовом устройстве, указывающая на события (требование 094, за исключением случая превышения скорости).

```
VuEventData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    noOfVuEvents                ЦЕЛОЕ ЧИСЛО (0,255),  
    vuEventRecords              УСТАНОВЛЕННЫЙ РАЗМЕР (noOfVuEvents)  
                                параметра VuEventRecord  
}
```

noOfVuEvents - число событий, перечисленных в массиве данных vuEventRecords.

vuEventRecords - совокупность записей данных о событиях.

2.132 VuEventRecord (записи событий в БУ)

Информация, записанная в бортовом устройстве, указывающая на соответствующее событие (требование 094, за исключением случая превышения скорости).

```
VuEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    eventType                   тип события/неисправности,  
    eventRecordPurpose          причина регистрации события/неисправности,  
    eventBeginTime              реальное время,  
    eventEndTime                реальное время,  
    cardNumberDriverSlotBegin   полный номер карточки,  
    cardNumberCodriverSlotBegin полный номер карточки,  
    cardNumberDriverSlotEnd     полный номер карточки,  
    cardNumberCodriverSlotEnd   полный номер карточки,  
    similarEventsNumber         число аналогичных событий  
}
```

eventType - тип события.

eventRecordPurpose - цель регистрации данного события.

eventBeginTime - дата и время начала события.

eventEndTime - дата и время конца события.

cardNumberDriverSlotBegin - идентификатор вставленной карточки в считывающее устройство водителя в начале события.

cardNumberCodriverSlotBegin - идентификатор вставленной карточки в считывающее устройство второго водителя в начале события.

cardNumberDriverSlotEnd - идентификатор вставленной карточки в считывающее устройство водителя в конце события.

cardNumberCodriverSlotEnd - идентификатор вставленной карточки в считывающее устройство второго водителя в конце события.

similarEventsNumber - число аналогичных событий в указанный день.

Эта последовательность может быть использована для всех событий, помимо случаев превышения скорости.

2.133 VuFaultData (данные о неисправностях в БУ)

Информация, записанная в бортовом устройстве, указывающая на неисправности (требование 096).

```
VuFaultData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    noOfVuFaults                ЦЕЛОЕ ЧИСЛО (0,255),  
    vuFaultRecords              УСТАНОВЛЕННЫЙ РАЗМЕР (noOfVuFaults)  
                                параметра VuFaultRecord  
}
```

noOfVuFaults - число неисправностей, перечисленных в массиве данных vuFaultRecords.

vuFaultRecords - совокупность записей о неисправностях.

2.134 VuFaultRecord (записи о неисправностях в БУ)

Информация, записанная в бортовом устройстве, которое указывает на неисправность (требование 096).

```
VuFaultRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    faultType                    тип неисправности,  
    faultRecordPurpose           цель регистрации неисправности,  
    faultBeginTime              реальное время,  
    faultEndTime                реальное время,  
    cardNumberDriverSlotBegin   полный номер карточки,
```

cardNumberCodriverSlotBegin	полный номер карточки,
cardNumberDriverSlotEnd	полный номер карточки,
cardNumberCodriverSlotEnd	полный номер карточки

}

faultType - тип неисправности контрольного устройства.

faultRecordPurpose - цель регистрации данной неисправности.

faultBeginTime - дата и время начала неисправности.

faultEndTime - дата и время конца 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.

2.135 VuIdentification (идентификация БУ)

Информация, записанная в бортовом устройстве, которая указывает на идентификацию бортового устройства (требование 075).

VuIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {

vuManufacturerName	название изготовителя БУ,
vuManufacturerAddress	адрес изготовителя БУ,
vuPartNumber	номер детали БУ,
vuSerialNumber	серийный номер БУ,
vuSoftwareIdentification	идентификация программного обеспечения БУ,
vuManufacturingDate	дата изготовления БУ,
vuApprovalNumber	номер официального утверждения БУ

}

vuManufacturerName - название изготовителя бортового устройства.

vuManufacturerAddress - адрес изготовителя бортового устройства.

vuPartNumber - номер детали бортового устройства.

vuSerialNumber - серийный номер бортового устройства.

vuSoftwareIdentification - идентификатор программного обеспечения, использованного в бортовом устройстве.

vuManufacturingDate - дата изготовления бортового устройства.

vuApprovalNumber - номер официального утверждения бортового устройства.

2.136 VuManufacturerAddress (адрес изготовителя БУ)

Адрес изготовителя бортового устройства.

VuManufacturerAddress ::= адрес.

Присвоение значения: не определено.

2.137 (название изготовителя БУ)

Название изготовителя бортового устройства.

VuManufacturerName ::= название

Присвоение значения: дата изготовления бортового устройства.

2.138 VuManufacturingDate (дата изготовления БУ)

Дата изготовления бортового устройства.

VuManufacturingDate ::= реальное время

Присвоение значения: не определено.

2.139 VuOverSpeedingControlData (данные о контроле за превышением скорости в БУ)

Информация, записанная в бортовом устройстве, которая указывает на случаи превышения скорости после последнего контроля за превышением скорости (требование 095).

```
VuOverSpeedingControlData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    lastOverspeedControlTime        реальное время,  
    firstOverspeedSince             реальное время,  
    numberOfOverspeedSince          число превышений скорости  
}
```

lastOverspeedControlTime - дата и время последнего контроля за превышением скорости.

firstOverspeedSince - дата и время первого превышения скорости после указанного контроля за превышением скорости.

numberOfOverspeedSince - число случаев превышения скорости после последнего контроля за превышением скорости.

2.140 VuOverSpeedingEventData (данные о случаях превышения скорости в БУ)

Информация, записанная в бортовом устройстве, которая указывает на случаи превышения скорости (требование 094).

```
VuOverSpeedingEventData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    noOfVuOverSpeedingEvents        ЦЕЛОЕ ЧИСЛО(0..255),  
    vuOverSpeedingEventRecords      УСТАНОВЛЕННЫЙ  
                                    РАЗМЕР(noOfVuOverSpeedingEvents) ПАРАМЕТРА  
                                    VuOverSpeedingEventRecord  
}
```

noOfVuOverSpeedingEvents - число случаев, перечисленных в массиве данных vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords - массив данных, содержащий записи случаев превышения скорости.

2.141 VuOverSpeedingEventRecord (записи случаев превышения скорости в БУ)

Информация, записанная в бортовом устройстве, которая указывает на случаи превышения скорости (требование 094).

VuOverSpeedingEventRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
 eventType тип события/неисправности,
 eventRecordPurpose цель регистрации события/неисправности,
 eventBeginTime реальное время,
 eventEndTime реальное время,
 maxSpeedValue максимальная скорость,
 averageSpeedValue средняя скорость,
 cardNumberDriverSlotBegin полный номер карточки,
 similarEventsNumber число аналогичных событий
}

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 - среднее арифметическое скорости, измеренной во время события.

cardNumberDriverSlotBegin - идентификатор карточки, вставленной в считывающее устройство водителя в начале события.

similarEventsNumber - число аналогичных событий в указанный день.

2.142 VuPartNumber (номер детали БУ)

Номер детали бортового устройства.

VuPartNumber ::= Строка IA5(РАЗМЕР(16))

Присвоение значения: по усмотрению изготовителя БУ.

2.143 VuPlaceDailyWorkPeriodData (данные о месте/ежедневном периоде работы в БУ)

Информация, записанная в бортовом устройстве, которая указывает на места, в которых водители начинают или завершают ежедневные периоды работы (требование 087).

```
VuPlaceDailyWorkPeriodData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    noOfPlaceRecords          ЦЕЛОЕ ЧИСЛО(0..255),  
    vuPlaceDailyWorkPeriodRecords  УСТАНОВЛЕННЫЙ РАЗМЕР  
                                   (noOfPlaceRecords) ПАРАМЕТРА  
                                   VuPlaceDailyWorkPeriodRecord  
}
```

noOfPlaceRecords - число записей, перечисленных в массиве данных vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords - массив записей с указанием мест.

2.144 VuPlaceDailyWorkPeriodRecord (записи о месте/ежедневном периоде работы в БУ)

Информация, записанная в бортовом устройстве, которая указывает на место, в котором водитель начинает или заканчивает ежедневный период работы (требование 087).

```
VuPlaceDailyWorkPeriodRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    fullCardNumber            полный номер карточки,  
    placeRecord              запись данных о месте  
}
```

fullCardNumber - тип карточки водителя, Договаривающаяся сторона, выдавшая карточку и номер карточки.

placeRecord - запись, содержащая информацию о месте въезда.

2.145 VuPrivateKey (закрытый ключ БУ)

Закрытый ключ бортового устройства.

VuPrivateKey ::= Закрытая экспонента ключа RSA

2.146 VuPublicKey (открытый ключ БУ)

Открытый ключ бортового устройства

VuPublicKey ::= открытый ключ

2.147 VuSerialNumber (серийный номер БУ)

Серийный номер бортового устройства (требование 075).

VuSerialNumber ::= расширенный серийный номер

2.148 VuSoftInstallationDate (дата установки программы БУ)

Дата установки варианта программного обеспечения бортового устройства.

VuSoftInstallationDate ::= реальное время

Присвоение значения: не определено.

2.149 VuSoftwareIdentification (идентификация программы БУ)

Информация, записанная в бортовом устройстве, которая указывает на установленное программное обеспечение.

VuSoftwareIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
 vuSoftwareVersion вариант программы БУ,
 vuSoftInstallationDate дата установки программы БУ
}

vuSoftwareVersion - номер версии программного обеспечения бортового устройства.

vuSoftInstallationDate - дата установки версии программного обеспечения.

2.150 VuSoftwareVersion (версия программы БУ)

Вариант программного обеспечения бортового устройства.

VuSoftwareVersion ::= IA5Размер(РАЗМЕР(4))

Присвоение значения: не определено.

2.151 VuSpecificConditionData (данные об особых ситуациях в БУ)

Информация, записанная в бортовом устройстве, которая указывает на особые ситуации.

VuSpecificConditionData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
 noOfSpecificConditionRecords ЦЕЛОЕ ЧИСЛО(0..216-1)
 specificConditionRecords УСТАНОВЛЕННЫЙ РАЗМЕР
 (noOfSpecificConditionRecords)
 ПАРАМЕТРА SpecificConditionRecord
}

noOfSpecificConditionRecords - число записей, перечисленных в массиве данных specificConditionRecords.

specificConditionRecords - массив данных, содержащих записи об особых ситуациях.

2.152 VuTimeAdjustmentData (данные о корректировке времени в БУ)

Информация, записанная в бортовом устройстве, которая указывает на корректировки времени, произведенные вне программы регулярной калибровки (требование 101)

VuTimeAdjustmentData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
 noOfVuTimeAdjRecords ЦЕЛОЕ ЧИСЛО(0..6),
 vuTimeAdjustmentRecords УСТАНОВЛЕННЫЙ РАЗМЕР
 (noOfVuTimeAdjRecords) ПАРАМЕТРА
 VuTimeAdjustmentRecord
}

noOfVuTimeAdjRecords - число записей в массиве данных TimeAdjustmentRecords.

vuTimeAdjustmentRecords - массив данных с записями о корректировке времени.

2.153 VuTimeAdjustmentRecord (записи корректировки времени в БУ)

Информация, записанная в бортовом устройстве, указывающая на корректировку времени, произведенную вне программы регулярной калибровки (требование 101)

```
VuTimeAdjustmentRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    newTimeValue    реальное время,  
    workshopName    название,  
    workshopAddress адрес,  
    workshopCardNumber    полный номер карточки  
}
```

oldTimeValue, newTimeValue - прежнее и новое значения даты и времени.

workshopName, workshopAddress - название и адрес мастерской.

workshopCardNumber - идентификатор карточки мастерской, использованной для корректировки времени.

2.154 W-VehicleCharacteristicConstant (характеристическая постоянная W транспортного средства)

Характеристический коэффициент транспортного средства (определение k)).

```
W-VehicleCharacteristicConstant ::= ЦЕЛОЕ ЧИСЛО (0..216-1))
```

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

2.155 WorkshopCardApplicationIdentification (идентификация приложения карточки мастерской)

Информация, записанная в карточке мастерской, которая указывает на идентификацию приложения карточки (требование 190).

```
WorkshopCardApplicationIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    typeOfTachographCardId    тип оборудования  
    cardStructureVersion        вариант структуры карточки
```

noOfEventsPerType	число событий по типу
noOfFaultsPerType	число неисправностей по типу
activityStructureLength	диапазон длины записи, касающейся деятельности
noOfCardVehicleRecords	число записей, касающихся транспортного средства
noOfCardPlaceRecords	число записей, касающихся мест
noOfCalibrationRecords	число записей калибровок
}	

typeOfTachographCardId - данные, указывающие на тип использованной карточки.

cardStructureVersion - данные, указывающие вариант структуры, использованной в карточке.

noOfEventsPerType - число событий по типу события, которое может храниться на карточке.

noOfFaultsPerType - число неисправностей по типу неисправности, которое может храниться на карточке

activityStructureLength - число имеющихся байтов памяти для хранения записей, касающихся деятельности.

noOfCardVehicleRecords - число записей, касающихся транспортного средства, которое может храниться на карточке.

noOfCardPlaceRecords - число мест, которое может храниться на карточке.

noOfCalibrationRecords - число записей калибровки, которое может храниться на карточке.

2.156 WorkshopCardCalibrationData (данные о калибровке на карточке мастерской)

Информация, записанная на карточке мастерской, указывающая на операцию, произведенную мастерской с карточкой (требования 227 и 229).

```
WorkshopCardCalibrationData ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    calibrationTotalNumber          ЦЕЛОЕ ЧИСЛО (0 .. 216-1),  
    calibrationPointerNewestRecord  ЦЕЛОЕ ЧИСЛО(0 .. NoOfCalibrationRecords-1),  
    calibrationRecords              УСТАНОВЛЕННЫЙ РАЗМЕР  
                                    (NoOfCalibrationRecords) ПАРАМЕТРА  
                                    WorkshopCardCalibrationRecord  
}
```

calibrationTotalNumber - общее число калибровок, произведенных с карточкой.

calibrationPointerNewestRecord - индекс последней обновленной записи калибровки.

Присвоение значения: число, соответствующее численному показателю записи калибровки, которое начинается с '0' в случае первой записи калибровки в структуре.

calibrationRecords - массив данных с записями, содержащими данные о калибровке и/или корректировке времени.

2.157 WorkshopCardCalibrationRecord (записи калибровки на карточке мастерской)

Информация, записанная на карточке мастерской, которая указывает на калибровку, произведенную с карточкой (требование 227).

```
WorkshopCardCalibrationRecord ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {  
    calibrationPurpose              цель калибровки,  
    vehicleIdentificationNumber     номер идентификации транспортного средства,  
    vehicleRegistration             идентификация регистрации транспортного  
                                    средства,  
    wVehicleCharacteristicConstant характеристическая постоянная транспортного  
                                    средства W,  
    kConstantOfRecordingEquipment  постоянная записывающего оборудования K  
    lTyreCircumference              окружность шин L,  
    tyreSize                        размер шин,  
    authorisedSpeed                 разрешенная скорость,  
    oldOdometerValue               показания счетчика пробега,  
    newOdometerValue               показания счетчика пробега,  
    oldTimeValue                   реальное время,  
    newTimeValue                   реальное время,  
    nextCalibrationDate             реальное время,
```

<code>vuPartNumber</code>	номер детали БУ,
<code>vuSerialNumber</code>	серийный номер БУ,
<code>sensorSerialNumber</code>	серийный номер датчика

}

calibrationPurpose - цель калибровки.

vehicleIdentificationNumber - опознавательный номер транспортного средства (VIN).

vehicleRegistration - VIN и Договаривающаяся сторона регистрации.

wVehicleCharacteristicConstant - характеристический коэффициент транспортного средства.

kConstantOfRecordingEquipment - постоянная контрольного устройства.

ITyreCircumference - эффективная окружность шин колес.

tyreSize - обозначение размеров шин, установленных на транспортном средстве.

authorisedSpeed - максимальная разрешенная скорость транспортного средства.

oldOdometerValue, newOdometerValue - прежние и новые показания счетчика пробега.

oldTimeValue, newTimeValue - прежние и новые значения даты и времени.

nextCalibrationDate - дата следующей калибровки типа, указанного в файле CalibrationPurpose, которая должна осуществляться уполномоченным инспекционным органом.

vuPartNumber, vuSerialNumber и **sensorSerialNumber** - элементы данных, идентифицирующие контрольное устройство.

2.158 **WorkshopCardHolderIdentification** (идентификация держателя карточки мастерской)

Информация, записанная в карточке мастерской, указывающая на идентификацию держателя карточки (требование 216).

WorkshopCardHolderIdentification ::= ПОСЛЕДОВАТЕЛЬНОСТЬ {
workshopName название,
workshopAddress адрес,
cardHolderName фамилия держателя,
cardHolderPreferredLanguage язык
}

workshopName - название мастерской держателя карточки.

workshopAddress - адрес мастерской держателя карточки.

cardHolderName - фамилия и имя (имена) держателя (например, фамилия механика).

cardHolderPreferredLanguage - предпочитаемый язык держателя карточки.

2.159 WorkshopCardPIN (PIN-код карточки мастерской)

Персональный идентификационный номер карточки мастерской (требование 213).

WorkshopCardPIN ::= Строка IA5 (РАЗМЕР(8))

Присвоение значения: Известный номер PIN держателя карточки, за которым следует серия байтов 'FF' (до восьми байтов).

3. Определение диапазонов значений и размеров

Определение значений переменных, используемых для определений, содержащихся в пункте 2.

TimeRealRange ::= $2^{32}-1$

3.1 Определения для карточки водителя:

Название переменной	мин.	макс.
CardActivityLengthRange	5 544 байта (28 дней, 93 изменения вида деятельности в день)	13 776 байтов (28 дней, 240 изменений вида деятельности в день)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2 Определения для карточки мастерской:

Название переменной	мин.	макс.
CardActivityLengthRange	198 байтов (1 день, 93 изменения вида деятельности)	492 байта (1 день, 240 изменений вида деятельности)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfFaultsPerType	6	6
NoOfCalibrationRecords	88	255

3.3 Определения для карточки контролера:

Название переменной	мин.	макс.
NoOfControlActivityRecords	230	520

3.4 Определения для карточки предприятия:

Название переменной	мин.	макс.
NoOfCompanyActivityRecords	230	520

4. Наборы знаков

В строках IA5 используются знаки ASCII, определенные в стандарте ISO/IEC 8824-1. Для удобочитаемости и простоты присвоенные значения приводятся ниже. В случае разночтений вместо этой информационной записки следует использовать стандарт ISO/IEC 8824-1.

```
! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

В других строках знаков (адрес, название, номер регистрации транспортного средства) используются, кроме того, знаки, определенные кодами 192-255 стандарта ISO/IEC 8859-1 (Набор латинских знаков типа 1) или ISO/IEC 8859-7 (Набор греческих знаков).

5. Кодирование

В случае кодирования с помощью правил кодирования ASN.1 все определенные типы данных кодируются в соответствии со стандартом ISO/IEC 8825-2 (согласованный вариант).

ПОДРАЗДЕЛ II СПЕЦИФИКАЦИИ НА КАРТОЧКИ ТАХОГРАФА

СОДЕРЖАНИЕ

	<u>Стр.</u>
1. Введение.....	181
1.1 Сокращения.....	181
1.2 Источники	182
2. Электрические и физические характеристики	183
2.1 Напряжение питания и потребление тока.....	183
2.2 Программирующее напряжение V_{pp}	183
2.3 Формирование и частота тактовых сигналов	183
2.4 Контакт "вход-выход"	184
2.5 Состояние карточки	184
3. Аппаратное оборудование и передача данных.....	185
3.1 Введение.....	185
3.2 Протокол передачи данных	185
3.2.1 Протоколы.....	185
3.2.2 ATR (ответ на сигнал перезагрузки)	187
3.2.3 PTS (выбор протокола передачи).....	187
3.3 Условия доступа (АС).....	188
3.4 Шифрование данных.....	189
3.5 Сводный перечень команд и кодов ошибок	189
3.6 Описание команд.....	191
3.6.1 Select File (выбор файла)	192
3.6.1.1 Select File (AID) (Выбор по названию).....	192
3.6.1.2 Выбор элементарного файла (EF) с использованием идентификатора файла.....	193
3.6.2 Read Binary (считывание данных)	194
3.6.2.1 Команда, передаваемая в некриптозащищенном виде	194
3.6.2.2 Команда, передаваемая в криптозащищенном виде	196
3.6.3 Update Binary (обновление данных)	199
3.6.3.1 Команда, передаваемая в некриптозащищенном виде	199
3.6.3.2 Команда, передаваемая в криптозащищенном виде	200
3.6.4 Get Challenge (получение запроса)	202
3.6.5 Verify (проверка)	203
3.6.6 Get Response (получение ответа)	205
3.6.7 PSO: Verify Certificate (проверка сертификата).....	206
3.6.8 Internal Authenticate (внутренняя аутентификация).....	207
3.6.9 External Authenticate (внешняя аутентификация).....	209
3.6.10 Manage Security Environment (управление средой защиты).....	211
3.6.11 PSO: Hash (хеширование).....	212
3.6.12 Perform Hash of File (хеширование файла)	213

СОДЕРЖАНИЕ (продолжение)

	<u>Стр.</u>
3.6.13 PSO: Compute Digital Signature (расчет цифровой подписи).....	214
3.6.14 PSO: Verify Digital Signature (проверка цифровой подписи)	215
4. Структура карточек тахографа.....	216
4.1 Структура карточки водителя	217
4.2 Структура карточки мастерской	220
4.3 Структура карточки контролера	224
4.4 Структура карточки предприятия.....	226

1. Введение

1.1 Сокращения

Для целей настоящего подраздела используются следующие сокращения.

AC	Условия доступа
AID	Идентификатор приложения
ALW	Всегда
APDU	Элемент данных протокола приложения (структура команды)
ATR	Ответ на перезагрузку
AUT	Подтверждено
C6, C7	Контакты N° 6 и 7 карточки в соответствии с описанием в стандарте ISO/IEC 7816-2
cc	тактывные циклы (тц)
CHV	Информация для проверки идентификационных данных держателя карточки
CLA	Байт класса команды APDU
DF	Каталог: DF может содержать другие файлы (EF или DF)
EF	Элементарный файл
ENC	Зашифровано: доступ возможен только с использованием закодированных данных
etu	Элементарная единица времени (эев)
IC	Интегральная схема (ИС)
ICC	Карточка на интегральной схеме (КИС)
ID	Идентификатор
IFD	Интерфейс
IFS	Размер поля данных
IFSC	Размер поля данных на карточке
IFSD	Размер зоны данных (предназначенных для терминалов)
INS	Командный байт APDU
Lc	Длина вводимых данных для команды APDU
Le	Длина ожидаемых данных (выходные данные команды)
MF	Главный файл (корневой DF)
P1-P2	Параметрические байты
NAD	Узловой адрес, используемый в протоколе T=1
NEV	Никогда
PIN	Персональный идентификационный номер
PRO SM	Криптозащищенное сообщение
PTS	Выбор протокола передачи

RFU	Зарезервировано для будущего использования
RST	Перезагрузка (карточки)
SM	Криптозащищенный обмен сообщениями
SW1-SW2	Байты состояния
TS	Начальный знак ATR
VPP	Напряжение программирования
XXh	Значение XX в шестнадцатиричном исчислении
 	Символ связи 03 04=0304

1.2 Источники

В настоящем подразделе использованы следующие источники:

EN 726-3 Системы идентификационных карточек - Карточки и терминалы на интегральных схемах для передачи данных - Часть 3: применение независимых требований к карточке. Декабрь 1994 года.

ISO/IEC 7816-2 Информационные технологии - Карточки идентификационные - Карточки на интегральных схемах с контактами - Часть 2: Размеры и расположение контактов. Издание первое: 1999 год.

ISO/IEC 7816-3 Информационные технологии - Карточки идентификационные - Карточки на интегральных схемах с контактами - Часть 3: Электронные сигналы и протокол передачи данных. Издание 2: 1997 год.

ISO/IEC 7816-4 Информационные технологии - Карточки идентификационные - Карточки на интегральных схемах с контактами - Часть 4: Межотраслевые команды обмена данных. Издание первое: 1995 год + поправка 1: 1997 год.

ISO/IEC 7816-6 Информационные технологии - Карточки идентификационные - Карточки на интегральных схемах с контактами - Часть 6: Межотраслевые элементы данных. Издание первое: 1996 год + поправка 1: 1998 год.

ISO/IEC 7816-8 Информационные технологии - Карточки идентификационные - Карточки на интегральных схемах с контактами - Часть 8: Межотраслевые команды, связанные с защитой. Издание первое: 1999 год.

ISO/IEC 9797 Информационные технологии - методы защиты - механизм обеспечения целостности данных с использованием функции криптографической проверки на основе алгоритма блочного шифрования. Издание 2: 1994 год.

2. Электрические и физические характеристики

TCS_200 Все электрические сигналы должны соответствовать стандарту ISO/IEC 7816-3, если не указано иное.

TCS_201 Расположение и размеры контактов карточки должны соответствовать стандарту ISO/IEC 7816-2.

2.1 Напряжение питания и потребление тока

TCS_202 Карточка должна работать в соответствии со спецификациями на предельные значения потребления, указанные в стандарте ISO/IEC 7816-3.

TCS_203 Карточка должна работать при $V_{cc} = 3 \text{ В} (\pm 0,3\text{В})$ или при $V_{cc} = 5\text{В} (\pm 0,5\text{В})$.

Выбор напряжения производится в соответствии со стандартом ISO/IEC 7816-3.

2.2 Программирующее напряжение V_{pp}

TCS_204 Карточка не должна предусматривать наличие программирующего напряжения на выводе С6. Предполагается, что вывод С6 к интерфейсу не подсоединяется. На контакт С6 может подаваться напряжение V_{cc} с карточки, однако он не должен подсоединяться на массу. В любом случае это напряжение не должно интерпретироваться.

2.3 Формирование и частота тактовых сигналов

TCS_205 Карточка должна работать в диапазоне частот а 1-5 МГц в течение одного сеанса использования карточки. Тактовая частота может меняться в пределах $\pm 2\%$. Тактовая частота генерируется бортовым устройством, а не самой карточкой. Рабочий цикл может варьироваться в пределах 40-60%.

TCS_206 В соответствии с параметрами, заложенными в файле карточки EF_{ICC}, внешние часы могут останавливаться. Первый байт основного файла EF_{ICC} кодирует параметры режима остановки часов (более подробно см. стандарт EN 726-3):

Нулевой бит	Единичный бит		
бит 3	бит 2	бит 1	
0	0	1	Остановка часов разрешена, предпочитаемый уровень разряда 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 "вход-выход"

TCS_207 Контакт С7 "вход-выход" используется для получения данных от интерфейса и передачи данных на интерфейс. Во время работы в режиме передачи может находиться либо только карточка, либо интерфейс. В том случае, если оба устройства работают в режиме передачи, карточка повреждена не будет. Если передача данных с карточки не производится, она переключается в режим приема.

2.5 Состояние карточки

TCS_208 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 оборудование и передача данных

3.1 Введение

В настоящем пункте излагаются минимальные требования к функциям карточек тахографа и БУ в целях обеспечения правильной работы и эксплуатационной совместимости.

Карточки тахографа в максимальной степени соответствуют применимым нормам стандарта ISO/IEC (прежде всего ISO/IEC 7816). Однако в целях уточнения некоторых ограниченных видов использования или различий, в случае их наличия, характеристики всех команд и протоколов указываются полностью. Указанные команды полностью соответствуют упомянутым выше стандартам, если не оговорено иное.

3.2 Протокол передачи данных

TCS_300 Протокол передачи данных соответствует стандарту ISO/IEC 7816-3.

В частности, БУ должно распознавать сигналы продления времени ожидания, передаваемые карточкой.

3.2.1 Протоколы

TCS_301 Карточка должна поддерживать протокол **T=0** и протокол **T=1**.

TCS_302 **T=0** - протокол по умолчанию, поэтому для изменения протокола на **T=1** нужна команда **PTS** (выбор протокола передачи).

TCS_303 Устройства должны поддерживать **прямой режим** в обоих протоколах. В этой связи для карточки прямой режим обязателен.

TCS_304 Байт **Information Field Size Card** должен быть отображен в ATR в виде AT3. Это значение должно составлять как минимум: 'F0h' (240 байт).

К протоколу применяются следующие ограничения.

TCS_305 **T=0**

- Интерфейс должен принимать ответ на входе и выходе после нарастания сигнала на RST начиная с 400 тц.
- Интерфейс должен быть способен считывать знаки, отделенные во времени на 12 эев.
- Интерфейс должен распознавать ошибочные знаки и их повторение, если они разделены во времени на 13 эев. В случае обнаружения ошибочного знака контакт "вход-выход" должен отражать сигнал ошибки в интервале 1-2 эев. Устройство должно реагировать на задержку продолжительностью 1 эев.
- Интерфейс должен принимать ATR (ответ на перезагрузку) размером 33 байта (TS+ 32)
- Если в ATR есть знак TC1, то для знаков, передаваемых интерфейсом, должно быть предусмотрено дополнительное время хранения, хотя временной интервал между знаками, посылаемыми карточкой, может и в этом случае составлять 12 эев. Это также применимо к знаку АСК, посылаемому карточкой после передачи знака P3 интерфейсом.
- Интерфейс должен принимать знак NUL, передаваемый карточкой.
- Интерфейс должен принимать дополнительный режим для АСК.
- Команда на получение ответа не может использоваться в режиме прямого вывода для получения данных, длина которых может превышать 255 байтов.

TCS_306 **T=1**

- Байт NAD не используется (NAD устанавливается на "00").
- S-блок "ABORT": не используется.
- Ошибка состояния S-блока VPP: не используется.
- Общая длина цепочки вывода данных для поля данных не должна превышать 255 байтов (для обеспечения совместимости с интерфейсом).

- Размер поля данных для интерфейса (IFSD) указывается IFD сразу же после ATR (ответ на сигнал перезагрузки): интерфейс передает запрос на указание размера информационного S-блока после ATR, после чего карточка должна передать обратно данные о размере S-блока интерфейса. Рекомендуемое значение для IFSD: 254 байта.
- Карточка не должна требовать корректировки IFS.

3.2.2 ATR (ответ на сигнал перезагрузки)

TCS_307 Устройство проверяет байты ATR в соответствии со стандартом ISO/IEC 7816-3. Проверка архивных знаков ATR не производится.

Пример базового двойного протокола ATR в соответствии со стандартом ISO/IEC 7816-3

Знак	Значение	Примечания
TS	"3Bh"	Указывает на прямое соглашение.
T0	"85h"	TD1 присутствует; 5 архивных байтов присутствуют.
TD1	"80h"	TD2 присутствует; T=0 подлежит использованию
TD2	"11h"	TA3 присутствует; T=1 подлежит использованию
TA3	"XXh" (at least "F0h")	Размер поля данных карточки (IFSC)
TH1 to TH5	"XXh"	Архивные знаки
TCK	"XXh"	Проверочный знак (исключительно OR)

TCS_308 После ответа на сигнал перезагрузки (ATR) выбирается по косвенным признакам основной файл (MF), который становится текущей директорией.

3.2.3 PTS (выбор протокола передачи)

TCS_309 Протоколом по умолчанию является T=0. Для перехода на протокол T=1 устройство должно передать на карточку сигнал PTS (также обозначаемый сокращением PPS).

TCS_310 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_311 Если другая скорость передачи в бодах, помимо скорости по умолчанию, не поддерживается (или если не поддерживается выбранная скорость передачи в бодах), то карточка должна передать правильную команду PTS в соответствии со стандартом ISO/IEC 7816-3, опустив байт PPS1.

Примеры базовой команды PTS для выбора протокола указаны ниже:

Знак	Значение	Замечания
PPSS	"FFh"	Начальный знак.
PPS0	"00h" или "01h"	PPS1-PPS3 не присутствуют: "00h" для выбора T0, "01h" для выбора T1.
PK	"XXh"	Проверка знака: "XXh" = "FFh" если PPS0 = "00h", "XXh" = "FEh" если PPS0 = "'01h'".

3.3 Условия доступа (AC)

Условия доступа (AC) для команд UPDATE_BINARY и READ_BINARY определяется в каждом элементарном файле.

TCS_312 До открытия доступа к файлу с помощью этих команд должен удовлетворяться параметр AC для данного файла.

Определения имеющихся условий доступа указаны ниже:

- **ALW**: действие возможно во всех случаях и может быть выполнено без каких бы то ни было ограничений.
- **NEV**: действие невозможно ни в каких случаях.
- **AUT**: право, соответствующее успешной внешней аутентификации, должно быть открыто (производится с помощью команды EXTERNAL_AUTHENTICATE).
- **PRO SM**: команда должна передаваться с криптографической контрольной суммой в криптозащищенном виде (см. подраздел 11).
- **AUT** и **PRO SM** (комбинированные).

После обработки команды (UPDATE_BINARY и READ_BINARY) на карточке могут быть открыты следующие условия доступа:

	UPDATE_BINARY	READ_BINARY
ALW	Да	Да
NEV	Да	Да
AUT	Да	Да
PRO SM	Да	Нет
AUT и PRO SM	Да	Нет

Для команды READ_BINARY условие доступа PRO SM отсутствует. Это означает, что наличие криптографической контрольной суммы для команды READ необязательно ни в одном случае. Однако, используя значения 'OC' для данного класса, можно использовать команду READ_BINARY в криптозащищенном виде, как описано в пункте 3.6.2.

3.4 Шифрование данных

В том случае, если надо обеспечить конфиденциальность данных, считываемых с того или иного файла, этот файл должен быть отмечен "Encrypted". Шифрование производится с использованием системы криптозащищенного обмена данными (см. подраздел 11).

3.5 Сводный перечень команд и кодов ошибок

Команды и структура файлов определяются стандартом ISO/IEC 7816-4 и соответствуют ему.

TCS_313 В настоящем разделе приводятся параметры следующих пар "команда-ответ APDU":

Команда	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
PERFORM SECURITY OPERATION : COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A

Команда	INS
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
MANAGE SECURITY ENVIRONMENT : SETTING A KEY	22
PERFORM HASH OF FILE	2A

TCS_314 Слова 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	CX	Неправильный код CHV (PIN). Счетчик оставшихся попыток указывается с помощью "X"
64	00	Ошибка исполнения - состояние постоянной памяти не изменилось. Ошибка целостности
65	00	Ошибка исполнения - состояние постоянной памяти изменилось
65	81	Ошибка исполнения - состояние постоянной памяти изменилось - отказ памяти
66	88	Ошибка защиты: неправильная криптографическая контрольная сумма (во время криптозащищенного обмена сообщениями) или неправильный сертификат (во время проверки сертификата) или неправильная криптограмма (во время внешней аутентификации) или неправильная подпись (во время проверки подписи)
67	00	Неправильная длина (неправильные значения Lc или Le)
69	00	Запрещенная 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 элементарный файл отсутствует)
69	87	Отсутствие предусмотренных криптозащищенных объектов данных

SW1	SW2	Значение
69	88	Неправильные криптозащищенные объекты 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 элементарного файла)
6C	XX	Неправильная длина, SW2 указывает правильную длину. Поле данных не выдается
6D	00	Командный код не поддерживается или недействителен
6E	00	Класс не поддерживается
6F	00	Другие контрольные ошибки

3.6 Описание команд

В настоящей главе описываются параметры обязательных команд для карточек тахографа.

Дополнительные соответствующие данные, относящиеся к криптографическим операциям, даются в подразделе 11 "Общие механизмы защиты".

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_315 Если запрашиваются оба байта длины (Lc и Le), то описываемая команда разделяется на две части; если IFD (интерфейс) использует протокол T=0 : IFD передает команду, описанную с помощью данных P3=Lc + данные, после чего направляет команду GET_RESPONSE (см. пункт 3.6.6) с P3=Le.

TCS_316 Если запрашиваются оба байта длины и если Le=0 (криптозащищенный 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 передает ответ (на это имплицитное значение Le=0) с помощью байтов состояния '61La', где La - число

байтов, имеющих для ответа. После этого IFD генерирует команду GET RESPONSE с P3 = Lc для чтения данных.

3.6.1 Select File (выбор файла)

Эта команда соответствует стандарту ISO/IEC 7816-4, однако ее использование ограничено по сравнению с командой, определенной в указанном стандарте.

Команда SELECT FILE используется:

- для выбора приложения DF (должен использоваться выбор с использованием названия);
- для выбора элементарного файла, соответствующего представленному файлу ID

3.6.1.1 Select File (AID) (Выбор по названию)

Эта команда позволяет выбрать приложение DF на карточке.

TCS_317 Эта команда может быть выполнена из любой точки структуры файла (после ATR и в любое время).

TCS_318 Выбор приложения приводит к перезагрузке текущей среды защиты. После выбора приложения используемый открытый ключ больше не выбирается, а ключ прежнего сеанса криптозащищенной передачи сообщений более недоступен. Условие доступа AUT также теряется.

TCS_319 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Выбор по названию (AID)
P2	1	'0Ch'	Ответ не требуется
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

Ответ на команду SELECT FILE не требуется (в случае T=1 Lc отсутствует, а в случае T=0 запрос на ответ не передается).

TCS_320 Ответное сообщение (запроса на ответ нет)

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- ♦ Если команда проходит, карточка выдает '9000'.
- ♦ Если приложение, соответствующее AID, не найдено, состояние обработки выдается в виде '6A82'.
- ♦ При T=1, если присутствует байт Le, состояние выдается в виде '6700'.
- ♦ При T=0, если запрос на ответ поступает после команды SELECT FILE, состояние выдается в виде '6900'.
- ♦ Если выбранное приложение считается поврежденным (в атрибутах файла обнаружена ошибка целостности), состояние обработки выдается в виде '6400' или '6581'.

3.6.1.2 Выбор элементарного файла (EF) с использованием идентификатора файла

TCS_321 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Выбор EF по текущему каталогу DF
P2	1	'0Ch'	Ответ не требуется
Lc	1	'02h'	Число байтов, переданных на карточку
#6-#7	2	'XXXXh'	Идентификатор файла

Ответ на команду SELECT FILE не требуется (в случае T=1 байт Le отсутствует, а в случае T=0 запрос на ответ не передается).

TCS_322 Ответное сообщение (ответ не запрашивается)

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- ♦ Если команда проходит, карточка выдает '9000'.
- ♦ Если файл, соответствующий идентификатору, не найден, состояние обработки выдается в виде '6A82'.
- ♦ При T=1, если присутствует байт Le, состояние выдается в виде '6700'.
- ♦ При T=0, если запрос на ответ поступает после команды SELECT FILE, состояние выдается в виде '6900'.
- ♦ Если выбранное приложение считается поврежденным (в атрибутах файла обнаружена ошибка целостности), состояние обработки выдается в виде '6400' или '6581'.

3.6.2 Read binary (считывание данных)

Эта команда соответствует стандарту ISO/IEC 7816-4, однако ее использование ограничено по сравнению с командой, определенной в указанном стандарте.

Команда Read Binary используется для считывания данных с "прозрачного" файла.

Ответ карточки сводится к обратной передаче считанных данных, которые могут быть включены в структуру криптозащищенного обмена сообщениями.

TCS_323 Команда может быть выполнена только в том случае, если состояние защиты соответствует атрибутам защиты, определенным для элементарного файла и функции READ.

3.6.2.1 Команда, передаваемая в некриптозащищенном виде

Эта команда позволяет интерфейсу считывать данные с выбранного в данный момент файла EF в некриптозащищенном виде.

TCS_324 Считывание данных с файла с отметкой "Encrypted" с помощью этой команды невозможно.

TCS_325 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	Запрос на криптозащищенный обмен данными отсутствует
INS	1	'B0h'	
P1	1	'XXh'	Сдвиг байтов с начала файла: байт самого старшего разряда
P2	1	'XXh'	Сдвиг байтов с начала файла: байт самого младшего разряда
Le	1	'XXh'	Ожидается указание длины данных. Число байтов, подлежащих извлечению

Примечание: бит 8 байта P1 должен быть равен 0.

TCS_326 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#X	X	'XX..XXh'	Считанные данные
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- ♦ Если команда проходит, карточка выдает **'9000'**.
- ♦ Если выбран EF, состояние обработки выдается в виде **'6986'**.
- ♦ Если параметры контроля доступа к выбранному файлу не удовлетворены, команда прерывается с выдачей **'6982'**.
- ♦ Если сдвиг не соответствует размеру EF (Сдвиг > размера EF), состояние обработки выдается в виде **'6B00'**.
- ♦ Если размер данных, подлежащих извлечению, не соответствует размеру EF (Сдвиг + Le > размера EF), состояние обработки выдается в виде **'6700'** или **'6Cxx'**, где 'xx' указывает точную длину.

- ♦ Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл поврежден и не может быть восстановлен, и состояние обработки выдается в виде '6400' или '6581'.
- ♦ Если в записанных данных обнаруживается ошибка целостности, карточка возвращает затребованные данные, а состояние обработки выдается в виде '6281'.

3.6.2.2 Команда, передаваемая в криптозащищенном виде

Эта команда позволяет интерфейсу считывать данные с выбранного в данный момент файла EF в криптозащищенном виде в целях проверки целостности полученных данных и защиты конфиденциальности данных в том случае, если EF содержит отметку "Encrypted".

TCS_327 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'0Ch'	Запрос на криптозащищенный обмен данными
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (смещение байтов с начала файла): байт самого старшего разряда
P2	1	'XXh'	P2 (смещение байтов с начала файла): байт самого младшего разряда
Lc	1	'09h'	Длина вводимых данных в криптозащищенном виде
#6	1	'97h'	T _{LE} : метка, указывающая спецификацию ожидаемой длины
#7	1	'01h'	L _{LE} : длина ожидаемой длины
#8	1	'NNh'	Спецификация ожидаемой длины (исходная длина L _e): число байтов, подлежащих извлечению
#9	1	'8Eh'	T _{CC} : метка, указывающая криптографическую контрольную сумму
#10	1	'04h'	L _{CC} : длина следующей криптографической контрольной суммы
#11-#14	4	'XX..XXh'	Криптографическая сумма (4 байта самого старшего разряда)
L _e	1	'00h'	Как указано в стандарте ISO/IEC 7816-4

TCS_328 Ответ на сообщение, если файл EF не содержит отметку "Encrypted" и если входной формат криптозащищенного обмена данными правильный:

Байт	Длина	Значение	Описание
#1	1	'81h'	T _{РV} : метка, указывающая значение обычных данных
#2	L	'NNh' или '81 NNh'	L _{РV} : длина переданных обратно данных (=изначальная длина L _e). L равен 2 байтам, если L _{РV} >127 байтов
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Значения обычных данных
#(2+L+NN)	1	'8Eh'	T _{CC} : метка, указывающая криптографическую контрольную сумму
#(3+L+NN)	1	'04h'	L _{CC} : длина следующей криптографической контрольной суммы
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Криптографическая сумма (4 байта самого старшего разряда)
SW	2	'XXXXh'	Слова состояния (SW1, SW2)

TCS_329 Ответ на сообщение, если файл EF содержит отметку "Encrypted" и если входной формат криптозащищенного обмена данными правильный:

Байт	Длина	Значение	Описание
#1	1	'87h'	T _{Р1CG} : Метка, указывающая на зашифрованные данные (криптограмма)
#2	L	'MMh' или '81 MMh'	L _{Р1CG} : длина выданных зашифрованных данных (отличная от изначальной длины L _e команды, что обусловлено заполнением). L равно 2 байтам, если L _{Р1CG} > 127 байтов.
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Зашифрованные данные: показатель заполнения и криптограмма
#(2+L+MM)	1	'8Eh'	T _{CC} : Метка, указывающая на криптографическую контрольную сумму
#(3+L+MM)	1	'04h'	L _{CC} : Длина следующей криптографической контрольной суммы
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Криптографическая контрольная сумма (4 байта самого старшего разряда)
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

Возвращенные зашифрованные данные содержат первый байт, указывающий на использованный способ заполнения. В случае приложения тахографа показатель заполнения всегда принимает значение '01h', что указывает на соответствие использованного способа заполнения способу, предусмотренному в стандарте ISO/IEC 7816-4 (один байт, со значением '80h', за которым следует несколько нулевых байтов: ISO/IEC 9797, метод 2).

Данные о состояниях "нормальной" обработки, описанных в команде READ BINARY, передаваемой в некриптозащищенном виде (см. пункт 3.6.2.1), могут возвращаться с использованием структур ответного сообщения, описанного выше, с меткой "99h" (как указано в TCS 335).

Кроме того, могут иметь место некоторые ошибки, которые конкретно связаны с криптозащищенным обменом сообщениями. В этом случае данные о состоянии обработки просто возвращаются, не задействуя использованную структуру защиты данных:

TCS_330 Ответное сообщение, если входной формат криптозащищенного обмена данными неправильный

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- ♦ Если ключ текущего сеанса отсутствует, состояние обработки выдается в виде '6A88'. Это происходит либо по той причине, что ключ сеанса еще не создан, или по той, что ключ сеанса больше недействителен (в этом случае интерфейс должен повторить процесс взаимной аутентификации в целях генерации нового ключа сеанса).
- ♦ Если некоторые ожидаемые объекты данных (как указано выше) в формате криптозащищенного обмена данными отсутствуют, состояние обработки выдается в виде '6987': эта ошибка имеет место в том случае, если ожидаемая метка отсутствует или если основная часть команды составлена неправильно.
- ♦ Если некоторые объекты неправильны, состояние обработки выдается в виде '6988': эта ошибка имеет место в том случае, если требуемые метки есть, но длина некоторых из них отличается от ожидаемой длины.

- ♦ Если проверка криптографической контрольной суммы показала неправильный результат, состояние обработки выдается в виде '6688'.

3.6.3 Update Binary (обновление данных)

Эта команда соответствует стандарту ISO/IEC 7816-4, однако ее использование ограничено по сравнению с командой, определенной в указанном стандарте.

Командное сообщение UPDATE BINARY начинает обновление (стирание + запись) битов, которые уже присутствуют в данных файла EF с помощью битов, содержащихся в команде APDU.

TCS_331 Эта команда может выполняться в том случае, если состояние защиты удовлетворяет атрибутам защиты, определенным для EF и функции UPDATE (если контроль доступа к безопасной функции UPDATE включает PRO SM, в команду должен быть включен элемент защиты данных).

3.6.3.1 Команда, передаваемая в некриптозащищенном виде

Эта команда позволяет интерфейсу записывать данные в выбранный в данный момент элементарный файл без проверки целостности полученных данных карточкой. Этот обычный режим допускается только в том случае, если соответствующий файл не содержит отметку "Encrypted".

TCS_332 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	Запрос на криптозащищенный обмен данными отсутствует
INS	1	'D6h'	
P1	1	'XXh'	Смещение байтов с начала файла: байт самого старшего разряда
P2	1	'XXh'	Смещение байтов с начала файла: байт самого младшего разряда
Lc	1	'NNh'	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_333 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- ♦ Если команда проходит, карточка выдает **'9000'**.
- ♦ Если элементарный файл не выбран, состояние обработки выдается в виде **'6986'**.
- ♦ Если параметры контроля доступа к выбранному файлу не удовлетворены, передача команды прерывается и выдается в виде **'6982'**.
- ♦ Если сдвиг не соответствует размеру элементарного файла (сдвиг > размера EF), состояние обработки выдается в виде **'6B00'**.
- ♦ Если размер данных, подлежащих записи, не соответствует размеру элементарного файла (сдвиг + Lc > размера EF), состояние обработки выдается в виде **'6700'**.
- ♦ Если в атрибутах файла обнаружена ошибка целостности, карточка считает файл поврежденным и невозстанавливаемым, и состояние обработки выдается в виде **'6400'** или **'6500'**.
- ♦ Если при записи произошел сбой, состояние обработки выдается в виде **'6581'**.

3.6.3.2 Команда, передаваемая в криптозащищенном виде

Эта команда позволяет интерфейсу записывать данные в элементарный файл, выбранный в данный момент, с проверкой целостности полученных данных карточкой. Поскольку требование конфиденциальности отсутствует, данные не шифруются.

TCS_334 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'0Ch'	Криптозащищенный обмен сообщениями. Запрос
INS	1	'D6h'	INS
P1	1	'XXh'	Сдвиг в байтах от начала файла: Байт самого старшего разряда
P2	1	'XXh'	Сдвиг в байтах от начала файла: Байт самого младшего разряда
Lc	1	'XXh'	Длина поля защищенных данных
#6	1	'81h'	T_{PV} : Метка, указывающая на значение обычных данных
#7	L	'NNh' or '81 NNh'	L_{PV} : Длина переданных данных. L равно 2 байтам, если $L_{PV} > 127$ байтов
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Значение обычных данных (Данные, подлежащие записи)
#(7+L+NN)	1	'8Eh'	T_{CC} : Метка, указывающая на криптографическую контрольную сумму
#(8+L+NN)	1	'04h'	L_{CC} : Длина следующей криптографической контрольной суммы
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	Криптографическая контрольная сумма (4 байта самого старшего разряда)
Le	1	'00h'	Как указано в стандарте ISO/IEC 7816-4

TCS_335 Ответное сообщение, если входной формат криптозащищенного обмена данными правильный

Байт	Длина	Значение	Описание
#1	1	'99h'	T_{SW} : Метка, указывающая на слова состояния (должна быть защищена с помощью криптографической суммы)
#2	1	'02h'	L_{SW} : Длина переданных обратно слов состояния
#3-#4	2	'XXXXh'	Слова состояния (SW1, SW2)
#5	1	'8Eh'	T_{CC} : Метка, указывающая на слова состояния
#6	1	'04h'	L_{CC} : Длина следующей криптографической контрольной суммы
#7-#10	4	'XX..XXh'	Криптографическая контрольная сумма (4 байта самого старшего разряда)
SW	2	'XXXXh'	Слова состояния (SW1, SW2)

Данные о состояниях "нормальной" обработки, описанные для команды UPDATE BINARY, передаваемой в некриптозащищенном виде (см. пункт 3.6.3.1), могут возвращаться с использованием структур ответного сообщения, описанного выше.

Кроме того, могут иметь место некоторые ошибки, которые конкретно связаны с криптозащищенным обменом сообщениями. В этом случае данные о состоянии обработки просто возвращаются, не задействуя использованную структуру защиты данных:

TCS_336 Ответное сообщение в случае ошибки в криптозащищенном обмене сообщениями

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- ◆ Если ключ текущего сеанса отсутствует, состояние обработки выдается в виде **'6A88'**.
- ◆ Если некоторые ожидаемые объекты данных (как указано выше) в формате криптозащищенного обмена сообщениями отсутствуют, состояние обработки выдается в виде **'6987'**: эта ошибка происходит в том случае, если отсутствует метка или если основная часть команды построена неправильно.
- ◆ Если некоторые объекты данных неправильны, состояние обработки выдается в виде **'6988'**: эта ошибка имеет место в том случае, если все требуемые метки есть, но длина некоторых из них отличается от ожидаемой длины.
- ◆ Если проверка криптографической контрольной суммы дала неправильные результаты, состояние обработки выдается в виде **'6688'**.

3.6.4 Get Challenge (получение запроса)

Эта команда соответствует стандарту ISO/IEC 7816-4, однако ее использование по сравнению с командой, определенной в указанном стандарте, ограничено.

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_337 Запрос, выданный карточкой, действителен только для следующей команды, которая использует запрос, переданный карточке.

TCS_338 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (Длина ожидаемого запроса).

TCS_339 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#8	8	'XX..XXh'	Запрос
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- ◆ Если команда проходит, карточка выдает **'9000'**.
- ◆ Если Le отличается от '08h', то состояние обработки выдается в виде **'6700'**.
- ◆ Если параметры P1-P2 неправильны, состояние обработки выдается в виде **'6A86'**.

3.6.5 Verify (проверка)

Эта команда соответствует стандарту ISO/IEC 7816-4, однако ее использование по сравнению с командой, определенной в указанном стандарте, ограничено.

Команда Verify инициирует сравнение на уровне карточки между переданными данными CHV (PIN) и исходными данными CHV, записанными на карточке.

Примечание: PIN, введенный пользователем, должен быть заполнен интерфейсом с правой стороны байтами 'FFh' до достижения длины 8 байтов.

TCS_340 Если команда проходит, права отображения CHV открываются и счетчик оставшихся попыток CHV выставляется на ноль.

TCS_341 Сравнение, которое дало неправильные результаты, регистрируется в карточке с целью ограничить число дальнейших попыток использования исходных данных CHV.

TCS_342 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
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_343 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояние (SW1,SW2)

- ◆ Если команда не проходит, карточка выдает '9000'.
- ◆ Если исходные данные CHV не найдены, состояние обработки выдается в виде '6A88'.
- ◆ Если данные CHV заблокированы (счетчик оставшихся попыток CHV показывает ноль), состояние обработки выдается в виде '6983'. В этом состоянии данные CHV больше никогда не принимаются.
- ◆ Если сравнение дало неправильные результаты, показание счетчика оставшихся попыток уменьшается и статус обработки выдается в виде '63CX' (X > 0 и X равно показанию счетчика оставшихся попыток CHV. Если X = 'F', то показания счетчика попыток CHV больше 'F').

- ◆ Если исходные данные CHV считаются поврежденными, состояние обработки выдается в виде **'6400'** или **'6581'**.

3.6.6 Get Respons (получение ответа)

Эта команда соответствует стандарту ISO/IEC 7816-4.

Эта команда (необходимая и доступная только для протокола T = 0) используется для передачи подготовленных данных с карточки на интерфейс (случай, когда команда включает 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_344 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_345 Ответное сообщение

Байт	Длина	Значение	Описание
#1-#X	X	'XX..XXh'	Данные
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- ◆ Если команда проходит, карточка выдает **'9000'**.
- ◆ Если данные карточкой подготовлены не были, состояние обработки выдается в виде **'6900'** или **'6F00'**.
- ◆ Если длина байта превышает число имеющихся байтов или если Le равно нулю, то состояние обработки выдается в виде **'6Cxx'**, где xx указывает на точное число имеющихся байтов. В этом случае подготовленные данные все еще доступны для следующей команды GET_RESPONSE.

- ◆ Если длина байта Le не равна нулю и меньше, чем число имеющихся байтов, то требуемые данные нормально передаются карточкой, а состояние обработки выдается в виде '61xx', где 'xx' указывает число дополнительных байтов, все еще имеющихся для выполнения следующей команды GET_RESPONSE.
- ◆ Если команда не поддерживается (протокол T=1), карточка выдает '6D00'.

3.6.7 PSO: Verify Certificate (проверка сертификата)

Эта команда соответствует стандарту ISO/IEC 7816-8, однако ее использование по сравнению с командой, определенной в указанном стандарте, ограничено.

Команда VERIFY CERTIFICATE используется карточкой для получения открытого ключа извне и проверки его действительности.

TCS_346 Если команда VERIFY CERTIFICATE проходит, открытый ключ записывается для будущего использования в среде защиты. Этот ключ должен прямо конфигурироваться для использования команд, связанных с защитой (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE или VERIFY CERTIFICATE) с помощью команды MSE (см. пункт 3.6.10), использующей идентификатор этого ключа.

TCS_347 В любом случае команда VERIFY CERTIFICATE использует открытый ключ, ранее выбранный командой MSE для открытия сертификата. Открытый ключ должен быть ключом одной из Договаривающихся сторон.

TCS_348 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Выполнение операции по защите
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 подразделе 11)

TCS_349 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- ◆ Если команда проходит, карточка выдает **'9000'**.
- ◆ Если проверка сертификата дает неправильные результаты, состояние обработки выдается в виде **'6688'**. Процесс проверки и расшифровки сертификата описывается в подразделе 11.
- ◆ Если открытый ключ среды защиты отсутствует, выдается **'6A88'**.
- ◆ Если выбранный открытый ключ (используемый для расшифровки сертификата) считается поврежденным, состояние обработки выдается в виде **'6400'** или **'6581'**.
- ◆ Если параметр выбранного открытого ключа (используемого для расшифровки сертификата) CHA.LSB (CertificateHolderAuthorisation.equipmentType) отличается от '00' (т.е. не является ключом какой-либо Договаривающейся стороны), состояние обработки выдается в виде **'6985'**.

3.6.8 Internal Authenticate (внутренняя аутентификация)

Эта команда соответствует стандарту ISO/IEC 7816-4.

Используя команду INTERNAL AUTHENTICATE, интерфейс может произвести аутентификацию карточки.

Процесс аутентификации описывается в подразделе 11. Он включает следующие сообщения:

TCS_350 Команда INTERNAL AUTHENTICATE использует закрытый ключ (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 подразделе 11).

TCS_351 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. подраздел 11)
Le	1	'80h'	Длина данных, ожидаемых от карточки

TCS_352 Ответ на сообщение

Байт	Длина	Значение	Описание
#1-#128	128	'XX..XXh'	Маркер аутентификации карточки (см. подраздел 11)
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- ◆ Если команда проходит, карточка выдает **'9000'**.
- ◆ Если в среде защиты присутствует открытый ключ, состояние обработки дается в виде **'6A88'**.
- ◆ Если в среде защиты присутствует закрытый ключ, состояние обработки выдается в виде **'6A88'**.
- ◆ Если VU.CHR не соответствует данному идентификатору открытого ключа, состояние обработки выдается в виде **'6A88'**.
- ◆ Если выбранный закрытый ключ считается поврежденным, состояние обработки выдается в виде **'6400'** или **'6581'**.

TCS_353 Если команда INTERNAL_AUTHENTICATE проходит, ключ текущего сеанса, если он существует, стирается и для создания нового ключа сеанса больше не доступен. Для создания нового ключа сеанса команда EXTERNAL_AUTHENTICATE должна быть выполнена.

3.6.9 External Authenticate (внешняя аутентификация)

Эта команда соответствует стандарту ISO/IEC 7816-4.

Используя команду EXTERNAL AUTHENTICATE, карточка может произвести аутентификацию интерфейса.

Процесс аутентификации излагается в подразделе 11. Он включает следующие сообщения:

TCS_354 Команда GET CHALLENGE должна предшествовать непосредственно команде EXTERNAL_AUTHENTICATE. Карточка выдает запрос во внешнюю среду (RND3).

TCS_355 Для проверки криптограммы используется RND3 (запрос, выданный карточкой), закрытый ключ карточки (выбранный по косвенным признакам) и открытый ключ, выбранный ранее по команде MSE.

TCS_356 Карточка проверяет криптограмму и, если она правильная, открывается условие доступа AUT (на подтверждение).

TCS_357 Входная криптограмма передает второй элемент K2, указывающий на соответствие ключа сеанса.

TCS_358 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (открытый ключ, который должен использоваться, по косвенным признакам известен и был создан по команде MSE)
Lc	1	'80h'	Lc (длина данных, переданных на карточку)
#6-#133	128	'XX..XXh'	Криптограмма (см. подраздел 11)

TCS_359 Ответ на сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова статуса (SW1,SW2)

- ◆ Если команда проходит, карточка выдает **'9000'**.
- ◆ Если открытый ключ в среде защиты отсутствует, выдается **'6A88'**.
- ◆ Если СНА выбранного открытого ключа не соответствует соединению AID приложения тахографа и типа БУ, состояние обработки выдается в виде **'6F00'** (см. подраздел 11).
- ◆ Если в среде защиты закрытый ключ отсутствует, состояние обработки выдается в виде **'6A88'**.
- ◆ Если проверка криптограммы дала неправильные результаты, состояние обработки выдается в виде **'6688'**.
- ◆ Если этой команде не предшествует непосредственно команда GET CHALLENGE, состояние обработки выдается в виде **'6985'**.
- ◆ Если выбранный закрытый ключ считается поврежденным, состояние обработки выдается в виде **'6400'** или **'6581'**.

TCS_360 Если команда EXTERNAL AUTHENTICATE проходит и если доступ к первой части ключа сеанса в результате выполненной перед этим команды INTERNAL AUTHENTICATE есть, ключ сеанса готов для выполнения будущих команд по процедуре криптозащищенного обмена сообщениями.

TCS_361 Если по предыдущей команде INTERNAL AUTHENTICATE первая часть ключа сеанса не доступна, вторая часть ключа сеанса, переданная интерфейсом, в карточке не регистрируется. Этот механизм обеспечивает осуществление процесса взаимной аутентификации в порядке, указанном в подразделе 11.

3.6.10 *Manage Security Environment (управление средой защиты)*

Эта команда используется для определения открытого ключа в целях аутентификации.

Эта команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению с указанным стандартом ограничено.

TCS_362 Ключ, указанный в поле данных MSE, действителен для каждого файла DF тахографа.

TCS_363 Ключ, указанный в поле данных MSE, продолжает оставаться действующим открытым ключом до следующей правильной команды MSE.

TCS_364 Если указанный ключ в карточке еще не указан, среда защиты не меняется.

TCS_365 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	08h	'XX..XXh'	Идентификатор ключа, определенный в подразделе 11

TCS_366 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- ◆ Если команда проходит, карточка выдает '9000'.

- ◆ Если указанный ключ в карточке отсутствует, состояние обработки выдается в виде **‘6A88’**.
- ◆ Если некоторые ожидаемые объекты данных в формате криптозащищенного обмена сообщениями отсутствуют, состояние обработки выдается в виде **‘6987’**. Это может произойти, если отсутствует метка **‘83h’**.
- ◆ Если некоторые объекты данных неправильны, состояние обработки выдается в виде **‘6988’**. Это может произойти в том случае, если длина идентификатора ключа не соответствует **‘08h’**.
- ◆ Если выбранный ключ считается поврежденным, состояние обработки выдается в виде **‘6400’** и **‘6581’**.

3.6.11 *PSO: Hash (хеширование)*

Эта команда используется для передачи карточке результата расчета хеширования некоторых данных. Она используется для проверки цифровых подписей. Значение хеширования хранится в памяти EEPROM для следующей команды на проверку цифровой подписи.

Эта команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению с указанным стандартом ограничено.

TCS_367 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Выполнение операций по защите
P1	1	‘90h’	Возврат хеш-кода
P2	1	‘A0h’	Метка: поле данных содержит объекты данных, относящиеся к хешированию
Lc	1	‘16h’	Длина байта Lc последующего поля данных
#6	1	‘90h’	Метка, указывающая на хеш-код
#7	1	‘14h’	Длина хеш-кода
#8-#27	20	‘XX..XXh’	Хеш-код

TCS_368 **Ответное на сообщение**

Байт	Длина	Значение	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- ◆ Если команда проходит, карточка выдает **'9000'**.
- ◆ Если некоторые ожидаемые объекты данных (как указано выше) отсутствуют, состояние обработки выдается в виде **'6987'**. Это происходит в том случае, если одна из меток '90h' отсутствует.
- ◆ Если некоторые объекты данных неправильны, состояние обработки выдается в виде **'6988'**. Эта ошибка имеет место в том случае, если требуемая метка присутствует, но ее длина отличается от '14h'.

3.6.12 Perform Hash of File (хеширование файла)

Эта команда не соответствует стандарту ISO/IEC 7816-8. Поэтому байт CLA этой команды указывает на эксклюзивное использование команды PERFORM SECURITY OPERATION / HASH.

TCS_369 Команда PERFORM HASH FILE используется для хеширования зоны данных выбранного в данный момент транспарентного элементарного файла.

TCS_370 Результат операции хеширования регистрируется на карточке. Он может затем использоваться для получения цифровой подписи файла с использованием команды PSO-COMPUTE_DIGITAL_SIGNATURE. Этот результат остается доступным для команды COMPUTE DIGITAL SIGNATURE до следующей выполненной команды PERFORM HASH OF FILE.

TCS_371 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'80h'	CLA
INS	1	'2Ah'	Выполнение операций по защите
P1	1	'90h'	Метка: хеширование
P2	1	'00h'	P2: хеширование данных выбранного в данный момент транспарентного файла

TCS_372 Ответное сообщение

Байт	Длина	Значение	Описание
SW	2	'XXXh'	Слова состояния (SW1,SW2)

- ◆ Если команда проходит, карточка выдает '9000'.
- ◆ Если приложение не выбрано, состояние обработки выдается в виде '6985'.
- ◆ Если выбранный элементарный файл считается поврежденным (ошибки в атрибутах файла или целостности записанных данных), состояние обработки выдается в виде '6400' или '6581'.
- ◆ Если выбранный файл является транспарентным файлом, состояние обработки выдается в виде '6986'.

3.6.13 PSO: Compute Digital Signature (расчет цифровой подписи)

Эта команда используется для расчета цифровой подписи ранее рассчитанного хеш-кода (см. ХЕШИРОВАНИЕ ФАЙЛА, пункт 3.6.12).

Эта команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению с указанным стандартом ограничено.

TCS_373 Закрытый ключ карточки используется для расчета цифровой подписи и известен карточке по косвенным признакам.

TCS_374 Карточка производит цифровую подпись с использованием метода заполнения, соответствующего PKCS1 (более подробно см. подраздел 11).

TCS_375 Командное сообщение

Байт	Длина	Значения	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Осуществление операции защиты
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	'80h'	Длина ожидаемой подписи

TCS_376 **Ответное сообщение**

Байт	Длина	Значения	Описание
#1-#128	128	'XX..XXh'	Подпись ранее рассчитанного хеширования
SW	2	'XXXXh'	Слова состояний (SW1,SW2)

- ◆ Если команда проходит, карточка выдает **'9000'**.
- ◆ Если выбранный закрытый ключ считается по косвенным признакам поврежденным, состояние обработки выдается в виде **'6400'** или **'6581'**.

3.6.14 PSO: Verify Digital Signature (проверка цифровой подписи)

Данная команда используется для проверки цифровой подписи, представленной в качестве входных данных в соответствии с параметром PKCS1 сообщения, хеш-код которой карточке известен. Алгоритм подписи известен карточке по косвенным признакам.

Эта команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению с указанным стандартом ограничено.

TCS_377 Команда Verify Digital Signature всегда использует открытый ключ, выбранный на основании предыдущей команды Manage Security Environment, а предыдущий хеш-код вносится командой PSO: Hash (хеширование).

TCS_378 **Командное сообщение**

Байт	Длина	Значения	Описание
CLA	1	'00h'	CLA
INS	1	'2Ah'	Осуществление операций защиты
P1	1	'00h'	
P2	1	'A8h'	Метка: поле данных содержит объекты данных, относящиеся к проверке
Lc	1	'83h'	Длина Lc последующего поля данных
#28	1	'9Eh'	Метка, указывающая на цифровую подпись
#29-#30	2	'8180h'	Длина цифровой подписи (128 байтов, закодированных в соответствии со стандартом ISO/IEC 7816-6)
#31-#158	128	'XX..XXh'	Содержание цифровой подписи

TCS_379 Ответное сообщение

Байт	Длина	Значения	Описание
SW	2	'XXXXh'	Слова состояния (SW1,SW2)

- ◆ Если команда проходит, карточка выдает **'9000'**.
- ◆ Если проверка подписи дает неправильные результаты, состояние обработки выдается в виде **'6688'**. Процесс проверки описан в подразделе 11.
- ◆ Если открытый ключ не выбран, состояние обработки выдается в виде **'6A88'**.
- ◆ Если некоторые ожидаемые объекты данных (как указано выше) отсутствуют, состояние обработки выдается в виде **'6987'**. Это может произойти в том случае, если одна из требуемых меток отсутствует.
- ◆ Если хеш-кода для обработки команды нет (в результате предыдущей команды на хеширование), состояние обработки выдается в виде **'6985'**.
- ◆ Если некоторые объекты данных неправильные, состояние обработки выдается в виде **'6988'**. Это может произойти в том случае, если требуемая длина объектов данных неправильна.
- ◆ Если выбранный открытый ключ считается поврежденным, состояние обработки выдается в виде **'6400'** или **'6581'**.

4. Структура карточек тахографа

В настоящем пункте уточняются структуры файлов карточек тахографа для хранения доступных данных.

В нем не указываются внутренние структуры, определяемые по усмотрению изготовителя, такие, как заголовки файлов, а также элементы хранения и обработки данных, необходимые только для внутреннего пользования, например, EuropeanPublicKey, CardPrivateKey, TDesSessionKey или WorkshopCardPin.

Полезный объем хранения данных на карточках тахографа должен составлять не менее 11 килобайт. Допускается использование большего объема. В таком случае структура карточки остается той же, однако число записей некоторых элементов структуры

увеличивается. В этом пункте указываются минимальные и максимальные значения этого количества записей.

4.1 Структура карточки водителя

TCS_400 После ее персонализации карточка водителя должна иметь следующую постоянную структуру файла и условия доступа к файлам:

Файл	ИД файла	Условия доступа		
		Чтение	Обновление	Зашифрованный
MF	3F00			
├─ EF ICC	0002	ALW	NEV	Нет
├─ EF IC	0005	ALW	NEV	Нет
└─ DF Tachograph	0500			
├─ EF Application_Identification	0501	ALW	NEV	Нет
├─ EF Card_Certificate	C100	ALW	NEV	Нет
├─ EF CA_Certificate	C108	ALW	NEV	Нет
├─ EF Identification	0520	ALW	NEV	Нет
├─ EF Card_Download	050E	ALW	ALW	Нет
├─ EF Driving_Licence_Info	0521	ALW	NEV	Нет
├─ EF Events_Data	0502	ALW	PRO SM / AUT	Нет
├─ EF Faults_Data	0503	ALW	PRO SM / AUT	Нет
├─ EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Нет
├─ EF Vehicles_Used	0505	ALW	PRO SM / AUT	Нет
├─ EF Places	0506	ALW	PRO SM / AUT	Нет
├─ EF Current_Usage	0507	ALW	PRO SM / AUT	Нет
├─ EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Нет
└─ EF Specific_Conditions	0522	ALW	PRO SM / AUT	Нет

TCS_401 Все структуры элементарных файлов должны быть прозрачными.

TCS_402 Чтение криптозащищенных данных должно быть возможным для всех файлов тахографа типа DF.

TCS_403 Карточка водителя должна иметь следующую структуру данных:

Файл/Элемент данных	Число записей	Размер (байты)		Значения по умолчанию
		мин.	макс.	
MF		11411	24959	
└─ 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}
└─ 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 ₁	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		576	1152	
└─┬ CardFaultData		576	1152	
└─┬└ cardFaultRecords	2	288	576	
└─┬└└ CardFaultRecord	n ₂	24	24	
└─┬└└└ faultType		1	1	{00}
└─┬└└└ faultBeginTime		4	4	{00..00}
└─┬└└└ faultEndTime		4	4	{00..00}
└─┬└└└ faultVehicleRegistration				
└─┬└└└└ vehicleRegistrationNation		1	1	{00}
└─┬└└└└ vehicleRegistrationNumber		14	14	{00, 0..20}
─ EF Driver_Activity_Data		5548	13780	
└─┬ CardDriverActivity		5548	13780	
└─┬└ activityPointerOldestDayRecord		2	2	{00 00}
└─┬└ activityPointerNewestRecord		2	2	{00 00}
└─┬└ activityDailyRecords	n ₆	5544	13776	{00..00}
─ EF Vehicles_Used		2606	6202	
└─┬ CardVehiclesUsed		2606	6202	
└─┬└ vehiclePointerNewestRecord		2	2	{00 00}
└─┬└ cardVehicleRecords		2604	6200	
└─┬└└ CardVehicleRecord	n ₃	31	31	
└─┬└└└ vehicleOdometerBegin		3	3	{00..00}
└─┬└└└ vehicleOdometerEnd		3	3	{00..00}
└─┬└└└ vehicleFirstUse		4	4	{00..00}
└─┬└└└ vehicleLastUse		4	4	{00..00}
└─┬└└└ vehicleRegistration				
└─┬└└└└ vehicleRegistrationNation		1	1	{00}
└─┬└└└└ vehicleRegistrationNumber		14	14	{00, 20..20}
└─┬└└└ vuDataBlockCounter		2	2	{00 00}
─ EF Places		841	1121	
└─┬ CardPlaceDailyWorkPeriod		841	1121	
└─┬└ placePointerNewestRecord		1	1	{00}
└─┬└ placeRecords		840	1120	
└─┬└└ PlaceRecord	n ₄	10	10	
└─┬└└└ entryTime		4	4	{00..00}
└─┬└└└ entryTypeDailyWorkPeriod		1	1	{00}
└─┬└└└ dailyWorkPeriodCountry		1	1	{00}
└─┬└└└ dailyWorkPeriodRegion		1	1	{00}
└─┬└└└ vehicleOdometerValue		3	3	{00..00}
─ EF Current_Usage		19	19	
└─┬ CardCurrentUse		19	19	
└─┬└ sessionOpenTime		4	4	{00..00}
└─┬└ sessionOpenVehicle				
└─┬└└ vehicleRegistrationNation		1	1	{00}
└─┬└└ vehicleRegistrationNumber		14	14	{00, 20..20}
─ EF Control_Activity_Data		46	46	

└─ CardControlActivityDataRecord	46	46	
└─ controlType	1	1	{00}
└─ controlTime	4	4	{00..00}
└─ controlCardNumber			
└─ cardType	1	1	{00}
└─ CardIssuingMemberState	1	1	{00}
└─ cardNumber	16	16	{20..20}
└─ controlVehicleRegistration			
└─ vehicleRegistrationNation	1	1	{00}
└─ vehicleRegistrationNumber	14	14	{00, 20..20}
└─ controlDownloadPeriodBegin	4	4	{00..00}
└─ controlDownloadPeriodEnd	4	4	{00..00}
└─ EF Specific_Conditions	280	280	
└─ SpecificConditionRecord	56	5	5
└─ entryTime	4	4	{00..00}
└─ SpecificConditionType	1	1	{00}

TCS_404 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения количества записей, которые должны использоваться в структуре данных карточки водителя:

		мин.	макс.
n ₁	NoOfEventsPerType	6	12
n ₂	NoOfFaultsPerType	12	24
n ₃	NoOfCardVehicleRecords	84	200
n ₄	NoOfCardPlaceRecords	84	112
n ₆	CardActivityLengthRange	5 544 байта (28 дней * 93 изменения вида деятельности)	13 776 байт (28 дней * 240 изменений вида деятельности)

4.2 Структура карточки мастерской

TCS_405 После персонализации карточка мастерской должна иметь следующую постоянную структуру файлов и условия доступа к файлам:

Файл	ИД файла	Условия доступа		
		Чтение	Обновление	Зашифрованный
MF	3F00			
└─ EF ICC	0002	ALW	NEV	Нет
└─ EF IC	0005	ALW	NEV	Нет
└─ DF Tachograph	0500			
└─ EF Application_Identification	0501	ALW	NEV	Нет
└─ EF Card_Certificate	C100	ALW	NEV	Нет
└─ EF CA_Certificate	C108	ALW	NEV	Нет
└─ EF Identification	0520	ALW	NEV	Нет

EF Card_Download	0509	ALW	ALW	Нет
EF Calibration	050A	ALW	PRO SM / AUT	Нет
EF Sensor_Installation_Data	050B	ALW	NEV	Да
EF Events_Data	0502	ALW	PRO SM / AUT	Нет
EF Faults_Data	0503	ALW	PRO SM / AUT	Нет
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Нет
EF Vehicles_Used	0505	ALW	PRO SM / AUT	Нет
EF Places	0506	ALW	PRO SM / AUT	Нет
EF Current_Usage	0507	ALW	PRO SM / AUT	Нет
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Нет
EF Specific_Conditions	0522	ALW	PRO SM / AUT	Нет

TCS_406 Все структуры элементарных файлов должны быть транспарентными.

TCS_407 Чтение криптозащищенных данных должно быть возможным для всех файлов тахографа типа DF.

TCS_408 Карточка мастерской должна иметь следующую структуру данных:

Файл/Элемент данных	Число записей		Размер (байты)		Значение по умолчанию
	мин.	макс.	мин.	макс.	
MF			11088	29061	
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}
DF Tachograph			11055	29028	
EF Application_Identification			11	11	
└ WorkshopCardApplicationIdentification			11	11	
└└ typeOfTachographCardId			1	1	{00}
└└ cardStructureVersion			2	2	{00 00}
└└ noOfEventsPerType			1	1	{00}
└└ noOfFaultsPerType			1	1	{00}
└└ activityStructureLength			2	2	{00 00}
└└ noOfCardVehicleRecords			2	2	{00 00}
└└ noOfCardPlaceRecords			1	1	{00}
└└ noOfCalibrationRecords			1	1	{00}
EF Card_Certificate			194	194	
└ CardCertificate			194	194	{00..00}
EF CA_Certificate			194	194	
└ MemberStateCertificate			194	194	{00..00}

EF Identification		211	211	
CardIdentification		65	65	
CardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		146	146	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		2	2	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		9243	26778	
WorkshopCardCalibrationData		9243	26778	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		9240	26775	
WorkshopCardCalibrationRecord	n ₅	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	n ₁	24	24	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

EF Faults_Data		288	288	
└─ CardFaultData		288	288	
└─┬─ cardFaultRecords	2	144	144	
└─┬─┬─ CardFaultRecord	n ₂	24	24	
└─└─┬─ faultType		1	1	{00}
└─└─┬─ faultBeginTime		4	4	{00..00}
└─└─┬─ faultEndTime		4	4	{00..00}
└─└─┬─ faultVehicleRegistration				
└─└─└─ vehicleRegistrationNation		1	1	{00}
└─└─└─ vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		202	496	
└─ CardDriverActivity		202	496	
└─┬─ activityPointerOldestDayRecord		2	2	{00 00}
└─┬─ activityPointerNewestRecord		2	2	{00 00}
└─┬─ activityDailyRecords	n ₆	198	492	{00..00}
EF Vehicles_Used		126	250	
└─ CardVehiclesUsed		126	250	
└─┬─ vehiclePointerNewestRecord		2	2	{00 00}
└─┬─ cardVehicleRecords		124	248	
└─┬─┬─ CardVehicleRecord	n ₃	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	n ₄	10	10	
└─└─┬─ entryTime		4	4	{00..00}
└─└─┬─ entryTypeDailyWorkPeriod		1	1	{00}
└─└─┬─ dailyWorkPeriodCountry		1	1	{00}
└─└─┬─ dailyWorkPeriodRegion		1	1	{00}
└─└─┬─ vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		19	19	
└─ CardCurrentUse		19	19	
└─┬─ sessionOpenTime		4	4	{00..00}
└─┬─ sessionOpenVehicle				
└─└─ vehicleRegistrationNation		1	1	{00}
└─└─ vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
└─ CardControlActivityDataRecord		46	46	
└─┬─ controlType		1	1	{00}
└─┬─ controlTime		4	4	{00..00}
└─┬─ controlCardNumber				
└─└─ cardType		1	1	{00}
└─└─ CardIssuingMemberState		1	1	{00}
└─└─ cardNumber		16	16	{20..20}

controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		10	10	
SpecificConditionRecord	2	5	5	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_409 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения количества записей, которые должны использоваться в структуре данных карточки мастерской:

		мин.	макс.
n ₁	NoOfEventsPerType	3	3
n ₂	NoOfFaultsPerType	6	6
n ₃	NoOfCardVehicleRecords	4	8
n ₄	NoOfCardPlaceRecords	6	8
n ₅	NoOfCalibrationRecords	88	255
n ₆	CardActivityLengthRange	198 байт (1 день * 93 изменения вида деятельности)	492 байта (1 день * 240 изменений вида деятельности)

4.3 Структура карточки контролера

TCS_410 После персонализации карточка контролера должна иметь следующую постоянную структуру файлов и условия доступа к файлам:

Файл	ИД файла	Условия доступа		
		Чтение	Обновление	Зашифрованный
MF	3F00			
EF ICC	0002	ALW	NEV	Нет
EF IC	0005	ALW	NEV	Нет
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Нет
EF Card_Certificate	C100	ALW	NEV	Нет
EF CA_Certificate	C108	ALW	NEV	Нет
EF Identification	0520	AUT	NEV	Нет
EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	Нет

TCS_411 Все структуры элементарных файлов должны быть транспарентными.

TCS_412 Чтение криптозащищенных данных должно быть возможным для всех файлов тахографа типа DF.

TCS_413 Карточка контролера должна иметь следующую структуру данных:

Файл/Элемент данных	Число записей		Размер (байты)		Значение по умолчанию
	мин.	макс.	мин.	макс.	
MF	11219	24559			
└─ 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}
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			

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_414 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения количества записей, которые должны использоваться в структуре данных карточки контролера:

		мин.	макс.
n7	NoOfControlActivityRecords	230	520

4.4 Структура карточки предприятия

TCS_415 После персонализации карточка предприятия должна иметь следующую постоянную структуру файлов и условия доступа к файлам:

Файл	ИД файла	Условия доступа		
		Чтение	Обновление	Зашифрованный
MF	3F00			
EF ICC	0002	ALW	NEV	Нет
EF IC	0005	ALW	NEV	Нет
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Нет
EF Card_Certificate	C100	ALW	NEV	Нет
EF CA_Certificate	C108	ALW	NEV	Нет
EF Identification	0520	AUT	NEV	Нет
EF Company_Activity_Data	050D	ALW	PRO SM/AUT	Нет

TCS_416 Все структуры элементарных файлов должны быть транспарентными.

TCS_417 Чтение криптозащищенных данных должно быть возможным для всех файлов тахографа типа DF.

TCS_418 Карточка предприятия должна иметь следующую структуру данных:

Файл/Элемент данных	Число записей	Размер (байты)		Значение по умолчанию
		мин.	макс.	
MF		11147	24487	
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}
DF Tachograph		11114	24454	
EF Application_Identification		5	5	
CompanyCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF Card_Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		139	139	
CardIdentification		65	65	
CardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		74	74	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		10582	23922	
CompanyActivityData		10582	23922	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		10580	23920	
companyActivityRecord	n8	46	46	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_419 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения количества записей, которые должны использоваться в структуре данных карточки мастерской:

		мин.	макс.
n ₈	NoOfCompanyActivityRecords	230	520

ПОДРАЗДЕЛ III ПИКТОГРАММЫ

PIС_001 В контрольном устройстве могут использоваться следующие пиктограммы и их комбинации:

Основные пиктограммы

<u>Люди</u>	<u>Действия</u>	<u>Режимы работы</u>
▣	Предприятие	Режим предприятия
▣	Контролер Контроль	Режим контроля
⊖	Водитель Управление	Рабочий режим
Т	Мастерская/пункт техконтроля	Инспекция/калибровка
⊞	Изготовитель	Режим калибровки

<u>Виды деятельности</u>	<u>Периоды времени</u>
⊞	Готовность Текущий период готовности
⊖	Управление Время непрерывного управления
⊞	Отдых Текущий период отдыха
⊞	Работа Текущий период работы
⊞	Перерыв Совокупная продолжительность перерывов
?	Нет данных

<u>Аппаратура</u>	<u>Функции</u>	
1	Считывающее устройство для карточки водителя	
2	Считывающее устройство для карточки второго водителя	
▣	Карточка	
⊖	Часы	
□	Дисплей Индикация	
⊞	Внешний носитель данных	Загрузка
⊞	Источник питания	
⊞	Печатающее устройство/распечатка	Печать
Л	Датчик	

- Размер шин
- Д Транспортное средство/бортовое устройство

Особые ситуации

- OUT Неприменимо
- ⚠ Переезд на пароме/поезде

Разное

- ! События ✕ Неисправности
- ▶ Начало ежедневного периода работы ◀ Конец ежедневного периода работы
- Географический пункт
- М Ручной ввод данных
о деятельности водителя
- 🔒 Защита
- Скорость
- ⌚ Время
- Σ Суммарные/сводные данные

Периодичность

- 24h Ежедневно
- I Еженедельно
- II За две недели
- + С ... до ...

Комбинации пиктограмм

Разное

- ▣ • Пункт контроля
- ▶ Пункт начала ежедневного периода работы ◀ • Пункт ежедневного периода работы
- ⌚ + С ... + ⌚ Время: до ...
- Д + С транспортного средства
- OUT + Начало ситуации "неприменимо" + OUT Конец ситуации "неприменимо"

Карточки

- ⊗■ Карточка водителя
- ⊗■ Карточка предприятия
- ⊗■ Карточка контролера
- ⊗■ Карточка мастерской
- - - - Карточка не введена

Управление

- ⊗⊗ Управление осуществляется экипажем
- ⊗| Время управления за одну неделю
- ⊗|| Время управления за две недели

Распечатка данных

- 24h■⊗ Распечатка сохраненных на карточке данных о деятельности водителя за сутки
- 24h■⊗ Распечатка сохраненных в БУ данных о деятельности водителя за сутки
- ! ×■⊗ Распечатка сохраненных на карточке данных о событиях и неисправностях
- ! ×■⊗ Распечатка сохраненных в БУ данных о событиях и неисправностях
- ⊗⊗⊗ Распечатка технических данных
- ⊗ Распечатка данных о превышениях скорости

События

- ! ■ Ввод недействительной карточки
- ! ■■ Несовместимость карточки
- ! ⊗⊗ Нестыковка времени
- ! ⊗■ Управление без соответствующей карточки
- ! ■⊗ Ввод карточки во время управления
- ! ■■ Ошибка при завершении последнего сеанса работы с карточкой
- Превышение скорости
- ! † Прекращение электропитания
- ! Л Ошибка в данных о движении
- ! ■ Нарушение защиты
- ! ⊗ Корректировка времени (в мастерской)
- Контроль за превышениями скорости

Неисправности

- ✘■1 Сбой в работе карточки (считывающее устройство водителя)
- ✘■2 Сбой в работе карточки (считывающее устройство второго водителя)
- ✘□ Сбой в работе дисплея
- ✘⚡ Сбой загрузки данных
- ✘⚗ Сбой в работе печатающего устройства
- ✘L Сбой в работе датчика
- ✘A Внутренние неполадки в БУ

Процедура ручного ввода данных

- Ⓜ?Ⓜ Продолжение того же ежедневного периода работы?
- Ⓜ? Конец предыдущего периода работы?
- Ⓜ◆? Подтвердить или ввести пункт окончания рабочего периода
- ⓂⓂ? Ввести время начала
- ◆Ⓜ? Ввести пункт начала рабочего периода.

Примечание. В подразделе IV указаны дополнительные комбинации пиктограмм, используемые в качестве идентификаторов блоков или записей данных при распечатке.

ПОДРАЗДЕЛ IV

РАСПЕЧАТКА ДАННЫХ

СОДЕРЖАНИЕ

	Стр.
1. Общие положения	234
2. Спецификация блоков данных.....	234
3. Спецификация распечатки данных	247
3.1 Распечатка сохраненных на карточке данных о деятельности водителя за сутки	247
3.2 Распечатка сохраненных в БУ данных о деятельности водителя за сутки	248
3.3 Распечатка сохраненных на карточке данных о событиях и неисправностях.	250
3.4 Распечатка сохраненных в БУ данных о событиях и неисправностях.....	250
3.5 Распечатка технических данных.....	251
3.6 Распечатка данных о превышениях скорости.....	252

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, то 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, усеченной до размеров элемента данных.

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;

3. **Идентификационные данные держателя карточки**

Идентификатор блока данных.

P = пиктограмма "люди"

Фамилия держателя карточки

Имя (имена) держателя карточки (если имеются)

Идентификационные данные карточки

Срок действия карточки (если он ограничен)

-----P-----
P Фамилия_____
Имя_____
Идент._данные_карточки_____
дд/мм/гггг

На карточки, не принадлежащие конкретным лицам, вместо фамилии держателя наносится название предприятия, мастерской или контрольного органа.

4. **Идентификационные данные транспортного средства**

Идентификатор блока данных

VIN

Договаривающаяся сторона регистрации транспортного средства и VRN

-----D-----
D VIN_____
Гос/VRN_____

5. **Идентификационные данные БУ**

Идентификатор блока данных

Название изготовителя БУ

Номер детали БУ

-----B-----
B Изготовитель_БУ_____
Номер_детали_БУ__

6. **Последняя калибровка контрольного устройства**

Идентификатор блока данных

Название мастерской

Идентификационные данные карточки мастерской

Дата калибровки

-----T-----
T Фамилия_____
Идент._данные_карточки_____
T дд/мм/гггг

7. **Последний контроль (проверка контролером)**

Идентификатор блока данных

Идентификационные данные карточки
контролера

Дата, время и вид контроля

-----■----- Идент._данные_карточки_____ ■ дд/мм/гггг чч:мм рррр

Вид контроля: до четырех пиктограмм. Возможные виды контроля (по отдельности или в сочетании друг с другом):

■: загрузка данных с карточки, ▣: загрузка данных с БУ, ▤: распечатка, □: вывод на дисплей.

8. **Данные о деятельности водителя, сохраняемые на карточке в хронологической последовательности**

Идентификатор блока данных

Проверяемая дата (календарный день,
данные за который подлежат распечатке) +
календарный счетчик вводов карточки

-----■----- дд/мм/гггг ххх

8.1 **Период, в течение которого карточка находилась вне устройства**

8.1a Идентификатор записи (начало периода)

8.1b Период, за который нет данных. Время
начала и окончания, продолжительность

8.1c Данные о деятельности, введенные
вручную.

----- чч:мм чч:мм чччмм А чч:мм чч:мм чччмм *

Пиктограмма вида деятельности, время
начала и окончания (включительно),
продолжительность, периоды отдыха
длительностью не менее одного часа
помечаются звездочкой.

8.2 *Ввод карточки в считывающее устройство S*

Идентификатор записи; S = пиктограмма считывающего устройства

Договаривающаяся сторона регистрации транспортного средства и его VRN

Показания счетчика пробега на момент ввода карточки

-----S-----
▣ Гос/VRN _____
x xxx xxx км

8.3 *Деятельность (между вводом и извлечением карточки)*

Пиктограмма вида деятельности, время начала и окончания (включительно), продолжительность, состав экипажа (пиктограмма "экипаж" при наличии экипажа (CREW), пробелы при наличии одиночного водителя (SINGLE)), периоды отдыха длительностью не менее одного часа помечаются звездочкой.

A чч:мм чч:мм чччмм

8.3a *Особые ситуации.* Время ввода данных, пиктограмма (или комбинация пиктограмм) особой ситуации.

чч:мм -----pppp-----

8.4 *Извлечение карточки*

Показания счетчика пробега и расстояние, пройденное с момента последнего ввода карточки, при котором были зафиксированы показания счетчика пробега.

x xxx xxx км; x xxx км

9. *Данные о деятельности водителей, сохраненные в БУ отдельно для каждого считывающего устройства в хронологическом порядке*

Идентификатор блока данных

Проверяемая дата (календарные сутки, данные за которые подлежат распечатке)

Показания счетчика пробега на 00:00 часов и на 24:00 часа

-----□-----
дд/мм/гггг
x xxx xxx - x xxx xxx км

10. *Данные о деятельности водителей со считывающего устройства S*

Идентификатор блока данных

-----S-----

10.1 *Период отсутствия карточки в считывающем устройстве S*

Идентификатор записи

Карточка не введена

Показания счетчика пробега на начало периода

 ☐☐ ---
 x xxx xxx км

10.2 *Ввод карточки*

Идентификатор записи о вводе карточки

Фамилия водителя

Имя водителя

Идентификационные данные карточки водителя

Срок действия карточки водителя

Договаривающаяся сторона регистрации предыдущего транспортного средства, которым управлял водитель, и его VRN

Дата и время извлечения карточки из предыдущего транспортного средства

Пустая строка

Показания счетчика пробега на момент ввода карточки, метка ручного ввода данных о деятельности водителя (M - "да", пробел - "нет").

 ☐ Фамилия _____
 Имя _____
 Идент. _данные_ карточки _____

 дд/мм/гггг
 д+Гос/VRN _____

 дд/мм/гггг чч:мм

 x xxx xxx км M

10.3 *Деятельность*

Пиктограмма вида деятельности, время начала и окончания (включительно), продолжительность, состав экипажа (пиктограмма "экипаж" при наличии экипажа (CREW), пробелы при наличии одиночного водителя (SINGLE)), периоды отдыха длительностью не менее одного часа помечаются звездочкой.

A чч:мм чч:мм чччмм ☐☐ *

- 10.3а *Особые ситуации.* Время ввода данных, пиктограмма (или комбинация пиктограмм) особой ситуации. чч : мм -----pppp-----
- 10.4 *Извлечение карточки или окончание периода отсутствия карточки*
Показания счетчика пробега на момент извлечения карточки или окончания периода отсутствия карточки в устройстве и расстояние, пройденное с момента ввода карточки или с начала периода отсутствия карточки в устройстве. x xxx xxx км; x xxx км
11. **Суточная сводка**
Идентификатор блока данных -----Σ-----
- 11.1 *Сводка данных БУ за периоды отсутствия карточки в считывающем устройстве для карточки водителя*
Идентификатор блока данных 1▣---
- 11.2 *Сводка данных БУ за периоды отсутствия карточки в считывающем устройстве для карточки второго водителя*
Идентификатор блока данных 2▣---
- 11.3 *Суточная сводка данных БУ по каждому водителю*
Идентификатор записи
Фамилия водителя
Имя (имена) водителя
Идентификационные данные карточки водителя -----
Фамилия_____
Имя_____
Идент._данные_карточки_____
- 11.4 *Введенные данные о месте начала и/или окончания ежедневного периода работы*
пи = пиктограмма места начала / окончания, время, страна, район
Показания счетчика пробега пи чч : мм Стр Рег

x xxx xxx км

11.5 *Суммарные данные о деятельности водителя (с карточки)*

Общее время управления, пройденное расстояние

⊕ ЧЧЧММ X XXX КМ

Общее время работы и готовности

※ ЧЧЧММ ⊖ ЧЧЧММ

Общее время отдыха и отсутствия данных

┌ ЧЧЧММ ? ЧЧЧММ

Суммарное время деятельности экипажа

⊕⊕ ЧЧЧММ

11.6 *Суммарные данные о деятельности (периоды отсутствия карточки в считывающем устройстве для карточки водителя)*

Общее время управления, пройденное расстояние

⊕ ЧЧЧММ X XXX КМ

Общее время работы и готовности

※ ЧЧЧММ ⊖ ЧЧЧММ

Общее время отдыха

┌ ЧЧЧММ

11.7 *Суммарные данные о деятельности (периоды отсутствия карточки в считывающем устройстве для карточки второго водителя)*

Общее время работы и готовности

※ ЧЧЧММ ⊖ ЧЧЧММ

Общее время отдыха

┌ ЧЧЧММ

11.8 *Суммарные данные о деятельности (каждого водителя по данным обоих считывающих устройств)*

Общее время управления, пройденное расстояние

⊕ ЧЧЧММ X XXX КМ

Общее время работы и готовности

※ ЧЧЧММ ⊖ ЧЧЧММ

Общее время отдыха

┌ ЧЧЧММ

Суммарное время деятельности экипажа

⊕⊕ ЧЧЧММ

При вводе команды на распечатку суточной сводки за текущий день имеющиеся данные за сутки суммируются по состоянию на момент распечатки.

12. *События и/или неисправности, зарегистрированные на карточке*

12.1 Идентификатор блока данных: последние 5 "событий и неисправностей", зарегистрированных на карточке

-----!※-----

12.2 Идентификатор блока данных: все "события", зарегистрированные на карточке

-----!■-----

12.3 Идентификатор блока данных: все "неисправности", зарегистрированные на карточке

-----x■-----

12.4 *Запись о событии и/или неисправности*

Идентификатор записи

Пиктограмма события/неисправности, назначение записи, дата и время начала

Дополнительный код события/неисправности (если имеется), продолжительность

Договаривающаяся сторона регистрации транспортного средства, в котором имело место событие или неисправность, и VRN этого транспортного средства

Пик дд/мм/гггг чч:мм

!xxx чччмм

▲ Гос/VRN_____

13. *Прошлые или текущие события и/или неисправности, зарегистрированные или регистрируемые бортовым устройством*

13.1 Идентификатор блока данных: последние 5 "событий и неисправностей" по данным БУ

-----!x▲-----

13.2 Идентификатор блока данных: все прошлые или текущие "события", зарегистрированные или регистрируемые БУ

-----!▲-----

13.3 Идентификатор блока данных: все прошлые или текущие "неисправности", зарегистрированные или регистрируемые БУ

-----xд-----

13.4 *Запись о событии и/или неисправности*

Идентификатор записи

Пиктограмма события/неисправности, цель записи, дата и время начала

Дополнительный код события/неисправности (если имеется), количество аналогичных событий за текущий день, продолжительность

Идентификационные данные карточек, находившихся в устройстве на момент начала или окончания события или неисправности (до 4 строк без повторения одних и тех же номеров карточек)

Отсутствие карточки в устройстве

Пик (ц) дд/мм/гггг чч:мм

! xxx (xxx) чччмм

Идент. _данные_карточки_____

Идент. _данные_карточки_____

Идент. _данные_карточки_____

Идент. _данные_карточки_____

■ ---

Цель записи (ц) указывается числовым кодом, обозначающим цель регистрации события или неисправности и определяемым в порядке, предусмотренном для элемента данных EventFaultRecordPurpose.

14. *Идентификационные данные БУ*

Идентификатор блока данных

Название изготовителя БУ

Адрес изготовителя БУ

Номер детали БУ

Номер решения об официальном утверждении данного образца БУ

Серийный номер БУ

Год выпуска БУ

Версия и дата установки программного обеспечения БУ

-----в-----

в Название_____

Адрес_____

НомерДетали_____

Утвержд._____

С/Н_____

гггг

в xx.xx.xx дд/мм/гггг

15. **Идентификационные данные датчика**

Идентификатор блока данных
Серийный номер датчика
Номер решения об официальном
утверждении данного образца датчика
Дата первой установки датчика

----- L ----- л С/Н _____ Утвержд. _____ дд/мм/гггг
--

16. **Данные калибровки**

Идентификатор блока данных

----- T -----

16.1 **Запись о калибровке**

Идентификатор записи
Мастерская, где произведена калибровка
Адрес мастерской
Идентификационные данные карточки
мастерской
Срок действия карточки мастерской
Пустая строка
Дата калибровки + цель калибровки
VIN
Договаривающаяся сторона регистрации
транспортного средства и его VRN
Характеристический коэффициент
транспортного средства
Постоянная контрольного устройства
Эффективная окружность шин колес
Размер шин, установленных на
транспортном средстве
Положение устройства ограничения
скорости
Показания счетчика пробега до и после
калибровки

----- T Название_мастерской _____ Адрес_мастерской _____ Идент._данные_карточки _____ дд/мм/гггг T дд/мм/гггг (ц) # VIN _____ Гос/VRN _____ w xx xxx имп/км k xx xxx имп/км l xx xxx мм * РазмерШин _____ > xxx км/ч x xxx xxx – x xxx xxx км

Цель калибровки (p) указывается числовым кодом, обозначающим цель регистрации соответствующих калибровочных параметров и определяемым в порядке, предусмотренном для элемента данных CalibrationPurpose.

17. **Корректировка времени**

Идентификатор блока данных

-----@-----

17.1 **Запись о корректировке времени**

Идентификатор записи

Дата и время до корректировки

Дата и время после корректировки

Мастерская, где произведена
корректировка времени

Адрес мастерской

Идентификационные данные карточки
мастерской

Срок действия карточки мастерской

дд/мм/гггг чч:мм
дд/мм/гггг чч:мм
Название_мастерской____

Адрес_мастерской_____
Идент._данные_карточки__

дд/мм/гггг

18. **Зарегистрированные БУ данные о последних по времени событиях и неисправности**

Идентификатор блока данных

Дата и время последнего события

Дата и время последней неисправности

-----!xд-----
дд/мм/гггг чч:мм
дд/мм/гггг чч:мм

19. **Информация о контроле за превышениями скорости**

Идентификатор блока данных

Дата и время последнего контроля за
превышениями скорости

Дата и время первого превышения скорости
и количество последующих превышений
скорости

----->>-----
>дд/мм/гггг чч:мм

>>дд/мм/гггг чч:мм (nnn)

20. **Запись о превышениях скорости**

20.1 Идентификатор блока данных: первое превышение скорости со времени последней калибровки

----->>T-----

20.2 Идентификатор блока данных: 5 наиболее серьезных превышений за последние 365 дней

----->>(365)-----

20.3 Идентификатор блока данных: наиболее серьезное превышение за каждые из последних 10 дней, когда превышения имели место

----->>(10)-----

20.4 Идентификатор записи

Дата, время и продолжительность

Максимальная и средняя скорость, количество аналогичных событий за данный день

Фамилия водителя

Имя (имена) водителя

Идентификационные данные карточки водителя

>>ДД/ММ/ГГГГ ЧЧ:ММ ЧЧММ

xxx км/ч xxx км/ч(xxx)

☐ Фамилия_____

Имя_____

Идент._данные_карточки_____

20.5 Если в блоке данных записи о превышениях скорости отсутствуют

>>---

21 **Информация, вписываемая от руки**

Идентификатор блока данных

21.1 Место контроля

21.2 Подпись контролера

21.3 Время: от

21.4 Время: до

21.5 Подпись водителя

☐*

☐

☐+

+☐

☐

"Информация, вписываемая от руки": над названием графы, заполняемой от руки, следует оставить достаточное количество пустых строк для вписывания необходимой информации или для собственноручной подписи.

3. Спецификации распечатки данных

В тексте данной главы применяются следующие условные обозначения:

N	Распечатка блока или записи данных под номером N
N	Распечатка блока или записи данных под номером N нужное количество раз
X / Y	Распечатка по мере необходимости блоков или записей данных под номером X и/или Y и ее повторение нужное количество раз

3.1 Распечатка сохраненных на карточке данных о деятельности водителя за сутки

PRT_007 При распечатке сохраненных на карточке данных о деятельности водителя за сутки соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные контролера (если в БУ введена карточка контролера)
3	Идентификационные данные водителя (согласно карточке, с которой распечатываются данные)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
5	Идентификационные данные БУ (с которого получены распечатываемые данные)
6	Последняя калибровка данного БУ
7	Предыдущий контроль деятельности проверяемого водителя
8	Ограничитель данных о деятельности водителя
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Деятельность водителя в хронологическом порядке
11	Ограничитель данных суточной сводки

11.4	Въезд в географические пункты в хронологическом порядке
11.5	Суммарные данные о деятельности
12.1	Ограничитель сохраненных на карточке данных о событиях и неисправностях
12.4	Записи о событиях/неисправностях (последние 5 событий или неисправностей, зарегистрированные на карточке)
13.1	Ограничитель данных БУ о событиях и неисправностях
13.4	Записи о событиях/неисправностях (последние 5 событий или неисправностей, зарегистрированных или регистрируемых БУ)
21.1	Место контроля
21.2	Подпись контролера
21.5	Подпись водителя

3.2 Распечатка сохраненных в БУ данных о деятельности водителя за сутки

PRT_008 При распечатке сохраненных в БУ данных о деятельности водителя за сутки соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные держателя карточки (для всех карточек, введенных в БУ)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
5	Идентификационные данные БУ (с которого получены распечатываемые данные)
6	Последняя калибровка данного БУ
7	Предыдущий контроль с помощью данного контрольного устройства
9	Ограничитель данных о деятельности водителя
10	Ограничитель данных со считывающего устройства для карточки водителя (считывающее устройство 1)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Деятельность в хронологическом порядке (данные со считывающего устройства для карточки водителя)

10	Ограничитель данных со считывающего устройства для карточки второго водителя (считывающее устройство 2)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Деятельность в хронологическом порядке (данные со считывающего устройства для карточки второго водителя)
11	Ограничитель данных суточной сводки
11.1	Сводные данные о периодах отсутствия карточки в считывающем устройстве для карточки водителя
11.4	Въезд в географические пункты в хронологическом порядке
11.6	Суммарные данные о деятельности
11.2	Сводные данные о периодах отсутствия карточки в считывающем устройстве для карточки второго водителя
11.4	Въезд в географические пункты в хронологическом порядке
11.7	Суммарные данные о деятельности
11.3	Суммарные данные о деятельности водителя по данным обоих считывающих устройств
11.4	Въезд данного водителя в географические пункты в хронологическом порядке
11.7	Суммарные данные о деятельности данного водителя
13.1	Ограничитель данных о событиях и отказах
13.4	Записи о событиях/неисправностях (последние 5 событий или неисправностей, зарегистрированных или регистрируемых БУ)
21.1	Место контроля
21.2	Подпись контролера
21.3	Время: с (место для указания водителем, не имеющим
21.4	Время: до карточки, относящихся к нему периодов времени)
21.5	Подпись водителя

3.3 Распечатка сохраненных на карточке данных о событиях и неисправностях

PRT_009 При распечатке сохраненных на карточке данных о событиях и неисправностях соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные контролера (если в БУ введена карточка контролера)
3	Идентификационные данные водителя (согласно карточке, с которой распечатываются данные)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
12.2	Ограничитель данных о событиях
12.4	Записи о событиях (все события, зарегистрированные на карточке)
12.3	Ограничитель данных о неисправностях
12.4	Записи о неисправностях (все неисправности, зарегистрированные на карточке)
21.1	Место контроля
21.2	Подпись контролера
21.5	Подпись водителя

3.4 Распечатка сохраненных в БУ данных о событиях и неисправностях

PRT_010 При распечатке сохраненных в БУ данных о событиях и неисправностях соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные держателя карточки (для всех карточек, введенных в БУ)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
13.2	Ограничитель данных о событиях
13.4	Записи о событиях (все события, зарегистрированные или регистрируемые БУ)

13.3	Ограничитель данных о неисправностях
13.4	Записи о событиях (все неисправности, зарегистрированные или регистрируемые БУ)
21.1	Место контроля
21.2	Подпись контролера
21.5	Подпись водителя

3.5 Распечатка технических данных

PRT_011 При распечатке технических данных соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные держателя карточки (для всех карточек, введенных в БУ)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
14	Идентификационные данные БУ
15	Идентификационные данные датчика
16	Ограничитель данных калибровки
16.1	Записи о калибровке (все имеющиеся записи в хронологическом порядке)
17	Ограничитель данных о корректировке времени
17.1	Записи о корректировке времени (все имеющиеся записи о корректировке времени, в том числе относящиеся к калибровке)
18	Последние по времени событие и неисправность, зарегистрированные БУ

3.6 Распечатка данных о превышениях скорости

PRT_012 При распечатке данных о превышениях скорости соблюдается следующий формат:

1	Дата и время распечатки документа
2	Вид распечатки
3	Идентификационные данные держателя карточки (для всех карточек, введенных в БУ)
4	Идентификационные данные транспортного средства (с которого получены распечатываемые данные)
19	Информация о контроле за превышениями скорости
20.1	Идентификатор данных о превышениях скорости
20.4 / 20.5	Первое превышение скорости со времени последней калибровки
20.2	Идентификатор данных о превышениях скорости
20.4 / 20.5	5 наиболее серьезных превышений скорости за последние 365 дней
20.3	Идентификатор данных о превышениях скорости
20.4 / 20.5	Наиболее серьезное превышение скорости за каждые из последних 10 дней, когда превышения имели место
21.1	Место контроля
21.2	Подпись контролера
21.5	Подпись водителя

ПОДРАЗДЕЛ V

ИНДИКАЦИЯ НА ДИСПЛЕЕ

В тексте настоящего подраздела применяются следующие условные обозначения:

- **жирным шрифтом** обозначена информация, выводимая на дисплей в текстовой форме (на дисплее используется обычный шрифт),
- обычным шрифтом указаны переменные параметры (поля для пиктограмм или виды данных), вместо которых отображаются соответствующие пиктограммы или значения:
- дд мм гггг: день, месяц, год;
- чч: часы;
- мм: минуты;
- В: пиктограмма периода времени;
- СО: комбинация пиктограмм события и неисправности;
- Р: пиктограмма режима работы.

DIS_001 При индикации данных контрольного устройства соблюдается следующий формат:

Данные	Формат
Вид дисплея по умолчанию	
Местное время	чч:мм
Режим работы	Р
Информация, касающаяся водителя	1Вчччмм чччмм
Информация, касающаяся второго водителя	2Вчччмм
Начало ситуации "неприменимо"	OUT
Предупреждающие индикаторы	
Превышение времени непрерывного управления	1Ⓢчччмм чччмм
Событие или неисправность	СО
Прочие индикаторы	
Дата в формате UTC	UTCⓈдд/мм/гггг или UTCⓈдд.мм.гггг
Время	чч:мм
Время непрерывного управления и совокупная продолжительность перерывов у водителя	1Ⓢчччмм чччмм

Время непрерывного управления и совокупная продолжительность перерывов у второго водителя	20чччмм 11чччмм
Совокупное время управления за прошлую и текущую неделю у водителя	10 11 ччччмм
Совокупное время управления за прошлую и текущую неделю у второго водителя	20 11 ччччмм

ПОДРАЗДЕЛ VI

ВНЕШНИЕ ИНТЕРФЕЙСЫ

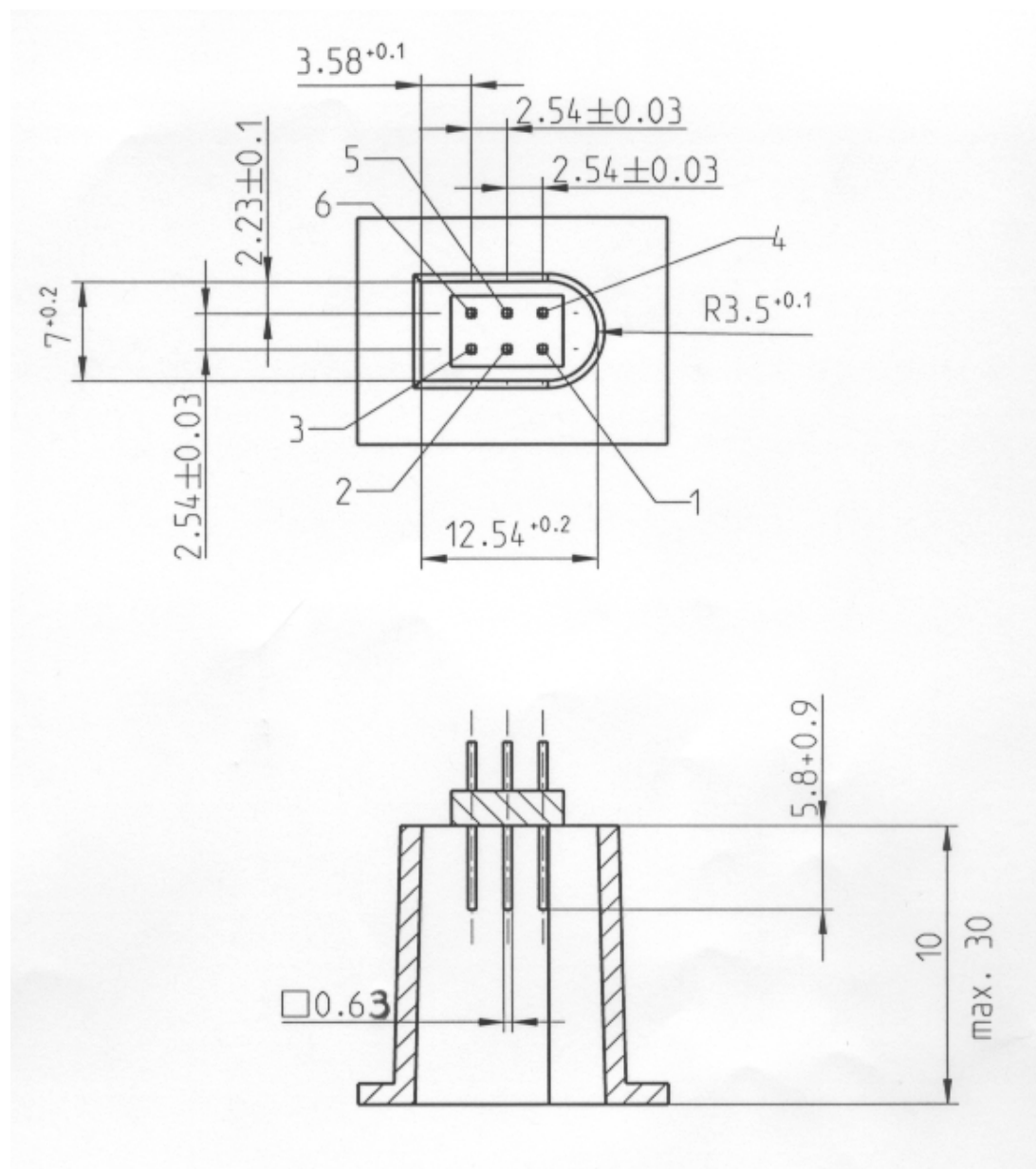
СОДЕРЖАНИЕ

	<u>Стр.</u>
1. Аппаратная часть	256
1.1 Разъем.....	256
1.2 Разводка контактов	258
1.3 Блок-схема	259
2. Интерфейс загрузки данных	259
3. Интерфейс калибровки	260

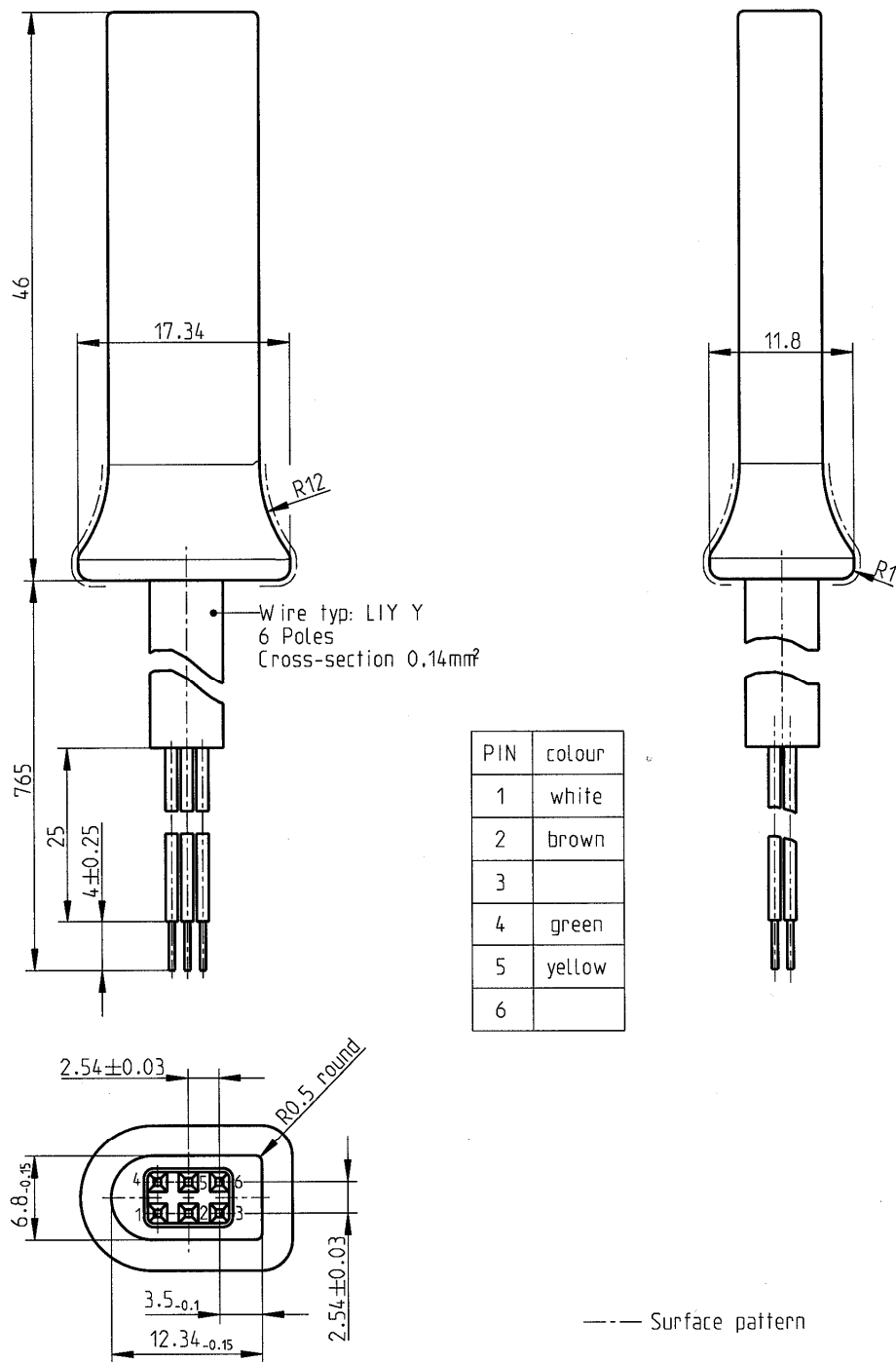
1. Аппаратная часть

1.1 Разъем

INT_001 Соединительное гнездо для загрузки данных и калибровки должно располагаться на передней панели, быть доступным без снятия каких-либо деталей контрольного устройства и представлять собой 6-контактный разъем, выполненный в соответствии с нижеследующими чертежами (все размеры указаны в миллиметрах):



Типовая схема вилки 6-контактного штепсельного разъема:



Тип провода: LIY Y	
6 полюсов	
Поперечное сечение 0,14 мм ²	
Контакт	Цвет
1	белый
2	коричневый

3	
4	зеленый
5	желтый
6	
Закругление R0,5	Профиль поверхности

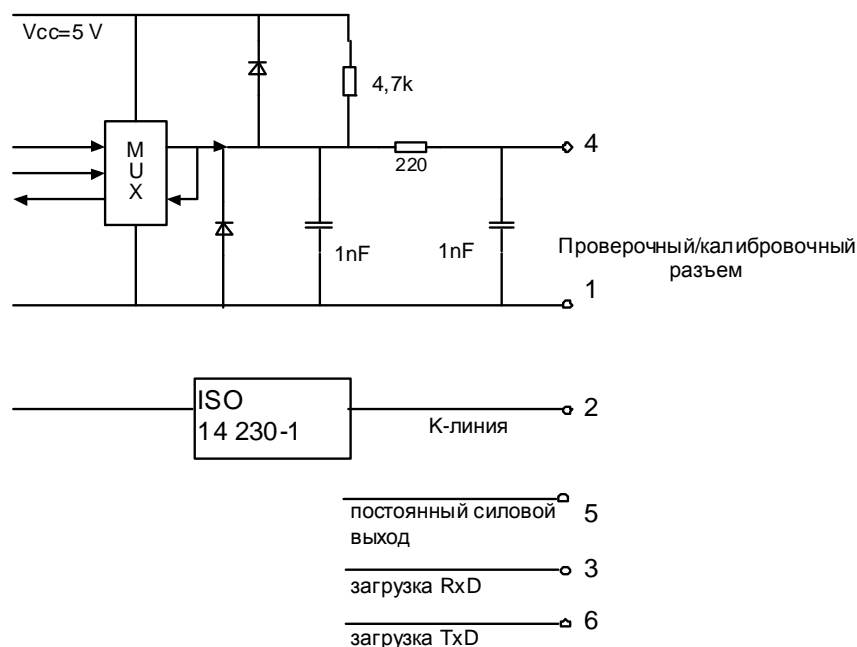
1.2 Разводка контактов

INT_002 Разводка контактов указана в таблице ниже.

Контакт	Назначение	Примечания
1	Отрицательный полюс источника питания	Соединяется с отрицательным полюсом бортовой аккумуляторной батареи
2	Передача данных	К-линия (ISO 14230-1)
3	RxD – Загрузка данных	Ввод данных в контрольное устройство
4	Входной/выходной сигнал	Калибровка
5	Постоянный силовой выход	Номинальный диапазон напряжений равен напряжению бортовой сети питания минус 3 В с учетом падения напряжения на предохранительных цепях Выход 40 мА
6	TxD – Загрузка данных	Вывод данных из контрольного устройства

1.3 Блок-схема

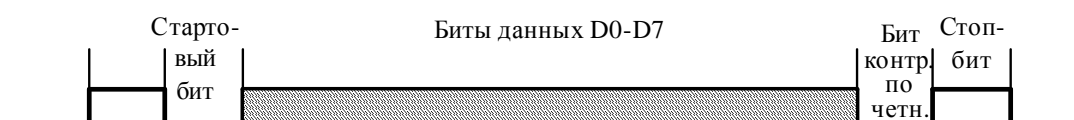
INT_003 Блок-схема должна соответствовать приведенной ниже.



2. Интерфейс загрузки данных

INT_004 Интерфейс загрузки данных должен соответствовать спецификациям RS232.

INT_005 Порядок загрузки данных через интерфейс: один стартовый бит, 8 битов данных начиная с младшего бита, один бит контроля по четности, один стоп-бит.



Структура байта данных

Стартовый бит:	один бит с уровнем логического нуля;
Биты данных:	бит младшего разряда передается первым;
Бит контроля по четности:	положительная четность;
Стоп-бит:	один бит с уровнем логической единицы.

При передаче числовых данных объемом больше одного байта байт старшего разряда передается первым, байт младшего разряда – последним.

INT_006 Скорость передачи данных должна быть регулируемой в диапазоне от 9 600 бит/с до 115 200 бит/с. При инициализации обмена данными задается начальная скорость передачи 9 600 бит/с; затем скорость доводится до максимальной возможной величины.

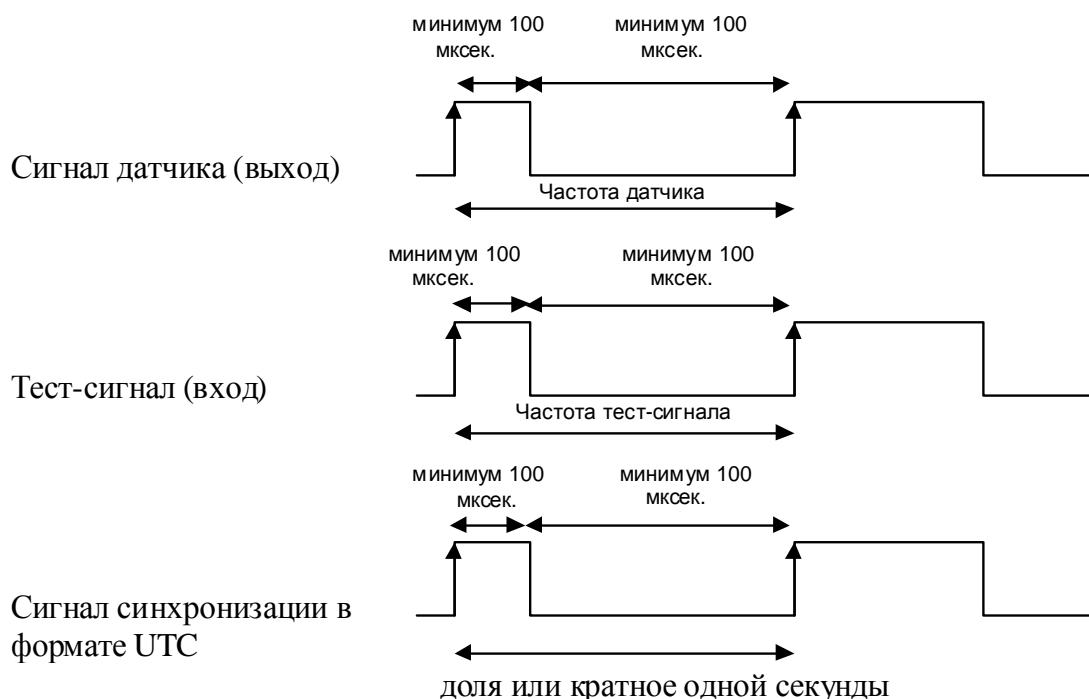
3. Интерфейс калибровки

INT_007 Обмен данных осуществляется в соответствии со стандартом ISO 14230-1 (Транспорт дорожный. Системы диагностического контроля. Протокол ключевых слов 2000. Часть 1. Физический уровень. Издание первое, 1999 год).

INT_008 Электрические характеристики входного/выходного сигнала должны соответствовать указанным ниже.

Параметр	Минимум	Норма	Максимум	Примечание
$U_{\text{ниж}}$ (ВХОД)			1,0 В	$I = 750 \text{ мкА}$
$U_{\text{верх}}$ (ВХОД)	4 В			$I = 200 \text{ мкА}$
Частота			4 кГц	
$U_{\text{ниж}}$ (ВЫХОД)			1,0 В	$I = 1 \text{ мА}$
$U_{\text{верх}}$ (ВЫХОД)	4 В			$I = 1 \text{ мА}$

INT_009 Временные диаграммы входного/выходного сигнала приводятся ниже:



ПОДРАЗДЕЛ VII
ПРОТОКОЛЫ ЗАГРУЗКИ ДАННЫХ
СОДЕРЖАНИЕ

	<u>Стр.</u>
1. Введение.....	263
1.1 Сфера применения.....	263
1.2 Сокращения и обозначения.....	263
2. Загрузка данных из БУ.....	264
2.1 Процедура загрузки.....	264
2.2 Протокол загрузки данных.....	265
2.2.1 Структура сообщений.....	265
2.2.2 Типы сообщений.....	267
2.2.2.1 Start Communication Request –Запрос инициализации обмена данными (SID 81).....	268
2.2.2.2 Positive Response Start Communication – Положительный ответ: инициализация обмена данными (SID C1).....	268
2.2.2.3 Start Diagnostic Session Request – Запрос инициализации диагностического сеанса (SID 10).....	269
2.2.2.4 Positive Response Start Diagnostic – Положительный ответ: инициализация диагностики (SID 50).....	269
2.2.2.5 Link Control Service – Функция регулировки канала обмена данными (SID 87).....	269
2.2.2.6 Link Control Positive Response – Регулировка канала обмена данными: положительный ответ (SID C7).....	269
2.2.2.7 Request Upload – Запрос загрузки (SID 35).....	269
2.2.2.8 Positive Response Request Upload – Положительный ответ на запрос загрузки (SID 75).....	270
2.2.2.9 Transfer Data Request – Запрос передачи данных (SID 36).....	270
2.2.2.10 Positive Response Transfer Exit (SID 77).....	271
2.2.2.11 Stop Communication Request (SID 82).....	271
2.2.2.12 Positive Response Stop Communication (SID C2).....	271
2.2.2.13 Acknowledge Sub Message (SID 83).....	271
2.2.2.14 Negative Response (SID 7F).....	271
2.2.3 Поток сообщений.....	273
2.2.4 Временные параметры.....	274
2.2.5 Обработка ошибок.....	275
2.2.5.1 Стадия инициализации обмена данными.....	276
2.2.5.2 Стадия обмена данными.....	276
2.2.6 Содержание ответного сообщения.....	279
2.2.6.1 Positive Response Request Upload.....	280
2.2.6.2 Positive Response Transfer Data Activities.....	281
2.2.6.3 Positive Response Transfer Data Events and Faults.....	283

СОДЕРЖАНИЕ (продолжение)

	<u>Стр.</u>
2.2.6.4 Positive Response Transfer Data Detailed Speed	285
2.2.6.5 Positive Response Transfer Data Technical Data	285
2.3 Сохранение данных на ВН	287
3. Протокол загрузки данных с карточек тахографа.....	287
3.1 Сфера применения.....	287
3.2 Определения.....	287
3.3 Загрузка данных с карточки	287
3.3.1 Процедура инициализации	288
3.3.2 Процедура для неподписанных файлов данных.....	289
3.3.3 Процедура для подписанных файлов данных	289
3.3.4 Процедура обнуления счетчика калибровок.....	290
3.4 Формат сохранения данных.....	291
3.4.1 Введение.....	291
3.4.2 Формат файлов.....	291
4. Загрузка данных с карточек тахографа через бортовое устройство.....	292

1. Введение

В настоящем подразделе изложены процедуры различных вариантов загрузки данных на внешний носитель (ВН), а также протоколы, применение которых необходимо для правильной передачи данных и для обеспечения универсальной совместимости формата, в котором они загружаются, с тем чтобы любой контролер имел возможность ознакомиться с этими данными и перед началом их анализа убедиться в их подлинности и достоверности.

1.1 Сфера применения

На ВН могут загружаться данные:

- из бортового устройства при помощи подключенной к БУ специализированной программируемой аппаратуры (СПА),
- с карточки тахографа при помощи СПА, оснащенной устройством считывания карточек (УСК),
- 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 указанным в подразделе XI ("Общие механизмы защиты"). В состав загружаемой информации включаются идентификационные данные аппаратного источника (БУ или карточки) и соответствующие ему сертификаты безопасности (Договаривающейся стороны 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 подразделе используются следующие сокращения:

AID	(ИП) Идентификатор приложений
ATR	Ответ на сигнал перезагрузки
CS	Байт контрольной суммы
DF	Каталог

DS_	Диагностический сеанс
EF	Элементарный файл
ESM	(ВН) Внешний носитель
FID	(ID файла) Идентификатор файла
FMT	Байт формата (первый байт в заголовке сообщения)
Hex	Шестнадцатеричное значение
ICC	(МПК) Микропроцессорная карточка
IDE	(СПА) Специализированная программируемая аппаратура: аппаратура, используемая для загрузки данных на ВН (например, персональный компьютер)
IFD	(УСК) Устройство считывания карточек (интерфейс)
KWP	Протокол ключевых слов 2000
LEN	Байт длины (последний байт в заголовке сообщения)
PPS	(ВПП) Выбор параметров протокола
PSO	Выполнение защитной операции
SID	Идентификатор функции
SRC	Байт адреса источника
TGT	Байт адреса приемника
TLV	Метка-длина-значение
TREP	Параметр ответа на запрос передачи
TRTP	Параметр запроса передачи
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 разъему БУ;
- установить канал связи между СПА и БУ;
- с помощью СПА выбрать данные для загрузки и передать запрос в БУ;
- завершить сеанс загрузки.

*) Ввод карточки инициирует подтверждение соответствующих прав доступа к функции загрузки и загружаемым данным.

2.2 Протокол загрузки данных

Протокол построен по принципу "ведущий-ведомый", при котором в роли ведущего выступает СПА, а в роли ведомого – БУ.

Структура, типы и поток сообщений в основном соответствуют протоколу ключевых слов KWP 2000 (ISO 14230-2 Транспорт дорожный. Системы диагностического контроля. Протокол ключевых слов 2000. Часть 2. Уровень обмена данными).

Уровень приложений в основном соответствует нынешней версии проекта стандарта ISO 14229-1 (Транспорт дорожный. Системы диагностического контроля. Часть 1. Диагностические функции. Версия 6 от 22 февраля 2001 года).

2.2.1 Структура сообщений

DDP_002 Все сообщения, которыми обмениваются СПА и БУ, форматируются в соответствии с трехкомпонентной структурой:

- заголовок, состоящий из байта формата (FMT), байта адреса приемника (TGT), байта адреса источника (SRC) и в некоторых случаях также байта длины сообщения (LEN);
- поле данных, образуемое байтом идентификатора функции (SID) и переменным числом байтов данных, включая необязательный байт диагностического сеанса (DS_) и необязательный байт параметра передачи (TRTP или TREP);
- контрольная сумма, определяемая байтом контрольной суммы (CS).

Заголовок				Поле данных					Контрольная сумма
FMT	TGT	SRC	LEN	SID	DATA	CS
4 байта				до 255 байт					1 байт

Байты TGT и SRC указывают физические адреса получателя и отправителя сообщения. Их значения – F0 Hex для СПА и EE Hex для БУ.

Байт LEN представляет собой длину поля данных в сообщении.

Байт контрольной суммы представляет собой 8-битную сумму по модулю 256 всех байт сообщения, за исключением самой контрольной суммы.

Определения байтов FMT, SID, DS_, TRTP и TREP приводятся далее в настоящем документе.

DDP_003 Если объем передаваемых в сообщении данных превышает длину поля данных, то сообщение фактически высылается в виде нескольких подсообщений. Каждое подсообщение содержит заголовок, одни и те же байты SID и TREP, а также 2-байтовый счетчик подсообщений, указывающий порядковый номер данного подсообщения в общем сообщении. Чтобы обеспечить возможность обнаружения ошибок и отмены передачи, СПА подтверждает получение каждого подсообщения. СПА может принять подсообщение, запросить его повторную передачу, выдать БУ команду начать передачу заново или отменить ее.

DDP_004 Если поле данных последнего подсообщения содержит ровно 255 байт, то к нему должно добавляться заключительное подсообщение с пустым (то есть содержащим только SID, TREP и счетчик подсообщений) полем данных, означающее конец сообщения.

Пример:

Заголовок	SID	TREP	Сообщение			CS
4 байта	Более 255 байт					

Передается как

Заголовок	SID	TREP	00	01	Подсообщение 1	CS
4 байта	255 байт					
Заголовок	SID	TREP	00	02	Подсообщение 2	CS
4 байта	255 байт					

...

Заголовок	SID	TREP	xx	yy	Подсообщение n	CS
4 байта	Менее 255 байт					

или как:

Заголовок	SID	TREP	00	01	Подсообщение 1	CS
4 байта	255 байт					

Заголовок	SID	TREP	00	02	Подсообщение 2	CS
4 байта	255 байт					

...

Заголовок	SID	TREP	xx	yy	Подсообщение n	CS
4 байта	255 байт					

Заголовок	SID	TREP	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

	До 4 байт Заголовок				До 255 байт Данные			1 байт Контр. сумма
	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	ДАнные	CS
СПА ->								
<- БУ								
Запрос инициализации обмена данными	81	EE	F0		81			E0
Положит. ответ: инициализ. обмена данными	80	F0	EE	03	C1		'EA' '8F'	9B
Запрос инициализ. диагност. сеанса	80	EE	F0	02	10	81		F1
Положит. ответ: инициализ. диагност. сеанса	80	F0	EE	02	50	81		31
Функция регулировки канала обмена данными								
Проверка скорости передачи данных (этап 1)								
9 600 бод	80	EE	F0	04	87		01,01,01	EC
19 200 бод	80	EE	F0	04	87		01,01,02	ED
38 400 бод	80	EE	F0	04	87		01,01,03	EE
57 600 бод	80	EE	F0	04	87		01,01,04	EF
115 200 бод	80	EE	F0	04	87		01,01,05	F0
Положит. ответ: проверка скорости передачи	80	F0	EE	02	C7		01	28
Переходная скорость передачи (этап 2)	80	EE	F0	03	87		02,03	ED
Запрос загрузки	80	EE	F0	0A	35		00,00,00,00 ,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
Деятельность	80	EE	F0	06	36	02	Дата	CS

События и отказы	80	EE	F0	02	36	03		99
Подробные данные о скоростном режиме	80	EE	F0	02	36	04		9A
Технические данные	80	EE	F0	02	36	05		9B
Загрузка с карточки	80	EE	F0	02	36	06		9C
Положит. ответ: передача данных	80	F0	EE	Len	76	TREP	Данные	CS
Запрос завершения передачи	80	EE	F0	01	37			96
Положит. ответ: завершение передачи	80	F0	EE	01	77			D6
Запрос завершения обмена данными	80	EE	F0	01	82			E1
Положит. ответ: завершение обмена данными	80	F0	EE	01	C2			21
Подтверждение приема подсообщения	80	EE	F0	Len	83		Данные	CS
Отрицательные ответы								
Общий отрицательный результат	80	F0	EE	03	7F	Sid Req	10	CS
Функция не поддерживается	80	F0	EE	03	7F	Sid Req	11	CS
Подфункция не поддерживается	80	F0	EE	03	7F	Sid Req	12	CS
Неверная длина сообщения	80	F0	EE	03	7F	Sid Req	13	CS
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 приеме загружаемых данных	80	F0	EE	03	7F	Sid Req	50	CS
Ожидается ответ	80	F0	EE	03	7F	Sid Req	78	CS
Данные отсутствуют	80	F0	EE	03	7F	Sid Req	FA	CS

Примечания:

- Sid Req = Sid соответствующего запроса.
- TREP = TRTP соответствующего запроса.
- Темный фон ячейки в таблице означает отсутствие передачи данных.
- Термин "upload" (загрузка со стороны СПА) используется для целей совместимости с ISO 14229. Он имеет тот же смысл, что и термин "download" (загрузка со стороны БУ).
- 2-байтные счетчики подсообщений, которые могут содержаться в сообщениях, в таблице не показаны.

2.2.2.1 *Start Communication Request –
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 *Positive Response Start Communication – Положительный ответ:
инициализация обмена данными (SID C1)*

DDP_006 Данное сообщение высылается БУ в качестве положительного ответа на запрос инициализации обмена данными. Оно включает 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 *Start Diagnostic Session Request – Запрос инициализации диагностического 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" (сеанс по умолчанию) (81 Hex) указывает на то, что будет начат стандартный диагностический сеанс.

2.2.2.4 *Positive Response Start Diagnostic – Положительный ответ: инициализация диагностики (SID 50)*

DDP_008 Сообщение с положительным ответом на запрос инициализации диагностики высылает БУ, чтобы подтвердить начало диагностического сеанса.

2.2.2.5 *Link Control Service – Функция регулировки канала обмена данными (SID 87)*

DDP_052 Функция регулировки канала обмена данными используется СПА для того, чтобы инициировать изменение скорости передачи данных. 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. Получив подтверждение, БУ также переключается на новую скорость передачи.

2.2.2.6 *Link Control Positive Response – Регулировка канала обмена данными: положительный ответ (SID C7)*

DDP_053 Это сообщение высылается БУ в качестве положительного ответа на запрос регулировки канала обмена данными (первый этап). Следует обратить внимание на то, что ответ на запрос подтверждения не высылается (второй этап).

2.2.2.7 *Request Upload – 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, объеме 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 объем памяти задается максимальным.

2.2.2.8 *Positive Response Request Upload – Положительный ответ на 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 *Transfer Data Request – 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 с карточки (TRTP 06).

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 создает возможность проверки цифровой подписи).

Во втором случае (TRTP 02) сообщение с запросом передачи данных включает указание календарной даты (в формате реального времени), данные за которую подлежат загрузке.

2.2.2.10 Positive Response Transfer Data – Положительный ответ на запрос передачи 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 безопасности;
- идентификации транспортного средства;
- текущей дате и времени по хронометражу 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 Request Transfer Exit – Запрос завершения передачи (SID 37)

DDP_013 Сообщение с запросом завершения передачи высылается СПА с целью указать БУ на завершение сеанса загрузки.

2.2.2.12 Positive Response Request Transfer Exit – Положительный ответ на запрос завершения передачи (SID 77)

DDP_014 Сообщение с положительным ответом на запрос завершения передачи высылает БУ с целью подтвердить прием запроса завершения передачи.

2.2.2.13 Stop Communication Request – Запрос завершения обмена данными (SID 82)

DDP_015 Сообщение с запросом завершения обмена данными высылается СПА с целью закрыть канал обмена данными с БУ.

2.2.2.14 Positive Response Stop Communication – Положительный ответ на запрос на завершение обмена данными (SID C2)

DDP_016 Сообщение с положительным ответом на запрос завершения обмена данными высылается БУ с целью подтвердить прием запроса завершения обмена данными.

2.2.2.15 *Acknowledge Sub Message – Подтверждение приема подсообщения (SID 83)*

DDP_017 Подтверждение приема 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 приема подсообщения номер MsgC.
Запрос от СПА к БУ на отправку следующего подсообщения;

MsgC – указание на сбой при приеме подсообщения номер MsgC.
Запрос от СПА к БУ на повторную отправку данного подсообщения;

FFFF – запрос прекращения передачи сообщения.
Эта функция может использоваться СПА для прекращения по каким-либо причинам передачи сообщения от БУ.

Прием 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 на запрос передачи данных (SID 76).

2.2.2.16 *Отрицательный ответ (SID 7F)*

DDP_018 Сообщение с отрицательным ответом на те или иные из перечисленных выше запросов БУ высылает в тех случаях, когда запрос не может быть выполнен. Поле данных сообщения содержит SID ответа (7F), SID запроса и код, указывающий причину отрицательного ответа. Могут использоваться следующие коды:

- 10 Общее отклонение запроса
Действие не может быть выполнено по причине, не входящей в число нижеперечисленных;
- 11 Функция 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 запросов
Требуемая функция не активирована либо неверная очередность запросов;
- 31 Нештатный запрос
Значение параметра запроса (поле данных) недействительно;
- 50 Отказ в приеме загружаемых данных
Невозможно выполнить запрос (несоответствие режима работы БУ или внутренние неполадки в БУ);
- 78 Ожидается ответ
Запрошенная операция не может быть завершена своевременно; БУ не готов к приему нового запроса;
- FA Данные отсутствуют
Запрошенный к передаче объект данных отсутствует в БУ (например, не введена карточка, и т.п.).

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 диагностического сеанса	⇒	
	⇐	Положительный ответ
Запрос загрузки	⇒	
	⇐	Положительный ответ
Запрос передачи обзорных данных	⇒	
	⇐	Положительный ответ

Запрос передачи данных #2	⇒	Положительный ответ #1	
Подтверждение приема подсообщения #1	⇐		
	⇒		
Подтверждение приема подсообщения #2	⇐		Положительный ответ #2
Подтверждение приема подсообщения #2	⇒		
Подтверждение приема подсообщения #m	⇐		Положительный ответ #m
Подтверждение приема подсообщения #m	⇒		
Подтверждение приема подсообщения (не обязательно)	⇐	Положительный ответ (поле данных <255 байт)	
	⇒		
...			
Запрос передачи данных #n	⇒	Положительный ответ	
	⇐		
Запрос завершения передачи	⇒	Положительный ответ	
	⇐		
Запрос завершения обмена данными	⇒	Положительный ответ	
	⇐		

2.2.4 Временные параметры

DDP_019 Временные параметры для нормального режима работы указаны в таблице ниже:

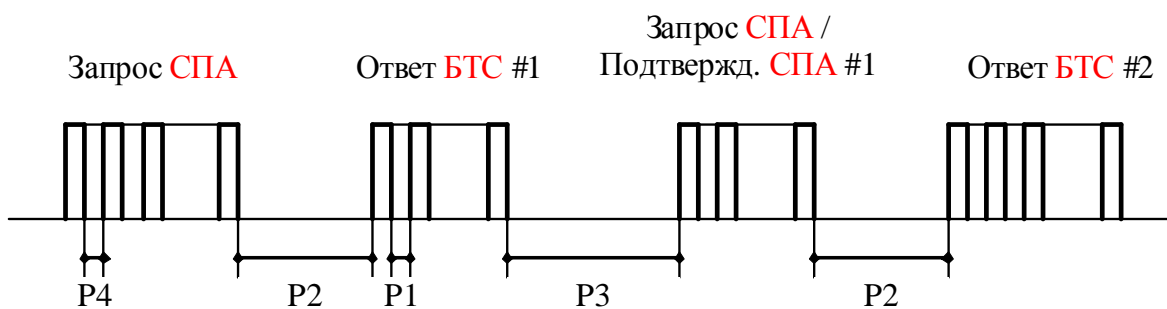


Рис. 1
Поток сообщений и временные параметры

Где:

P1 = Межбайтовый интервал для ответа БУ.

P2 = Время между окончанием запроса СПА и началом ответа БУ или между окончанием подтверждения СПА и началом следующего ответа БУ.

P3 = Время между окончанием ответа БУ и началом нового запроса СПА или между окончанием ответа БУ и началом подтверждения СПА, или между окончанием запроса СПА и началом нового запроса СПА при отсутствии ответа от БУ.

P4 = Межбайтовый интервал для запроса СПА.

P5 = 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).

Временной параметр	Нижнее предельное значение (мс)	Верхнее предельное значение (мс)
P1	0	20
P2	20	1000 *)
P3	10	5000
P4	5	20
P5	10	20 минут

*) если БУ выдает отрицательный ответ с кодом, означающим "запрос получен правильно – ожидается ответ", то это значение увеличивается до соответствующего верхнего предельного значения P3.

2.2.5 Обработка ошибок

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 Стадия инициализации обмена данными

DDP_020 Если СПА обнаруживает ошибку синхронизации или ошибку в битовом потоке на стадии инициализации обмена данными, то период ожидания СПА перед повторением запроса равняется $P3 \text{ min}$.

DDP_021 Если БУ обнаруживает ошибку в очередности сообщений от СПА, то оно не высылает ответа и ожидает нового сообщения с запросом инициализации обмена данными в течение периода, равного $P3 \text{ max}$.

2.2.5.2 Стадия обмена данными

На этой стадии можно выделить два типовых случая обработки ошибок:

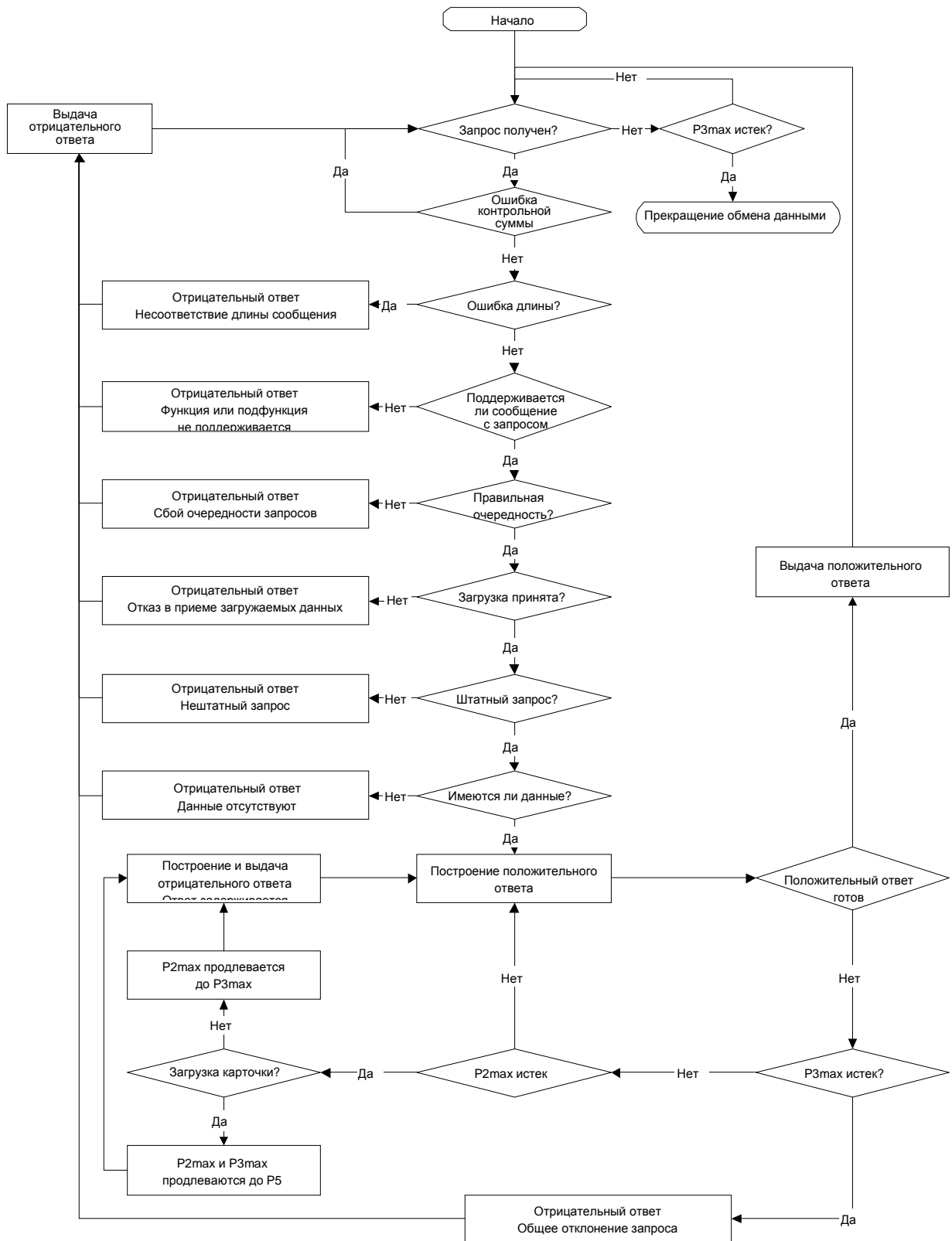
БУ обнаруживает ошибку в передаче данных от СПА

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 этом случае БУ высылает СПА отрицательный ответ с указанием характера ошибки.

Рис. 2
Обработка ошибок: БТС



2. СПА обнаруживает ошибку в передаче данных от БУ

DDP_025 СПА проверяет каждое полученное сообщение на ошибки синхронизации, ошибки в формате байтов (например, в стартовом и стоповом разрядах) и ошибки в передаче кадров (неверное число полученных байтов, ошибки в байте контрольной суммы).

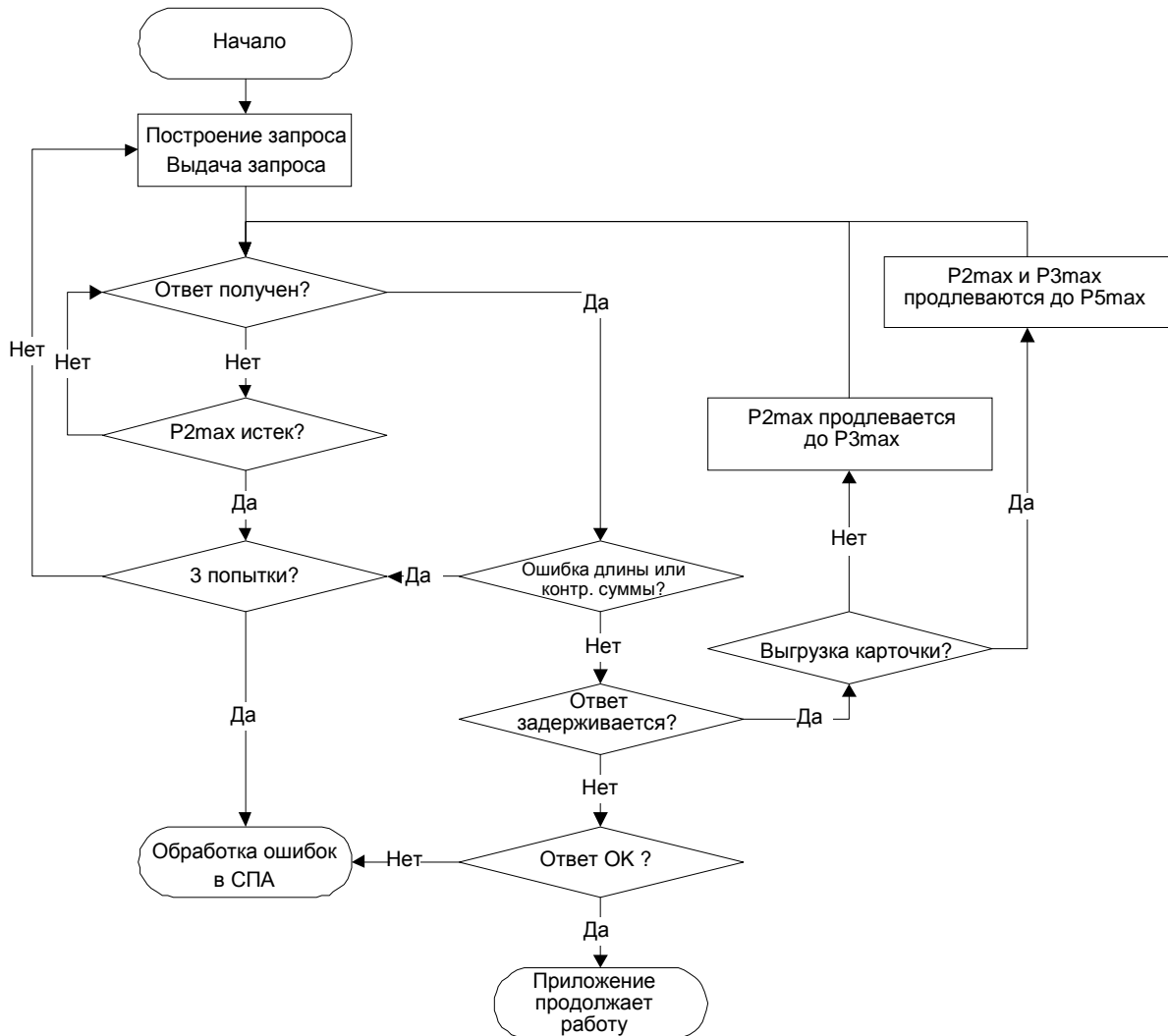
DDP_026 СПА проверяет поступающие сообщения на ошибки очередности, такие как сбой возрастания порядковых номеров подсообщений в последовательно поступающих сообщениях.

DDP_027 Если СПА обнаруживает ошибку или не получает от БУ ответа в течение периода, равного $P2_{max}$, то запрос высылается повторно, причем общее число передач ограничивается тремя. Для случаев обнаружения ошибок данного вида подтверждение приема подсообщения рассматривается как запрос к БУ.

DDP_028 Период ожидания СПА перед началом каждой передачи равняется или превышает $P3_{min}$; этот период отсчитывается с расчетного момента приема последнего стопового бита после обнаруженной ошибки.

Рис. 3

Обработка ошибок: СПА



2.2.6 Содержание ответного сообщения

В данном пункте указано содержание полей данных различных сообщений с положительным ответом.

Определения элементов данных приводятся в подразделе I (словарь данных).

2.2.6.1 *Positive Response Transfer Data Overview – Положительный ответ на запрос передачи 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:

Элемент данных	Длина (байт)	Примечания
MemberStateCertificate	194	Сертификаты защиты БУ
VUCertificate	194	
VehicleIdentificationNumber	17	Идентификационные данные транспортного средства
VehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
CurrentDateTime	4	Текущая дата и время согласно хронометражу БУ
VuDownloadablePeriod		Период, за который могут быть загружены данные
minDownloadableTime	4	
maxDownloadableTime	4	
CardSlotsStatus	1	Типы карточек, введенных в считывающее устройство БУ
VuDownloadActivityData		Предыдущая загрузка данных из БУ
downloadingTime	4	
fullCardNumber	18	
companyOrWorkshopName	36	
VuCompanyLocksData		Все сохраненные блокировки, установленные предприятием. Если раздел не заполнен, высылается только noOfLocks = 0.
noOfLocks	1	
...	(98)	
BU Company Locks Record		
lockInTime	4	
lockOutTime	4	
companyName	36	
companyAddress	36	
companyCardNumber	18	
::		
VuControlActivityData		Все сохраненные в БУ контрольные записи. Если раздел не заполнен, высылается только noOfControls = 0.
noOfControls	1	
::	(31)	
BU Control Activity Record		
controlType	1	
controlTime	4	
controlCardNumber	18	
downloadPeriodBeginTime	4	
downloadPeriodEndTime	4	
::		

Подпись

128

Подпись криптосистемы RSA для всех данных (кроме сертификатов), от VehicleIdentificationNumber до последнего байта последней VuControlActivityRecord.

2.2.6.2 *Positive Response Transfer Data Activities – Положительный ответ на запрос передачи данных о деятельности водителей*

DDP_030 В поле данных сообщения "Положительный ответ на запрос передачи данных о деятельности водителей" включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 02 Hex, с соответствующим выделением и нумерацией подсообщений:

Элемент данных	Длина (байт)	Примечания
TimeReal	4	Дата загрузки
OdometerValueMidnight	3	Показания счетчика пробега на конец суток, к которым относятся загружаемые данные.
VuCardIWData		Информация о циклах ввода/извлечения карточек.
noOfVuCardIWRecords	2	– Если в разделе нет данных, высылается только noOfVuCardIWRecords = 0. – Если внутри периода, охватываемого записью VuCardIWRecord, находится отметка 00:00 часов (карточка введена накануне) или 24:00 часа (карточка извлечена на следующий день), эта запись в полном объеме включается в данные за оба дня.
...	(129)	
cardHolderName	36	
holderSurname	36	
holderFirstNames	18	
fullCardNumber	4	
cardExpiryDate	4	
cardInsertionTime	3	
vehicleOdometerValueAtInsertion	1	
cardSlotNumber	4	
cardWithdrawalTime	3	
vehicleOdometerValueAtWithdrawal	1	
previousVehicleInfo	14	
vehicleRegistrationIdentification	4	
vehicleRegistrationNation	1	
vehicleRegistrationNumber	4	
cardWithdrawalTime	1	
manualInputFlag		
...		
VuActivityDailyData		Состояние считывающего устройства на 00:00 часов и изменения в деятельности водителей, зарегистрированные в течение суток, к которым относятся загружаемые данные.
noOfActivityChanges	2	
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		Информация о географических пунктах, зарегистрированная в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылается только noOfPlaceRecords = 0.
noOfPlaceRecords	1	
...	(28)	
fullCardNumber	18	
placeRecord	4	
entryTime	1	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		

VuSpecificConditionData			
noOfSpecificConditionRecords	2		Информация об особых ситуациях, зарегистрированная в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылается только noOfSpecificConditionRecords=0
...	(5)		
SpecificConditionRecord			
entryTime	4		
specificConditionType	1		
...			
Подпись	128		Подпись криптосистемы RSA для всех данных, от TimeReal до последнего байта последней записи об особых ситуациях.

2.2.6.3 Positive Response Transfer Data Events and Faults – 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:

Элемент данных		Длина (байт)	Примечания
VuFaultData			Вся сохраненная в БУ и текущая информация о неисправностях. Если раздел не заполнен, высылается только noOfVuFaults = 0.
noOfVuFaults	1		
...	(82)		
VuFaultRecord	faultType	1	
	faultRecordPurpose	1	
	faultBeginTime	4	
	faultEndTime	4	
	cardNumberDriverSlotBegin	18	
	cardNumberCodriverSlotBegin	18	
	cardNumberDriverSlotEnd	18	
cardNumberCodriverSlotEnd	18		
...			
VuEventData			Вся сохраненная в БУ и текущая информация о событиях (кроме превышений скорости). Если раздел не заполнен, высылается только noOfVuEvents = 0.
noOfVuEvents	1		
...	(83)		
ntReco			
eventType	1		
eventRecordPurpose	1		
eventBeginTime	4		

eventEndTime	4		
cardNumberDriverSlotBegin	18		
cardNumberCodriverSlotBegin	18		
cardNumberDriverSlotEnd	18		
cardNumberCodriverSlotEnd	18		
similarEventsNumber	1		
...			
VuOverSpeedingControlData			
lastOverspeedControlTime	4	Данные, относящиеся к последнему контролю за превышениями скорости (при отсутствии данных – значение по умолчанию).	
firstOverspeedSince	4		
numberOfOverspeedSince	1		
VuOverSpeedingEventData			
noOfVuOverSpeedingEvents	1	Вся сохраненная в БУ и текущая информация о превышениях скорости. Если раздел не заполнен, высылается только noOfVuOverSpeedingEvents = 0.	
...	(31)		
VuOverSpeeding EventRecord	eventType		1
	eventRecordPurpose		1
	eventBeginTime		4
	eventEndTime		4
	maxSpeedValue		1
	averageSpeedValue		1
	CardNumberDriverSlotBegin		18
similarEventsNumber	1		
...			
VuTimeAdjustmentData			
noOfVuTimeAdjRecords	1	Вся сохраненная в БУ информация о корректировках времени (кроме производимых в процессе общей калибровки). Если раздел не заполнен, высылается только noOfVuTimeAdjRecords = 0.	
...	(98)		
VuTime Adjustment Record	oldTimeValue		4
	newTimeValue		4
	workshopName		36
	workshopAddress		36
workshopCardNumber	18		
...			
Подпись	128	Подпись криптосистемы RSA для всех данных, от noOfVuFaults до последнего байта последней записи о корректировках времени.	

2.2.6.4 *Positive Response Transfer Data Detailed Speed – Положительный ответ на запрос передачи подробных данных о скоростном режиме*

DDP_032 В поле данных сообщения "Положительный ответ на запрос передачи подробных данных о скоростном режиме" включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 04 Hex, с соответствующим выделением и нумерацией подсообщений:

Элемент данных		Длина (байт)	Примечания
VuDetailedSpeedData			
noOfSpeedBlocks		2	Вся сохраненная в БУ подробная информация о скоростном режиме (один блок данных о скорости за каждую минуту движения транспортного средства); 60 значений скорости в минуту (по одному в секунду).
...			
VuDetailed SpeedBlock	speedBlockBeginDate	4	
	speedsPerSecond	60	
...			
Подпись		128	Подпись криптосистемы RSA для всех данных, от noOfSpeedBlocks до последнего байта последнего блока данных о скорости.

2.2.6.5 *Positive Response Transfer Data Technical Data – Положительный ответ на запрос передачи технических данных*

DDP_033 В поле данных сообщения "Положительный ответ на запрос передачи технических данных" включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 05 Hex, с соответствующим выделением и нумерацией подсообщений:

Элемент данных	Длина (байт)	Примечания
VuIdentification vuManufacturerName vuManufacturerAddress vuPartNumber vuSerialNumber vuSoftwareIdentification vuSoftwareVersion vuSoftInstallationDate vuManufacturingDate vuApprovalNumber	36 36 16 8 4 4 4 8	
SensorPaired sensorSerialNumber sensorApprovalNumber sensorPairingDateFirst	8 8 4	
VuCalibrationData noOfVuCalibrationRecords ... VuCalibrationRecord calibrationPurpose workshopName workshopAddress workshopCardNumber workshopCardExpiryDate vehicleIdentificationNumber vehicleRegistrationIdentification vehicleRegistrationNation vehicleRegistrationNumber wVehicleCharacteristicConstant kConstantOfRecordingEquipment lTyreCircumference tyreSize authorisedSpeed oldOdometerValue newOdometerValue oldTimeValue newTimeValue nextCalibrationDate ...	1 (167) 1 36 36 18 4 17 1 14 2 2 2 15 1 3 3 4 4 4	Все сохраненные в БУ калибровочные записи.
Подпись	128	Подпись криптосистемы RSA для всех данных, от vuManufacturerName до последнего байта последней VuCalibrationRecord.

2.3 Сохранение данных на ВН

DDP_034 В случаях, когда сеанс загрузки данных включает передачу данных с БУ, СПА сохраняет в виде одного физического файла все данные, полученные от БУ в ходе сеанса загрузки в сообщениях типа "Положительный ответ на запрос передачи данных". Сохраняемые данные не включают заголовки сообщений, счетчики подсообщений, пустые подсообщения и контрольные суммы, но включают SID и TREP (при наличии нескольких подсообщений – только для первого подсообщения).

3. Протокол загрузки данных с карточек тахографа

3.1 Сфера применения

В настоящем пункте изложен порядок прямой загрузки данных с карточки тахографа на СПА. СПА не является частью защищенной среды; поэтому процедура аутентификации между карточкой и СПА не предусмотрена.

3.2 Определения

Сеанс загрузки: Каждая загрузка данных с МПК. Сеанс включает всю процедуру, от перезапуска карточки считывающим устройством до деактивации МПК (т.е. извлечения или новой перезагрузки карточки).

Подписанный файл данных: Файл, полученный с МПК. Файл передается на УСК в текстовой форме. В МПК файл хешируется и подписывается; подпись высылается на УСК.

3.3 Загрузка данных с карточки

DDP_035 Процесс загрузки данных с карточки тахографа состоит из следующих этапов:

- Загрузка общей информации, записанной на карточке в элементарных файлах ISS и IC. Эта информация не является обязательной и не защищена цифровой подписью.
- Загрузка элементарных файлов Card_Certificate и CA_Certificate. Эта информация не защищена цифровой подписью.

Вышеуказанные файлы загружаются в обязательном порядке при каждом сеансе загрузки.

- Загрузка элементарных файлов с другими прикладными данными (входящих в каталог тахографа), кроме файла 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,
 - 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 обнуляется счетчик калибровок в элементарном файле Card_Download.

3.3.1 Процедура инициализации

DDP_036 СПА запускает процедуру следующим образом:

Карточка	Направл.	СПА / УСК	Пояснение / Примечания
	↶	Перезапуск аппаратуры	
ATR	↷		

Возможно использование ВПП для переключения на более высокую скорость передачи данных, если она поддерживается МПК.

3.3.2 Процедура для неподписанных файлов данных

DDP_037 Процедура загрузки элементарных файлов ICC, IC, Card_Certificate и CA_Certificate выглядит следующим образом:

Карточка	Направл.	СПА / УСК	Пояснение / Примечания
	↵	Выбор файла	Выбор файла по идентификаторам
ОК	⇒		
	↵	Считывание данных	Если объем данных файла превышает емкость буфера считывающего устройства или карточки, команда повторяется до тех пор, пока не будет считан весь файл.
Данные файла ОК	⇒	Сохранение данных на ВН	В соответствии с 3.4 (3.4 Формат сохранения данных)

Примечание: перед выбором элементарного файла Card_Certificate необходимо выбрать приложение "Тахограф" (выбор по ИП).

3.3.3 Процедура для подписанных файлов данных

DDP_038 Для каждого из нижеперечисленных файлов, загружаемых вместе с соответствующей подписью, применяется следующая процедура:

Карточка	Напр.	СПА / УСК	Пояснение / Примечания
	↵	Выбор файла	
ОК	⇒		
	↵	Расчет хеш-функции	Рассчитывает хеш-функцию по данным, содержащимся в выбранном файле, на основе хеш-алгоритма, предписанного в соответствии с подразделом 11. Эта команда не является ISO-командой.
Расчет и временное сохранение хеш-функции файла			
ОК	⇒		
	↵	Считывание данных	Если объем данных файла превышает емкость буфера считывающего устройства или

			карточки, команда повторяется до тех пор, пока не будет считан весь файл.
Данные файла OK	⇒	Сохранение полученных данных на ВН	В соответствии с 3.4 (3.4 Формат сохранения данных)
	⇐	PSO: Расчет цифровой подписи	
На основе временно сохраненной хеш-функции выполняется защитная операция "Генерировать цифровую подпись"			
Подпись OK	⇒	Данные приобщаются к данным, сохраненным на ВН ранее	В соответствии с 3.4 (3.4 Формат сохранения данных)

3.3.4 Процедура обнуления счетчика калибровок

DDP_039 Для обнуления счетчика NoOfCalibrationsSinceDownload в элементарном файле Card_Download, хранящемся на карточке мастерской, применяется следующая процедура:

Карточка	Напр.	СПА / УСК	Пояснение / Примечания
	⇐	Выбор файла Card_Download	Выбор файла по идентификаторам
OK	⇒		
	⇐	Считывание файла NoOfCalibrationsSinceDownload = '00 00'	
Обнуление счетчика сеансов загрузки данных с карточки			
OK	⇒		

3.4 Формат сохранения данных

3.4.1 Введение

DDP_040 Загружаемые данные должны сохраняться с соблюдением следующих требований:

- 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 файлов

DDP_041 Формат файла представляет собой совокупность нескольких взаимосвязанных TLV-объектов.

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, то никакая информация о нем сохранению не подлежит (т.е. не сохраняется ни метка, ни нулевой параметр длины).

DDP_046 В качестве TLV-объекта, следующего непосредственно за TLV-объектом с данными файла, сохраняется подпись.

Определение	Пояснение	Длина
FID (2 байта) „00“	Метка EF (FID)	3 байта
FID (2 байта) „01“	Метка подписи EF (FID)	3 байта
Xx xx	Длина поля значений	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 карточек тахографа через бортовое устройство

DDP_047 БУ должно обеспечивать возможность загрузки данных с введенной в него карточки водителя на подключенную СПА.

DDP_048 Для инициализации данного режима СПА направляет БУ сообщение "Transfer Data Request Card Download" – "Запрос передачи данных, загруженных 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 определен в пункте 0, и передает все полученные таким образом данные на СПА в соответствующем TLV-формате (см. 3.4.2), заключенные внутри сообщения "Положительный ответ на запрос передачи данных".

DDP_050 СПА извлекает данные карточки из сообщения "Положительный ответ на запрос передачи данных" (освобождая их от всех заголовков, SIDов, TREPов, счетчиков 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 файла Card_Download на карточке водителя.

ПОДРАЗДЕЛ VIII
ПРОТОКОЛ КАЛИБРОВКИ

СОДЕРЖАНИЕ

	<u>Стр.</u>
1. Введение	295
2. Термины, определения и источники	295
3. Обзор функций	296
3.1 Перечень имеющихся функций	296
3.2 Коды ответов	297
4. Функции обмена данными	297
4.1 Функция StartCommunication	298
4.2 Функция StopCommunication	302
4.2.1 Описание сообщения	302
4.2.2 Формат сообщений	302
4.2.3 Определение параметров.....	303
4.3 Функция TesterPresen.....	304
4.3.1 Описание сообщения	304
4.3.2 Формат сообщений	304
5. Административные функции	306
5.1 Функция StartDiagnosticSession	306
5.1.1 Описание сообщения	306
5.1.2 Формат сообщений	307
5.1.3 Определение параметров.....	308
5.2 Функция SecurityAccess (защищенный доступ).....	309
5.2.1 Описание сообщения	310
5.2.2 Формат сообщений SecurityAccess - requestSeed	311
5.2.3 Формат сообщений SecurityAccess - sendKey	313
6. Функции передачи данных.....	315
6.1 Функция ReadDataByIdentifier	315
6.1.1 Описание сообщения	315
6.1.2 Формат сообщений	315

СОДЕРЖАНИЕ (продолжение)

	<u>Стр.</u>
6.1.3	Определение параметров..... 316
6.2	Функция WriteDataByIdentifier 318
6.2.1	Описание сообщения 318
6.2.2	Формат сообщений 319
6.2.3	Определение параметров..... 320
7.	Настройка проверочных импульсов – функциональный блок регулировки входного/выходного сигнала 320
7.1	Функция InputOutputControlByIdentifier 321
7.1.1	Описание сообщения 321
7.1.2	Формат сообщений 322
7.1.3	Определение параметров..... 324
8.	Форматы dataRecords (записей данных) 325
8.1	Диапазоны передаваемых параметров 325
8.2	Форматы dataRecords 326

1. Введение

В настоящем подразделе рассматривается процесс обмена данными между бортовым устройством и тестером по К-линии, предусмотренной в калибровочном интерфейсе, описание которого приводится в подразделе VI. В нем также указан способ управления каналом ввода-вывода на калибровочном разъеме.

Процедура установления связи по К-линии описана в пункте 4 "Функции обмена данными".

Для определения задач управления обменом данными по К-линии при различных условиях в данном подразделе 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 на бортовом устройстве невозможно.

Выбор вида диагностического сеанса рассмотрен в пункте 5 ("Административные функции").

CPR_001 Сеанс "ECUProgrammingSession" позволяет вводить данные в бортовое устройство. При этом для ввода калибровочных данных (требования 097 и 098) бортовое устройство должно быть переведено в режим CALIBRATION.

Процесс передачи данных по К-линии описан в пункте 6 ("Функции передачи данных"). Форматы передаваемых данных подробно указаны в пункте 8 ("Форматы записей данных").

CPR_002 Сеанс "ECUAdjustmentSession" позволяет выбирать режим работы канала ввода-вывода калибровочных данных через интерфейс К-линии. Способ управления каналом ввода-вывода калибровочных данных изложен в пункте 7 ("Настройка проверочных импульсов – функциональный блок регулировки входного/выходного сигнала").

CPR_003 Адрес тестера везде в настоящем документе обозначен как 'tt'. Хотя для тестеров могут существовать общепринятые адреса, БУ должно быть способно правильно поддерживать связь с тестером по любому адресу. Физический адрес БУ - 0xEE.

2. Термины, определения и источники

Протоколы, сообщения и коды ошибок в основном соответствуют нынешней версии проекта стандарта ISO 14229-1 (Транспорт дорожный. Системы диагностического контроля. Часть 1. Диагностические функции. Версия 6 от 22 февраля 2001 года).

Для идентификаторов функций, запросов функций и ответов на них, а также для стандартных параметров используются 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.

Источники:

ISO 14230-2 Транспорт дорожный. Системы диагностического контроля. Протокол ключевых слов 2000. Часть 2. Уровень обмена данными. Первое издание, 1999 год. Транспортные средства. Системы диагностического контроля.

3. Обзор функций

3.1 Перечень имеющихся функций

В таблице ниже представлен обзорный перечень функций, которые должны быть предусмотрены в контрольном устройстве и определения которых приводятся в настоящем документе.

CPR_004 В таблице показаны функции, доступные после начала диагностического сеанса.

- В **1-м столбце** приведен перечень имеющихся функций.
- Во **2-м столбце** перечислены номера пунктов данного подраздела, содержащих развернутые определения соответствующих функций.
- В **3-м столбце** указаны значения идентификаторов соответствующих функций, используемые в запросах.
- В **4-м столбце** указаны функции сеанса "**StandardDiagnosticSession**" (SD), которые должны быть реализованы в каждом БУ.
- В **5-м столбце** указаны функции сеанса "**ECUAdjustmentSession**" (ECUAS), которые должны быть реализованы для обеспечения возможности управления каналом ввода-вывода калибровочного разъема на передней панели БУ.
- В **6-м столбце** указаны функции сеанса "**ECUProgrammingSession**" (ECUPS), которые должны быть выполнены для обеспечения возможности программирования параметров работы БУ.

Таблица 1

Сводная таблица идентификаторов функций

Название диагностической функции	№. пунктов	Идент. функции д/запроса	Диагностические сеансы		
			SD	ECUAS	ECUPS
StartCommunication	<u>4.1</u>	81	■	■	■
StopCommunication	<u>4.2</u>	82	■		
TesterPresent	<u>4.3</u>	3E	■	■	■
StartDiagnosticSession	<u>5.1</u>	10	■	■	■
SecurityAccess	<u>5.2</u>	27	■	■	■
ReadDataByIdentifier	<u>6.1</u>	22	■	■	■
WriteDataByIdentifier	<u>6.2</u>	2E			■
InputOutputControlByIdentifier	<u>7.1</u>	2F		■	

- Символ, означающий обязательность функции для данного диагностического сеанса.

Отсутствие символа означает, что в процессе данного диагностического сеанса указанная функция невозможна.

3.2 Коды ответов

Для каждой функции предусмотрены определенные коды ответов.

4. Функции обмена данными

Ряд функций необходимы для установления и поддержания канала обмена данными. На уровне приложений они не отображаются. Описание имеющихся функций приведено в таблице ниже.

Таблица 2
Функции обмена данными

Название функции	Описание
StartCommunication	Запрос клиента на инициализацию сеанса обмена данными с сервером(ами).
StopCommunication	Запрос клиента на прекращение текущего сеанса обмена данными.
TesterPresent	Сообщение клиента серверу о продолжении своего присутствия на линии.

CPR_005 Функция StartCommunication используется для инициализации обмена данными. Для выполнения любой функции необходимо начать обмен данными и обеспечить, чтобы его параметры соответствовали нужному режиму.

4.1 Функция StartCommunication

CPR_006 По получении примитива индикации StartCommunication БУ проверяет возможность инициализации запрошенного канала обмена данными при существующих условиях. Описание условий, необходимых для инициализации канала обмена данными, приведено в документе ISO 14230-2.

CPR_007 После этого БУ выполняет все действия, необходимые для инициализации канала обмена данными, и возвращает примитив ответа StartCommunication с выбранными параметрами положительного ответа.

CPR_008 Если на БУ, которое уже инициализовано (и уже находится в процессе того или иного диагностического сеанса), поступает новый запрос StartCommunication (например, при восстановлении работы тестера после сбоя), то этот запрос принимается и производится повторная инициализация БУ.

CPR_009 Если по каким-либо причинам канал обмена данными не может быть инициализован, то БУ продолжает функционировать в том же режиме, в котором оно находилось непосредственно перед попыткой инициализации канала обмена данными.

CPR_010 Сообщение с запросом StartCommunication должно иметь физическую адресацию.

CPR_011 Инициализация БУ для выполнения соответствующих функций производится методом "ускоренной инициализации":

- любой операции предшествует определенный период бездействия шины;
- затем тестер высылает шаблон инициализации;
- ответ БУ содержит всю информацию, необходимую для установления канала обмена данными.

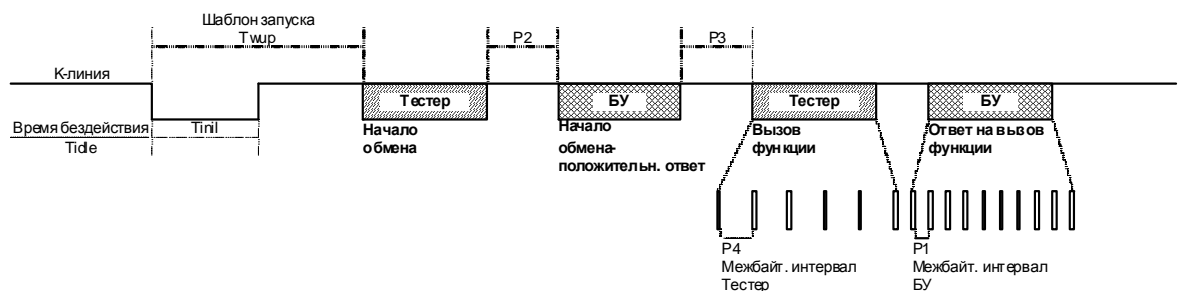
CPR_012 По завершении инициализации

значения всех параметров обмена данными задаются такими, как определено в

- в соответствии с байтами ключей;
- 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 T_{in1} . Тестер высылает первый бит сообщения StartCommunicationService по истечении периода T_{wup} с момента первого спада тактового сигнала.



CPR_017 Значения временных параметров ускоренной инициализации и обмена данными в целом приведены в нижеследующих таблицах. Время бездействия может быть различным:

- от включения питания до первой передачи данных: Tidle = 300 мс;
- после завершения функции StopCommunication: Tidle = P3 мин;
- после прекращения обмена данными из-за превышения времени ожидания P3 max: Tidle = 0.

Таблица 3

Временные параметры ускоренной инициализации

Параметр		мин. значение	макс. значение
Tinil	25 ± 1 мс	24 мс	26 мс
Twup	50 ± 1 мс	49 мс	51 мс

Таблица 4

Временные параметры обмена данными

Временной 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

CPR_018 Формат сообщений для ускоренной инициализации подробно указан в нижеследующих таблицах.

Таблица 5

Запрос StartCommunication

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	81	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Идентификатор функции запроса StartCommunication	81	SCR
#5	Контрольная сумма	00-FF	CS

Таблица 6

Положительный ответ на запрос StartCommunication

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции положительного ответа на запрос StartCommunication	C1	SCRPR
#6	Байт ключа 1	EA	KB1
#7	Байт ключа 2	8F	KB2
#8	Контрольная сумма	00-FF	CS

CPR_019 Отрицательный ответ на запрос StartCommunication невозможен. При отсутствии положительного ответа инициализация БУ не происходит, никакие сообщения не передаются, и устройство продолжает функционировать в обычном режиме.

4.2 Функция StopCommunication

4.2.1 Описание сообщения

Эта функции 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, то в этом случае БУ выполняет все действия, необходимые для прекращения сеанса обмена данными.

CPR_021 Если обмен данными может быть прекращен, то перед прекращением обмена данными БУ возвращает примитив ответа StopCommunication с выбранными параметрами положительного ответа.

CPR_022 Если по каким-либо причинам прекращение обмена данными невозможно, то БУ возвращает примитив ответа StopCommunication с выбранными параметрами отрицательного ответа.

CPR_023 Если БУ фиксирует истечение периода ожидания $R3max$, то обмен данными прекращается без направления какого-либо примитива ответа.

4.2.2 Формат сообщений

CPR_024 Форматы сообщений для примитивов StopCommunication подробно указаны в нижеследующих таблицах.

Таблица 7

Запрос StopCommunication

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	01	LEN
#5	Идентификатор функции запроса StopCommunication	82	SPR
#6	Контрольная сумма	00-FF	CS

Таблица 8

Положительный ответ на запрос StopCommunication

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	01	LEN
#5	Идентификатор функции положительного ответа на запрос StopCommunication	C2	SPRPR
#6	Контрольная сумма	00-FF	CS

Таблица 9

Отрицательный ответ на запрос StopCommunication

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса StopCommunication	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Контрольная сумма	00-FF	CS

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 счетчик времени P3 обнуляется при каждом очередном поступлении этого запроса.

4.3.2 Формат сообщений

CPR_079 Форматы сообщений для примитивов TesterPresent подробно указаны в нижеследующих таблицах.

Таблица 10

Запрос TesterPresent

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	02	LEN
#5	Идентификатор функции запроса TesterPresent	3E	TP
#6	Подфункция = responseRequired да (требуется ответ) нет	01 02	RESPREQ_Y RESPREQ_NO
#7	Контрольная сумма	00-FF	CS

CPR_080 Если параметр responseRequired установлен на ответ "да", то сервер возвращает положительный ответ, показанный ниже. Если параметр установлен на ответ "нет", то на данный запрос сервер не отвечает.

Таблица 11

Положительный ответ на запрос TesterPresent

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	01	LEN
#5	Идентификатор функции положительного ответа на запрос TesterPresent	7E	TPPR
#6	Контрольная сумма	00-FF	CS

CPR_081 В данной функции предусмотрены следующие коды возможного отрицательного ответа:

Таблица 12

Отрицательный ответ на запрос TesterPresent

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса TesterPresent	3E	TP
#7	ResponseCode (код ответа) = [SubFunctionNotSupported- InvalidFormat incorrectMessageLength] (подфункция не поддерживается-неправильный формат- неверная длина сообщения)	12 13	RC_SFNS_IF RC_IML
#8	Контрольная сумма	00-FF	CS

5. Административные функции

Описание имеющихся функций приводится в таблице ниже.

Таблица 13

Административные функции

Название функции	Описание
StartDiagnosticSession	Клиент запрашивает инициализацию диагностического сеанса с БУ.
SecurityAccess	Клиент запрашивает доступ к функциям, предназначенным только для санкционированных пользователей.

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 определенному набору функций, согласно указанному в таблице 17. Некоторые функции, возможные в ходе таких сеансов, специфичны для транспортных средств конкретных изготовителей и в настоящем документе не рассматриваются. Правила технической реализации соответствующих систем должны отвечать следующим требованиям:

- БУ 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, то стандартный сеанс диагностики продолжается до тех пор, пока питание БУ не будет отключено;
- если тестером запрашивается уже запущенный диагностический сеанс, то БУ возвращает положительный ответ;
- если тестером запрашивается новый диагностический сеанс, то БУ сначала высылает положительный ответ на запрос StartDiagnosticSession, а затем запускает новый сеанс. Если БУ не 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, определенные в таблице, начинают применяться после успешного выполнения запроса StartDiagnosticSession, в котором параметр diagnosticSession был установлен на “StandardDiagnosticSession” (стандартный сеанс диагностики), если до этого выполнялся другой диагностический сеанс.

5.1.2 Формат сообщений

CPR_028 Формат сообщений для примитивов StartDiagnosticSession подробно указан в нижеследующих таблицах.

Таблица 14
Административные функции

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	02	LEN
#5	Идентификатор функции запроса StartDiagnosticSession	10	STDS
#6	DiagnosticSession (диагностический сеанс) = [одно из значений в Таблице 17]	xx	DS_...
#7	Контрольная сумма	00-FF	CS

Таблица 15
Положительный ответ на запрос StartDiagnosticSession

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	02	LEN
#5	Идентификатор функции положительного ответа на запрос StartDiagnosticSession	50	STDSPR
#6	DiagnosticSession (диагностический сеанс) = [то же значение, что и у байта #6 в Таблице 14]	xx	DS_...
#7	Контрольная сумма	00-FF	CS

Таблица 16

Отрицательный ответ на запрос StartDiagnosticSession

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса StartDiagnosticSession	10	STDS
#7	ResponseCode = [subFunctionNotSupported ^a (код ответа) (подфункция не поддерживается)	12	RC_SFNS
	incorrectMessageLength ^b (неверная длина сообщения)	13	RC_IML
	conditionsNotCorrect ^c (недопустимые условия)	22	RC_CNC
#8	Контрольная сумма	00-FF	CS

^a – значение, заданное в байте #6 запроса, не поддерживается и поэтому не фигурирует в таблице 17,

^b – длина сообщения не соответствует ожидаемой,

^c – не соблюдены критерии выполнения запроса StartDiagnosticSession.

5.1.3 Определение параметров

CPR_029 Параметр *diagnosticSession (DS_)* используется функцией StartDiagnosticSession для выбора того или иного режима работы сервера(ов). В настоящем документе указаны его значения для следующих видов диагностических сеансов:

Таблица 17

Определение значений параметра diagnosticSession

Шестн. значение	Описание	Мнемокод
81	<p>StandardDiagnosticSession (стандартный диагностический сеанс).</p> <p>В ходе данного диагностического сеанса могут использоваться все функции, указанные в столбце 4 ("SD") таблицы 1. Эти функции позволяют считывать данные, хранящиеся на сервере (БУ). Данный диагностический сеанс запускается после успешного завершения инициализации канала связи между клиентом (тестер) and сервером (БУ). Этот сеанс может быть впоследствии заменен другими диагностическими сеансами, о которых говорится в настоящем пункте.</p>	SD
85	<p>ECUProgrammingSession (сеанс программирования контрольной аппаратуры).</p> <p>В ходе данного диагностического сеанса могут использоваться все функции, указанные в столбце 6 ("ECUPS") таблицы 1. Эти функции обеспечивают программирование памяти сервера (БУ). Данный диагностический сеанс может быть впоследствии заменен другими диагностическими сеансами, о которых говорится в настоящем пункте.</p>	ECUPS
87	<p>ECUAdjustmentSession (сеанс настройки контрольной аппаратуры).</p> <p>В ходе данного диагностического сеанса могут использоваться все функции, указанные в столбце 5 ("ECUAS") таблицы 1. Эти функции обеспечивают регулировку параметров входного/выходного сигнала сервера (БУ). Данный диагностический сеанс может быть впоследствии заменен другими диагностическими сеансами, о которых говорится в настоящем пункте.</p>	ECUAS

5.2 Функция SecurityAccess (защищенный доступ)

Запись калибровочных данных и доступ к каналу ввода/вывода этих данных возможны лишь при условии, что БУ находится в режиме CALIBRATION (калибровка). Для получения доступа к режиму CALIBRATION необходимо, помимо ввода в БУ действительной карточки мастерской, ввести в бортовое устройство соответствующий PIN-код.

Функция SecurityAccess обеспечивает возможность введения PIN-кода и получения тестером информации о том, находится ли БУ в режиме CALIBRATION.

Допустимы и другие методы введения PIN-кода.

5.2.1 Описание сообщения

Функция SecurityAccess предусматривает направление сообщения SecurityAccess "requestSeed" (запрос стартового значения для генерации ключа), за которым на соответствующем этапе следует сообщение SecurityAccess "sendKey" (передача ключа). Функция SecurityAccess выполняется в обязательном порядке после функции StartDiagnosticSession.

CPR_033 Сообщение SecurityAccess "requestSeed" используется тестером для проверки готовности бортового устройства к приему PIN-кода.

CPR_034 Если бортовое устройство уже находится в режиме CALIBRATION, то в ответ на запрос оно при помощи функции положительного ответа SecurityAccess возвращает стартовое значение 0x0000.

CPR_035 Если бортовое устройство готово принять PIN-код для проверки с помощью карточки мастерской, то оно при помощи функции положительного ответа SecurityAccess возвращает стартовое значение, превышающее 0x0000.

CPR_036 Если бортовое устройство не готово принять от тестера PIN-код, поскольку карточка мастерской недействительна или не была введена в устройство, либо потому, что бортовое устройство ожидает введения PIN-кода другим способом, то оно возвращает отрицательный ответ с кодом conditionsNotCorrectorRequestSequenceError (недопустимые условия или неверная последовательность запросов).

CPR_037 В таких случаях тестер передает PIN-код на бортовое устройство с помощью сообщения SecurityAccess "sendKey". Для обеспечения достаточного времени, необходимого для завершения процесса аутентификации карточки, БУ использует код отрицательного ответа requestCorrectlyReceived-ResponsePending (запрос получен правильно – ожидается ответ), 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 PIN-кода;

invalidKey: неверный PIN-код; допустимое количество попыток подтверждения PIN-кода не превышено;

exceededNumberOfAttempts: неверный PIN-код; допустимое количество попыток подтверждения PIN-кода превышено;

generalReject: PIN-код верен, но взаимную аутентификацию устройства и карточки мастерской произвести не удалось.

5.2.2 Формат сообщений SecurityAccess –requestSeed

CPR_040 Форматы сообщений для примитивов SecurityAccess "requestSeed" подробно указаны в нижеследующих таблицах.

Таблица 18
Запрос SecurityAccess –requestSeed

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	02	LEN
#5	Идентификатор функции запроса SecurityAccess	27	SA
#6	accessType (тип доступа) – requestSeed	7D	AT_RSD
#7	Контрольная сумма	00-FF	CS

Таблица 19
Положительный ответ на запрос SecurityAccess – requestSeed

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	04	LEN
#5	Идентификатор функции положительного ответа на запрос SecurityAccess	67	SAPR
#6	accessType (тип доступа) – requestSeed	7D	AT_RSD
#7	Стартовое значение - верхний байт	00-FF	SEEDH
#8	Стартовое значение - нижний байт	00-FF	SEEDL
#9	Контрольная сумма	00-FF	CS

Таблица 20
Отрицательный ответ на запрос SecurityAccess

# байта	Параметр	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса SecurityAccess	27	SA
#7	responseCode (код ответа) = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength]	22 13	RC_CNC RC_IML
#8	Контрольная сумма	00-FF	CS

5.2.3 Формат сообщений SecurityAccess – sendKey

CPR_041 Форматы сообщений для примитивов SecurityAccess "sendKey" подробно указаны в нижеследующих таблицах.

Таблица 21
Запрос SecurityAccess – sendKey

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	m+2	LEN
#5	Идентификатор функции запроса SecurityAccess	27	SA
#6	accessType (тип доступа) – sendKey	7E	AT_SK
#7 to #m+6	Ключ #1 (верхний) ... Key #m (нижний, m должно составлять не менее 4 и не более 8)	xx ... xx	KEY
#m+7	Контрольная сумма	00-FF	CS

Таблица 22

Положительный ответ на запрос SecurityAccess – sendKey

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	02	LEN
#5	Идентификатор функции положительного ответа на запрос SecurityAccess	67	SAPR
#6	accessType (тип доступа) – sendKey	7E	AT_SK
#7	Контрольная сумма	00-FF	CS

Таблица 23

Отрицательный ответ на запрос SecurityAccess

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса SecurityAccess	27	SA
#7	ResponseCode (код ответа) = [generalReject	10	RC_GR
	subFunctionNotSupported	12	RC_SFNS
	(подфункция не поддерживается)		
	incorrectMessageLength	13	RC_IML
	(неверная длина сообщения)		
#7	conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	invalidKey	35	RC_IK
#7	(недопустимые условия – ошибка в запросе – недействительный ключ)		
	exceededNumberOfAttempts	36	RC_ENA
#7	(превышение числа попыток)		
	requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#7	(запрос получен правильно – ожидается ответ)		
	#8	Контрольная сумма	00-FF

6. Функции передачи данных

Описание имеющихся функций приведено в таблице ниже.

Таблица 24
Функции передачи данных

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.

6.1 Функция ReadDataByIdentifier

6.1.1 Описание сообщения

CPR_050 Функция ReadDataByIdentifier используется клиентом с целью запроса у сервера значения записей данных. Данные опознаются по идентификатору recordDataIdentifier. Изготовитель БУ должен обеспечить, чтобы эта функция выполнялась с соблюдением заданных условий работы сервера.

6.1.2 Формат сообщений

CPR_051 Форматы сообщений для примитивов ReadDataByIdentifier подробно указаны в нижеследующих таблицах.

Таблица 25
Запрос ReadDataByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции запроса ReadDataByIdentifier	22	RDBI
#6 to #7	recordDataIdentifier = [значение из таблицы 28]	xxxx	RDI_...
#8	Контрольная сумма	00-FF	CS

Таблица 26

Положительный ответ на запрос ReadDataByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	m+3	LEN
#5	Идентификатор функции положительного ответа на запрос ReadDataByIdentifier	62	RDBIPR
#6 and #7	recordDataIdentifier = [то же значение, что и у байтов #6 и #7 в таблице 25]	xxxx	RDI_...
#8 to #m+7	dataRecord[] = [данные#1 : данные#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Контрольная сумма	00-FF	CS

Таблица 27

Отрицательный ответ на запрос ReadDataByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса ReadDataByIdentifier	22	RDBI
#7	ResponseCode (код ответа) = [requestOutOfRange (нештатный запрос) incorrectMessageLength (неверная длина сообщения) conditionsNotCorrect (недопустимые условия)]	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Контрольная сумма	00-FF	CS

Определение параметров

CPR_052 Параметр *recordDataIdentifier* (RDI_) в запросе ReadDataByIdentifier служит для идентификации записи данных.

CPR_053 Значения параметра recordDataIdentifier, определенные в настоящем документе, указаны в таблице ниже.

Таблица значений параметра recordDataIdentifier состоит из четырех столбцов и ряда строк.

В 1-м столбце (Шестн. значение) приведено шестнадцатеричное значение, закрепленное за идентификатором recordDataIdentifier, который указан в 3-м столбце.

Во 2-м столбце (Data element) указан элемент данных согласно подразделу I, лежащий в основе параметра recordDataIdentifier (в некоторых случаях требуется перекодирование).

В 3-м столбце (Идентификатор) указано наименование соответствующего идентификатора recordDataIdentifier.

В 4-м столбце (Мнемокод) указан мнемокод данного идентификатора recordDataIdentifier.

Таблица 28

Определение значений параметра recordDataIdentifier

Шестн. значение	Элемент данных	Идентификатор recordDataIdentifier (формат см. в пункте 8.2)	Мнемокод
F90B	CurrentDateTime (текущая дата и время)	TimeDate	RDI_TD
F912	HighResOdometer (показания счетчика пробега с высоким разрешением)	HighResolutionTotalVehicle Distance	RDI_HRTV D
F918	K-ConstantOfRecording Equipment (K- постоянная записывающей аппаратуры)	Kfactor	RDI_KF
F91C	L-TyreCircumference (L- показатель окружности шин)	LfactorTyreCircumference	RDI_LF

Шестн. значение	Элемент данных	Идентификатор recordDataIdentifier (формат см. в пункте 8.2)	Мнемокод
F91D	W-VehicleCharacteristic Constant (W- характеристическая постоянная транспортного средства)	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize (размер шин)	TyreSize	RDI_TS
F922	nextCalibrationDate (дата следующей калибровки)	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised (разрешенная скорость)	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation (страна регистрации транспортного средства)	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber (регистрационный номер транспортного средства)	VehicleRegistrationNumber	RDI_VRN
F190	VehicleIdentificationNumber (опознавательный номер транспортного средства)	VIN	RDI_VIN

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 пункте 8. Для удобства пользователя могут быть предусмотрены и другие, не определяемые в настоящем документе виды записей данных, включая специфичные для той или иной модели БУ входные, внутренние и выходные данные.

6.2 Функция WriteDataByIdentifier

6.2.1 Описание сообщения

CPR_056 Функция WriteDataByIdentifier используется клиентом в целях сохранения значений записей данных на сервере. Для идентификации данных служит параметр recordDataIdentifier. Изготовитель БУ должен обеспечить, чтобы эта функция выполнялась с соблюдением заданных условий работы сервера. Для обновления значений параметров, перечисленных в таблице 28, БУ должно быть переведено в режим CALIBRATION.

6.2.2 Формат сообщений

CPR_057 Форматы сообщений для примитивов WriteDataByIdentifier подробно указаны в нижеследующих таблицах.

Таблица 29
Запрос WriteDataByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	m+3	LEN
#5	Идентификатор функции запроса WriteDataByIdentifier	2E	WDBI
#6 - #7	recordDataIdentifier = [значение из таблицы 28]	xxxx	RDI_...
от #8 до m+7	запись данных[] = [данные#1 : данные#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Контрольная сумма	00-FF	CS

Таблица 30
Положительный ответ на запрос WriteDataByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции положительного ответа на запрос WriteDataByIdentifier	6E	WDBIPR
#6 - #7	recordDataIdentifier = [то же значение, что и у байтов #6 и #7 в таблице 29]	xxxx	RDI_...
#8	Контрольная сумма	00-FF	CS

Таблица 31

Отрицательный ответ на запрос WriteDataByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса WriteDataByIdentifier	2E	WDBI
#7	ResponseCode (код ответа) =[requestOutOfRange (нештатный запрос) incorrectMessageLength (неверная длина сообщения) conditionsNotCorrect (недопустимые условия)]	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Контрольная сумма	00-FF	CS

Определение параметров

Определение параметра recordDataIdentifier (RDI_) приводится в таблице 28.

Параметр dataRecord (DREC_) используется в запросе WriteDataByIdentifier для сообщения серверу (БУ) значений записей данных, опознаваемых по идентификаторам recordDataIdentifier. Форматы данных указаны в пункте 8.

7. Настройка проверочных импульсов – функциональный блок регулировки входного/выходного сигнала

Описание имеющихся функций приведено в таблице ниже.

Таблица 32

Функция InputOutputControlByIdentifier

Название функции	Описание
InputOutputControlByIdentifier	Клиент запрашивает управление параметрами входного/выходного сигнала данного сервера.

7.1 Функция InputOutputControlByIdentifier

Описание сообщения

Подключение соответствующего тестера к разъему на передней панели позволяет производить настройку или мониторинг проверочных импульсов.

CPR_058 Конфигурация калибровочного канала ввода-вывода может быть изменена с помощью команды, передаваемой по К-линии с использованием функции InputOutputControlByIdentifier, позволяющей задавать этому каналу необходимый режим ввода или вывода данных. Предусмотрены следующие режимы:

отключение,

режим speedSignalInput, при котором по каналу ввода-вывода калибровочных данных вводится тест-сигнал скорости, заменяющий собой сигнал скорости от датчика движения,

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 синхронизации в формате UTC.

CPR_059 Для изменения конфигурации канала на бортовом устройстве должен быть инициирован сеанс настройки, а само устройство должно находиться в режиме CALIBRATION. При завершении сеанса настройки или при выходе из режима CALIBRATION бортовое устройство должно обеспечивать возвращение канала ввода-вывода калибровочных данных в "отключенное" состояние (в котором он находится по умолчанию).

CPR_060 В случае поступления импульсов скорости по входному каналу БУ, предназначенному для приема сигнала скорости в реальном времени, когда канал ввода-вывода калибровочных данных переключен на ввод, канал ввода-вывода калибровочных данных переключается на вывод или возвращается в отключенное состояние.

CPR_061 Последовательность операций выглядит следующим образом:

инициализация обмена данными с помощью функции StartCommunication;

запуск сеанса настройки с помощью функции StartDiagnosticSession и переход в режим CALIBRATION (очередность выполнения этих двух операций значения не имеет);

регулировка канала вывода данных с помощью функции InputOutputControlByIdentifier.

7.1.2 Формат сообщений

CPR_062 Форматы сообщений для примитивов InputOutputControlByIdentifier подробно указаны в нижеследующих таблицах.

Таблица 33
Запрос InputOutputControlByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	EE	TGT
#3	Байт адреса источника	tt	SRC
#4	Дополнительный байт длины	xx	LEN
#5	Идентификатор функции запроса InputOutputControlByIdentifier	2F	ИОСБИ
#6 и #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 или #8 - #9	ControlOptionRecord = [inputOutputControlParameter – одно значение из таблицы 36 controlState – одно значение из таблицы 37 (см. примечание ниже)]	xx xx	COR_... IOCP_... CS_...
#9 или #10	Контрольная сумма	00-FF	CS

Примечание. Параметр controlState (управление конфигурацией) присутствует лишь в некоторых случаях (см. 7.1.3).

Таблица 34

Положительный ответ на запрос InputOutputControlByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	xx	LEN
#5	Идентификатор функции положительного ответа на запрос inputOutputControlByIdentifier	6F	IOCBIPR
#6 и #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 или #8 - #9	controlStatusRecord = [inputOutputControlParameter (то же значение, что и у байта #8 в таблице 33) controlState (то же значение, что и у байта #9 в таблице 33)] (если применимо)	xx xx	CSR_ IOCP_... CS_...
#9 или #10	Контрольная сумма	00-FF	CS

Таблица 35

Отрицательный ответ на запрос InputOutputControlByIdentifier

# байта	Наименование параметра	Шестн. значение	Мнемокод
#1	Байт формата – физическая адресация	80	FMT
#2	Байт адреса приемника	tt	TGT
#3	Байт адреса источника	EE	SRC
#4	Дополнительный байт длины	03	LEN
#5	Идентификатор функции отрицательного ответа	7F	NR
#6	Идентификатор функции запроса inputOutputControlByIdentifier	2F	IOCB I
#7	responseCode (код ответа) =[incorrectMessageLength (неверная длина сообщения) conditionsNotCorrect (недопустимые условия) requestOutOfRange (нештатный запрос) deviceControlLimitsExceeded (вне диапазона регулировки устройства)]	13 22 31 7A	RC_IML RC_CNC RC_ROOR RC_DCLE
#8	Контрольная сумма	00-FF	CS

Определение параметров

CPR_064 Определение параметра *inputOutputControlParameter (IOCP_)* приведено в нижеследующей таблице.

Таблица 36

Определение значений параметра *inputOutputControlParameter*

Шестн. значение	Описание	Мнемокод
00	ReturnControlToECU Это значение оповещает сервер (БУ) о том, что тестер перестал управлять каналом ввода-вывода калибровочных данных.	RCTECU
01	ResetToDefault Это значение оповещает сервер (БУ) о том, что ему следует вернуть канал ввода-вывода калибровочных данных в состояние, выбираемое по умолчанию.	RTD
03	ShortTermAdjustment Это значение оповещает сервер (БУ) о том, что ему следует настроить канал ввода-вывода калибровочных данных по значению, указанному в параметре <i>controlState</i> .	STA

CPR_065 Параметр *controlState* (управление конфигурацией) присутствует лишь в случаях, когда параметр *inputOutputControlParameter* установлен на *ShortTermAdjustment*. Определение значений параметра *controlState* приводится в таблице ниже.

Таблица 37

Определение значений параметра *controlState*

Режим	Шестн. значение	Описание
Отключен	00	Канал ввода/вывода отключен (выбирается по умолчанию)
Включен	01	Канал ввода/вывода калибровочных данных функционирует в режиме <i>speedSignalInput</i> (ввод сигнала скорости)
Включен	02	Канал ввода/вывода калибровочных данных функционирует в режиме <i>realTimeSpeedSignalOutputSensor</i> (выход сигнала датчика скорости в реальном времени)
Включен	03	Канал ввода/вывода калибровочных данных функционирует в режиме <i>RTCOutput</i> (выход сигнала синхронизации в формате UTC)

8. Форматы dataRecords (записей данных)

В настоящем разделе изложены:

- общие правила определения диапазона параметров, передаваемых бортовым устройством на тестер;
- форматы данных, передаваемых посредством функций передачи данных, о которых говорится в пункте б.

CPR_067 Все указанные здесь параметры должны поддерживаться БУ.

CPR_068 Данные, передаваемые БУ на тестер по соответствующему запросу, по своему типу представляют собой результаты замеров (т.е. текущее значение запрошенного параметра, измеренное или зафиксированное бортовым устройством).

8.1 Диапазоны передаваемых параметров

CPR_069 В таблице 38 определены диапазоны, по которым определяется допустимость передаваемых значений параметров.

CPR_070 Используя значения диапазона "указатель ошибки", БУ может незамедлительно сообщать о том, что достоверные параметрические данные на текущий момент отсутствуют из-за той или иной ошибки контрольного устройства.

CPR_071 Значения диапазона "данные отсутствуют" могут использоваться бортовым устройством при передаче сообщений, в которых указаны отсутствующие или не поддерживаемые данным модулем параметры. С помощью значений диапазона "данные не запрашиваются" устройство может при передаче команды указать параметры, ответ по которым от устройства-адресата не требуется.

CPR_072 Если из-за отказа того или иного компонента передача достоверных данных о каком-либо параметре невозможна, то вместо этих данных используется указатель ошибки, приведенный в таблице 38. Если же данные, полученные в результате расчетов или измерений, являются достоверными, но выходят за пределы заданного диапазона значений запрошенного параметра, то указатель ошибки не используется. В этом случае при передаче данных используется соответствующее минимальное или максимальное значение параметра.

Таблица 38
Диапазоны dataRecords

Наименование диапазона	1 байт (Шестн. значение)	2 байта (Шестн. значение)	4 байта (Шестн. значение)	ASCII
Допустимый сигнал	00 - FA	0000 - FAFF	00000000 - FAFFFFFF	1 - 254
Указатель конкретного параметра	FB	FB00 - FBFF	FB000000 - FBFFFFFF	нет
Диапазон зарезервирован под разряды будущих указателей	FC - FD	FC00 - FDFE	FC000000 - FDFFFFFFFF	нет
Указатель ошибки	FE	FE00 - FEFF	FE000000 - FEFFFFFF	0
Данные отсутствуют или не запрашиваются	FF	FF00 - FFFF	FF000000 - FFFFFFFF	FF

CPR_073 Для параметров, представляемых с помощью кода ASCII, символ ASCII “*” резервируется в качестве ограничителя.

8.2 Форматы dataRecords

В таблицах 39-42 ниже подробно показаны форматы, используемые в связи с функциями ReadDataByIdentifier и WriteDataByIdentifier.

CPR_074 В таблице 39 указываются длина поля данных, разрешение и рабочий диапазон для каждого параметра, определяемого соответствующим идентификатором recordDataIdentifier.

Таблица 39
Формат dataRecords

Наименование параметра	Длина поля данных (байт)	Разрешение	Диапазон
TimeDate (время - дата)	8	<i>Подробнее см. в таблице 40</i>	
HighResolutionTotalVehicleDistance (общее расстояние пробега)	4	прибавл.: 5 м/бит, обратн. сдвиг: 0 м	от 0 до +21 055 406 км
Kfactor (коэффициент K)	2	прибавл.: 0,001 имп./м/бит, обратн. сдвиг: 0	от 0 до 64,255 имп./м
LfactorTyreCircumference (коэффициент L окружности шины)	2	прибавл.: 0,125 10 ⁻³ м /бит, обратн. сдвиг: 0	от 0 до 8,031 м
WvehicleCharacteristicFactor (характеристический коэффициент W)	2	прибавл.: 0,001 имп./м/бит, обратн. сдвиг: 0	от 0 до 64,255 имп./м
TyreSize (размер шин)	15	ASCII	ASCII
NextCalibrationDate (дата следующей калибровки)	3	<i>Подробнее см. в таблице 40</i>	
SpeedAuthorised (разрешенная скорость)	2	прибавл.: 1/256 км/ч/бит, обратн. сдвиг: 0	0-250,996 км/ч
RegisteringMemberState (государство - член регистрации)	3	ASCII	ASCII
VehicleRegistrationNumber (номер регистрации транспортного средства)	14	<i>Подробнее см. в таблице 40</i>	
VIN	17	ASCII	ASCII

CPR_075 В таблице 40 подробно указаны форматы различных байтов параметра TimeDate:

Таблица 40

Подробное описание формата TimeDate (значение recordDataIdentifier # F90B)

Байт	Параметр	Разрешение	Диапазон
1	Секунды	прибавл.: 0,25 с/бит, обратн. сдвиг: 0 с	от 0 до 59,75 с
2	Минуты	прибавл.: 1 мин./бит, обратн. сдвиг: 0 мин.	от 0 до 59 мин.
3	Часы	прибавл.: 1 ч/бит, обратн. сдвиг: 0 ч	от 0 до 23 ч
4	Месяц	прибавл.: 1 мес./бит, обратн. сдвиг: 0 мес.	от 1 до 12 месяцев
5	День	прибавл.: 0,25 сут./бит, обратн. сдвиг: 0 сут. (см. ПРИМЕЧАНИЕ к таблице 41)	от 0,25 до 31,75 суток
6	Год	прибавл.: 1 год/бит, обратн. сдвиг: +1985 год (см. ПРИМЕЧАНИЕ к таблице 41)	1985 - 2235 годы
7	Поправка на местное время (мин)	прибавл.: 1 мин./бит обратн. сдвиг: -125 мин.	от -59 до +59 мин.
8	Поправка на местное время (ч)	прибавл.: 1 ч/бит, обратн. сдвиг: -125 ч	от -23 до +23 ч

CPR_076 В таблице 41 подробно указаны форматы различных байтов параметра NextCalibrationDate.

Таблица 41

Подробное описание формата NextCalibrationDate
(значение recordDataIdentifier # F922)

Байт	Определение параметра	Разрешение	Диапазон
1	Месяц	прибавл.: 1 мес./бит, обратн. сдвиг: 0 мес.	от 1 до 12 месяцев
2	День	прибавл.: 0,25 сут./бит, обратн. сдвиг: 0 сут. (см. ПРИМЕЧАНИЕ ниже)	от 0,25 до 31,75 суток
3	Год	прибавл.: 1 год/бит, обратн. сдвиг: +1985 год (см. ПРИМЕЧАНИЕ ниже)	1985 - 2235 год

ПРИМЕЧАНИЕ относительно использования параметра "День":
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.
Данный параметр никак не влияет на параметр "часы" в таблице выше и не изменяет его.

ПРИМЕЧАНИЕ относительно использования параметра "Год":
значение года, равное 0, соответствует 1985 году; значение, равное 1, –1986 году, и т.д.

CPR_078 В таблице 42 подробно указаны форматы различных байтов параметра
VehicleRegistrationNumber.

Таблица 42

**Подробное описание формата VehicleRegistrationNumber (значение
recordDataIdentifier # F97E)**

Байт	Определение параметра	Разрешение	Диапазон
1	Кодовая страница (согласно определению, содержащемуся в подразделе I)	ASCII	от 01 до 0A
2 – 14	Регистрационный номер транспортного средства (согласно определению, содержащемуся в подразделе I)	ASCII	ASCII

ПОДРАЗДЕЛ IX

ОФИЦИАЛЬНОЕ УТВЕРЖДЕНИЕ ТИПА

ПЕРЕЧЕНЬ МИНИМАЛЬНЫХ ТРЕБУЕМЫХ ИСПЫТАНИЙ

СОДЕРЖАНИЕ

	<u>Стр.</u>
1. Введение	332
1.1 Официальное утверждение типа	332
1.2 Источники	333
2. Рабочие испытания бортового устройства	335
3. Рабочие испытания датчика движения	340
4. Рабочие испытания карточек тахографа	342
5. Испытания на эксплуатационную совместимость	344

1. Введение

1.1 Официальное утверждение типа

Процедура официального утверждения типа регистрирующей аппаратуры (либо ее компонентов) или карточек тахографа состоит из следующих основных частей:

- сертификация защиты, проводимая органом по общей оценке безопасности информационной технологии безопасности в целях подтверждения соответствия тому или иному из контрольных показателей защиты, которые должны полностью отвечать положениям подраздела X настоящего добавления;
- сертификация функциональности, проводимая органом Договаривающейся стороны в целях подтверждения того, что испытываемое изделие соответствует требованиям настоящего добавления по набору выполняемых функций, точности измерений и допустимым условиям эксплуатации;
- сертификация эксплуатационной совместимости, проводимая компетентным органом в целях подтверждения полной эксплуатационной совместимости контрольного устройства (или карточки тахографа) с необходимыми моделями карточек тахографа (или контрольных устройств) (см. главу VIII настоящего добавления).

В данном подразделе содержится перечень минимальных рабочих испытаний, которые должны быть проведены ответственным за это органом Договаривающейся стороны, а также испытаний на совместимость, которые должен провести соответствующий компетентный орган. Процедуры проведения этих испытаний и их виды дополнительно не конкретизируются.

Аспекты, связанные с сертификацией защиты, в настоящем подразделе не рассматриваются. Если какие-либо из испытаний, необходимых для официального утверждения типа, уже были проведены в процессе аттестации и сертификации систем защиты, то повторное их проведение не требуется. В таких случаях можно ограничиться проверкой результатов этих испытаний. Характеристики, которые должны испытываться при сертификации защиты (или которые тесно связаны с проводимыми при этом испытаниями) в справочных целях помечены в настоящем подразделе знаком "*".

Официальное утверждение типа датчика движения и бортового устройства рассматривается в настоящем подразделе отдельно, так как речь идет о разных компонентах контрольного устройства. Эксплуатационная совместимость каждой модели датчика движения с каждой моделью бортового устройства необязательна; поэтому тип датчика движения может быть утвержден только в сочетании с соответствующим типом бортового устройства, и наоборот.

1.2 Источники

При подготовке данного подраздела использовались следующие источники:

IEC 68-2-1 Испытания на воздействие внешних факторов. Часть 2: Испытания. Испытание А. Холод. 1990 год + Поправка 2, 1994 год.

IEC 68-2-2 Испытания на воздействие внешних факторов. Часть 2: Испытания. Испытание В. Сухое тепло. 1974 + Поправка 2, 1994 год.

IEC 68-2-6 Основные процедуры испытаний на воздействие внешних факторов. Методы испытаний. Испытание Fc и руководство. Вибрация (синусоидальная). Издание шестое, 1985 год.

IEC 68-2-14 Основные процедуры испытаний на воздействие внешних факторов. Методы испытаний. Испытание N. Колебания температуры. Изменение 1, 1986 год.

IEC 68-2-27 Основные процедуры испытаний на воздействие внешних факторов. Методы испытаний. Испытание Ea и руководство. Ударные воздействия. Издание третье, 1987 год.

IEC 68-2-30 Основные процедуры испытаний на воздействие внешних факторов. Методы испытаний. Испытание Db и руководство. Влажное тепло, циклический режим (12 + 12 - часовой цикл). Изменение 1, 1985 год.

IEC 68-2-35 Основные процедуры испытаний на воздействие внешних факторов. Методы испытаний. Испытание Fda. Широкополосная случайная вибрация. Высокая воспроизводимость. Изменение 1, 1983 год.

IEC 529 Степени защиты, обеспечиваемой корпусами изделий (код IP). Издание второе, 1989 год.

- IEC 61000-4-2 Совместимость электромагнитная (EMC). Методы испытаний и измерений. Испытание на устойчивость к электростатическому разряду. 1995 год/Поправка 1, 1998 год.
- ISO 7637-1 Транспорт дорожный. Электрические помехи, вызываемые проводимостью и взаимодействием. Часть 1. Легковые автомобили и автомобили малой грузоподъемности для коммерческих перевозок с номинальным напряжением электропитания 12 В. Распространение помех, вызываемых переходными процессами, только по линиям, обеспечивающим электропитание. Издание второе, 1990 год.
- ISO 7637-2 Транспорт дорожный. Электрические помехи, вызываемые проводимостью и взаимодействием. Часть 2. Автомобили для коммерческих перевозок с номинальным напряжением электропитания 24 В. Распространение помех, вызываемых переходными процессами, только по линиям, обеспечивающим электропитание. Издание первое, 1990 год.
- ISO 7637-3 Транспорт дорожный. Электрические помехи, вызываемые проводимостью и взаимодействием. Часть 3. Автомобили с номинальным напряжением электропитания 12 В или 24 В. Распространение помех, вызываемых переходными процессами, обусловленными емкостным или индуктивным соединением, по линиям, не обеспечивающим электропитание. Издание первое, 1995 год + Поправка 1, 1995 год.
- ISO/IEC 7816-1 Информационные технологии. Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 1. Физические характеристики. Издание первое, 1998 год.
- ISO/IEC 7816-2 Информационные технологии. Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 2. Размеры и расположение контактов. Издание первое, 1999 год.
- ISO/IEC 7816-3 Информационные технологии. Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 3. Электронные сигналы и протоколы передачи. Издание второе, 1997 год.
- ISO/IEC 10373 Карточки идентификационные. Методы испытаний. Издание первое, 1993 год.

2. Рабочие испытания бортового устройства

№	Вид испытания	Описание	Предъявляемые требования
1	Административная проверка		
1.1	Документация	Правильность оформления документации	
1.2	Результаты испытаний, проведенных изготовителем	Результаты испытаний, проводившихся изготовителем при сборке. Проверка технических характеристик по документам.	070, 071, 073
2	Визуальный осмотр		
2.1	Соответствие документации		
2.2	Идентификация/маркировка		168, 169
2.3	Материалы		163 - 167
2.4	Пломбировка		251
2.5	Внешние интерфейсы		
3	Рабочие испытания		
3.1	Предусмотренные функции		002, 004, 244
3.2	Режимы работы		006*, 007*, 008*, 009*, 106, 107
3.3	Функции и права доступа к данным		010*, 011*, 240, 246, 247
3.4	Контроль за вводом и извлечением карточек		013, 014, 015*, 016*, 106
3.5	Измерение скорости и пробега		017 - 026
3.6	Отсчет времени (испытание проводится при 20°C)		027 - 032
3.7	Контроль за деятельностью водителей		033 - 043, 106
3.8	Контроль за управлением		044, 045, 106
3.9	Ввод данных водителем вручную		046 - 050b
3.10	Установка блокировки предприятием		051 - 055
3.11	Мониторинг контрольных операций		056, 057
3.12	Обнаружение событий и/или неисправностей		059 - 069, 106
3.13	Идентификационные данные аппаратуры		075*, 076*, 079
3.14	Данные о вводе и извлечении карточек водителя		081* - 083*
3.15	Данные о деятельности водителей		084* - 086*
3.16	Данные о географических пунктах		087* - 089*

№	Вид испытания	Описание	Предъявляемые требования
3.17		Показания счетчика пробега	090* - 092*
3.18		Подробные данные о скоростном режиме	093*
3.19		Данные о событиях	094*, 095
3.20		Данные о неисправностях	096*
3.21		Данные калибровки	097*, 098*
3.22		Данные о корректировке времени	100*, 101*
3.23		Данные о контрольных операциях	102*, 103*
3.24		Данные о блокировках, установленных предприятием	104*
3.25		Данные об операциях по загрузке данных	105*
3.26		Данные об особых ситуациях	105a*, 105b*
3.27		Регистрация и сохранение данных на карточках тахографа	108, 109*, 109a*, 110*, 111, 112
3.28		Индикация данных на дисплее	072, 106, 113 - 128, PIC_001, DIS_001
3.29		Распечатка данных	072, 106, 129 - 138, PIC_001, PRT_001 - PRT_012
3.30		Сигналы предупреждения	106, 139 - 148, PIC_001
3.31		Сохранение данных на внешнем носителе	072, 106, 149 - 151
3.32		Вывод данных на дополнительные внешние устройства	152, 153
3.33		Калибровка	154*, 155*, 156*, 245
3.34		Корректировка времени	157*, 158*
3.35		Отсутствие помех при выполнении дополнительных функций	003, 269
4	Испытания на воздействие внешних факторов		
4.1	Температура	Проверка работоспособности согласно: - стандарту IEC 68-2-1, испытание Ad: продолжительность испытания - 72 часа при нижней предельной температуре (-20°C); 1 час во включенном состоянии - 1 час в выключенном состоянии; - стандарту IEC 68-2-2, испытание Bd: продолжительность испытания -	

№	Вид испытания	Описание	Предъявляемые требования
		<p>72 часа при верхней предельной температуре (+70°C); 1 час во включенном состоянии - 1 час в выключенном состоянии.</p> <p>Термоциклирование: проверка способности бортового устройства выдерживать резкие перепады окружающей температуры согласно стандарту IEC 68-2-14 (испытание Na): 20 циклов с изменением температуры от нижнего (-20°C) до верхнего (+70°C) предела в каждом цикле, с выдержкой в течение 2 часов соответственно при минимальной и максимальной температуре.</p> <p>Возможно проведение сокращенной серии испытаний (из числа указанных в разделе 3 настоящей таблицы) при минимальной и максимальной предельной температуре, а также на протяжении термоциклов.</p>	
4.2	Испытания во влажной среде	<p>Проверка способности бортового устройства выдерживать циклические колебания температуры во влажной среде согласно стандарту IEC 68-2-30, 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>	160
4.3	Вибростойкость	<p>1. Синусоидальные вибрации:</p> <p>Проверка способности бортового устройства выдерживать синусоидальные вибрации со следующими характеристиками:</p> <p>постоянное смещение (пиковая амплитуда 10 мм) в диапазоне 5-11 Гц;</p> <p>постоянное ускорение (5 g) в диапазоне 11–300 Гц.</p> <p>Соответствие данному</p>	163

№	Вид испытания	Описание	Предъявляемые требования
		<p>требованию проверяется согласно стандарту IEC 68-2-6, испытание Fc минимальной продолжительностью 3х12 часов (по 12 часов на каждую ось).</p> <p>2. Случайные колебания: Проверка способности бортового устройства выдерживать случайные колебания со следующими характеристиками: частота 5–150 Гц, уровень 0,02 g²/Гц. Соответствие данному требованию проверяется согласно стандарту IEC 68-2-35, испытание Ffda минимальной продолжительностью 3х12 часов (12 часов на каждую ось), 1 час во включенном состоянии – 1 час в выключенном состоянии. Два вышеуказанных испытания проводятся с использованием двух разных экземпляров устройства испытываемого образца.</p>	
4.4	Защита от попадания воды и посторонних предметов	Индекс защищенности согласно IEC 529 для бортового устройства, установленного на транспортном средстве, должен составлять не менее IP 40 в реальных условиях эксплуатации.	164, 165
4.5	Защита от перегрузок по напряжению	<p>Проверка способности бортового устройства выдерживать следующее напряжение в цепи питания:</p> <p>в варианте, рассчитанном на 24 В: 34 В при +40°C в течение 1 часа;</p> <p>в варианте, рассчитанном на 12 В: 17 В при +40°C в течение 1 часа.</p>	161
4.6	Защита от несоблюдения полярности	Проверка способности бортового устройства выдерживать подключение к источнику питания противоположной полярности.	161

№	Вид испытания	Описание	Предъявляемые требования
4.7	Защита от короткого замыкания	Проверка защищенности входного и выходного сигналов от короткого замыкания на источник питания и на массу.	161
5.	Испытания на электромагнитную совместимость		
5.1	Излучения и электромагнитная защищенность	Соответствие Правилам ЕЭК ООН №10	162
5.2	Устойчивость к электростатическому разряду	Соответствие стандарту IEC 61000-4-2, ±2 кВ (уровень 1)	162
5.3	Невосприимчивость к быстрым переходным процессам в цепи питания	<p>В варианте, рассчитанном на 24 В – соответствие стандарту ISO 7637-2:</p> <p>импульс 1a: $V_s = -100$ В, $R_i = 10$ Ом импульс 2: $V_s = +100$ В, $R_i = 10$ Ом импульс 3a: $V_s = -100$ В, $R_i = 50$ Ом импульс 3b: $V_s = +100$ В, $R_i = 50$ Ом импульс 4: $V_s = -16$ В $V_a = -12$ В, $t_b = 100$ мс импульс 5: $V_s = +120$ В, $R_i = 2,2$ Ом,</p> <p>в варианте, рассчитанном на 12 В – соответствие стандарту ISO 7637-1:</p> <p>импульс 1: $V_s = -100$ В, $R_i = 10$ Ом импульс 2: $V_s = +100$ В, $R_i = 10$ Ом импульс 3a: $V_s = -100$ В, $R_i = 50$ Ом импульс 3b: $V_s = +100$ В, $R_i = 50$ Ом импульс 4: $V_s = -6$ В $V_a = -5$ В, $t_b = 15$ мс импульс 5: $V_s = +65$ В, $R_i = 3$ Ом,</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>	162

3. Рабочие испытания датчика движения

No	Вид испытания	Описание	Предъявляемые требования
1. Административная проверка			
1.1	Документация	Правильность оформления документации	
2. Визуальный осмотр			
2.1	Соответствие документации		
2.2	Идентификация / маркировка		169, 170
2.3	Материалы		163–167
2.4	Наложение пломб		251
3. Рабочие испытания			
3.1	Идентификационные данные датчика		077*
3.2	Подсоединение датчика движения к бортовому устройству		099*, 155
3.3	Регистрация движения Точность измерения параметров движения		022–026
4. Испытания на воздействие внешних факторов			
4.1	Рабочая температура	Проверка работоспособности (в соответствии с определением, приведенным для испытания No. 3.3) в температурном диапазоне [–40°C; +135°C] согласно: - стандарту IEC 68–2–1, испытание Ad: продолжительность испытания – 96 часов при нижней предельной температуре T_{\min} , - стандарту IEC 68–2–2, испытание Bd: продолжительность испытания – 96 часов при верхней предельной температуре T_{\max} .	159
4.2	Термоциклирование	Проверка работоспособности (в соответствии с определением, приведенным для испытания No. 3.3) согласно стандарту IEC 68–2–14,	159

№	Вид испытания	Описание	Предъявляемые требования
		<p>испытание Na: 20 циклов с изменением температуры от нижнего (-40°C) до верхнего ($+135^{\circ}\text{C}$) предела в каждом цикле, с выдержкой в течение 2 часов соответственно при минимальной и максимальной температуре.</p> <p>Возможно проведение сокращенной серии испытаний (из числа указанных в разделе 3.3) при минимальной и максимальной температуре, а также на протяжении термоциклов.</p>	
4.3	Циклические испытания во влажной среде	<p>Проверка работоспособности (в соответствии с определением, приведенным для испытания No. 3.3) согласно стандарту IEC 68-2-30, испытание Db: шесть 24-часовых циклов с изменением температуры от $+25^{\circ}\text{C}$ до $+55^{\circ}\text{C}$ в каждом цикле и относительной влажностью воздуха, равной 97% при $+25^{\circ}\text{C}$ и эквивалентной 93% при $+55^{\circ}\text{C}$.</p>	160
4.4	Вибростойкость	<p>Проверка работоспособности (в соответствии с определением, приведенным для испытания No. 3.3) согласно стандарту IEC 68-2-6, испытание Fc, продолжительность испытания не менее 100 частотных циклов:</p> <p>постоянное смещение (амплитуда 1,5 мм) в диапазоне 10-57 Гц;</p> <p>постоянное ускорение (20 g) в диапазоне 57-500 Гц.</p>	163
4.5	Ударопрочность	<p>Проверка работоспособности (в соответствии с определением, приведенным для испытания No. 3.3) согласно стандарту IEC 68-2-27, испытание Ea: по 3 ударных импульса в каждом из двух направлений по каждой из 3 осей.</p>	163
4.6	Защита от попадания воды и посторонних	Индекс защищенности согласно IEC 529 для датчика движения, установленного на	165

№	Вид испытания	Описание	Предъявляемые требования
	предметов	транспортном средстве, должен составлять не менее IP 64 в реальных условиях эксплуатации.	
4.7	Защита от несоблюдения полярности	Проверка способности датчика движения выдерживать подключение к источнику питания противоположной полярности.	161
4.8	Защита от короткого замыкания	Проверка защищенности входного и выходного сигналов от короткого замыкания на источник питания и на массу.	161
5.	Испытания на электромагнитную совместимость		
5.1	Излучения и электромагнитная защищенность	Проверка соответствия Правилам ЕЭК ООН N°10	162
5.2	Устойчивость к электростатическому разряду	Соответствие стандарту IEC 61000-4-2, ±2 кВ (уровень 1)	162
5.3	Невосприимчивость к быстрым переходным процессам на линиях передачи данных	Соответствие стандарту ISO7637-3 (уровень III)	162

4. Рабочие испытания карточек тахографа

№	Вид испытания	Описание	Предъявляемые требования
1.	Административная проверка		
1.1	Документация	Проверка правильности оформления документации	
2.	Визуальный осмотр		
2.1		Проверка правильности нанесения на карточку всех элементов защиты и визуальной информации и их соответствия установленным требованиям	171 - 181
3.	Физический контроль		

№	Вид испытания	Описание	Предъявляемые требования
3.1		Проверка размеров карточки и расположения контактов	184 ISO/IEC 7816-1 ISO/IEC 7816-2
4. Тестирование протоколов			
4.1	ATR	Проверка совместимости ATR	ISO/IEC 7816-3 TCS 304, 307, 308
4.2	T=0	Проверка совместимости протокола T=0	ISO/IEC 7816-3 TCS 302, 303, 305
4.3	PTS	Проверка совместимости команды PTS путем задания протокола T=1 при исходном T=0	ISO/IEC 7816-3 TCS 309 - 311
4.4	T=1	Проверка совместимости протокола T=1	ISO/IEC 7816-3 TCS 303, / 306
5. Структура данных на карточке			
5.1		Подтверждение соответствия файловой структуры на карточке путем проверки наличия обязательных файлов и тестирования условий доступа к ним	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6. Рабочие испытания			
6.1	Обработка данных в обычном режиме	Как минимум однократное тестирование каждого допустимого использования каждой команды (например, проверка исполнения команды UPDATE BINARY при CLA = "00", CLA = "0C" и при разных значениях параметров P1, P2 и Lc). Подтверждение фактического выполнения карточкой соответствующих операций (например, путем считки файла после исполнения команды на его обработку)	TCS 313 - TCS 379
6.2	Сообщения об ошибках	Как минимум однократное тестирование каждого сообщения об ошибке (из числа указанных в подразделе 2) при исполнении каждой команды. Как минимум однократное тестирование на общую ошибку каждого вида (кроме ошибок серии '6400' (искажение данных), которые тестируются при сертификации систем защиты)	

№	Вид испытания	Описание	Предъявляемые требования
7.	Испытания на воздействие внешних факторов		
7.1		Подтверждение способности карточек к функционированию в предельных режимах, определенных согласно стандарту ISO/IEC 10373	185 - 188 ISO/IEC 7816-1

5. Испытания на эксплуатационную совместимость

№	Вид испытания	Описание
1	Взаимная аутентификация	Проверка нормального выполнения процедур взаимной аутентификации бортового устройства и карточки тахографа
2	Проверка записи/считки данных	<p>Отработка типового сценария функционирования бортового устройства. Сценарий должен быть выбран с учетом типа тестируемой карточки и включать операции по записи данных в максимально возможном числе элементарных файлов на карточке.</p> <p>Загрузка данных с карточки для проверки наличия и правильности всех соответствующих записей данных.</p> <p>Распечатка данных с карточки за соответствующие сутки для проверки возможности правильной считки всех соответствующих записей</p>

ПОДРАЗДЕЛ X
ОБЩИЕ КОНТРОЛЬНЫЕ ПОКАЗАТЕЛИ ЗАЩИТЫ
СОДЕРЖАНИЕ

	<u>Стр.</u>
Общие контрольные показатели защиты датчика движения.....	350
1. Введение.....	350
2. Сокращения, определения и источники.....	350
2.1 Сокращения.....	350
2.2 Определения	351
2.3 Источники	351
3. Назначение и характеристика изделия.....	351
3.1 Описание и способ эксплуатации датчика движения.....	351
3.2 Жизненный цикл датчика движения	352
3.3 Опасности.....	354
3.3.1 Опасности, связанные с нарушением режима контроля за доступом	354
3.3.2 Опасности, связанные с конструкцией датчика	354
3.3.3 Опасности в процессе эксплуатации	354
3.4 Цели защиты	355
3.5 Цели защиты в области информационных технологий.....	356
3.6 Технические, организационные и процедурные средства	356
3.6.1 Конструкция аппаратуры.....	357
3.6.2 Поставка аппаратуры	357
3.6.3 Генерация, передача и ввод данных защиты	357
3.6.4 Установка, калибровка и проверка контрольного устройства.....	357
3.6.5 Правоохранительный контроль	358
3.6.6 Новые версии программного обеспечения	358
4. Защитные функции.....	358
4.1 Идентификация и аутентификация.....	358
4.2 Контроль за доступом	359
4.2.1 Режим контроля за доступом	359
4.2.2 Права доступа к данным.....	359
4.2.3 Структура файлов и условия доступа к ним.....	360
4.3 Учет.....	360
4.4 Контроль.....	360
4.5 Достоверность.....	361
4.5.1 Правила контроля за поступлением информации.....	361
4.5.2 Внутренняя передача данных.....	361
4.5.3 Целостность сохраненных данных	361
4.6 Надежность функционирования	362

СОДЕРЖАНИЕ (продолжение)

	<u>Стр.</u>
4.6.1	Испытания 362
4.6.2	Программное обеспечение..... 362
4.6.3	Физическая защита..... 362
4.6.4	Прекращение электропитания..... 363
4.6.5	Перезапуск 363
4.6.6	Доступность данных 363
4.6.7	Многоцелевое использование 363
4.7	Обмен данными 364
4.8	Криптографическая защита 364
5.	Определение механизмов защиты 364
6.	Минимальная эффективность механизмов защиты 364
7.	Степень надежности..... 365
8.	Обоснование..... 365
Общие контрольные показатели защиты бортового устройства 368	
1.	Введение 368
2.	Сокращения, определения и источники 369
2.1	Сокращения..... 369
2.2	Определения..... 369
2.3	Источники 370
3.	Назначение и характеристика изделия..... 370
3.1	Описание и способ эксплуатации бортового устройства 370
3.2	Жизненный цикл бортового устройства 372
3.3	Опасности..... 373
3.3.1	Опасности, связанные с идентификационными данными и режимом контроля за доступом 373
3.3.2	Опасности, связанные с конструкцией устройства..... 374
3.3.3	Опасности в процессе эксплуатации 374
3.4	Цели защиты 376
3.5	Цели защиты в области информационных технологий..... 376
3.6	Технические, организационные и процедурные средства..... 377
3.6.1	Конструкция аппаратуры..... 377
3.6.2	Поставка и активация аппаратуры..... 378
3.6.3	Генерация, передача и ввод данных защиты 378
3.6.4	Выдача карточек 378
3.6.5	Установка, калибровка и проверка контрольного устройства..... 379
3.6.6	Эксплуатация аппаратуры 379

СОДЕРЖАНИЕ (продолжение)

	<u>Стр.</u>
3.6.7	Правоприменительный контроль..... 379
3.6.8	Новые версии программного обеспечения 380
4.	Защитные функции..... 380
4.1	Идентификация и аутентификация..... 380
4.1.1	Идентификация и аутентификация датчика движения 380
4.1.2	Идентификация и аутентификация пользователей 381
4.1.3	Идентификация и аутентификация предприятия при дистанционном подключении 382
4.1.4	Идентификация и аутентификация административных устройств..... 383
4.2	Контроль за доступом 383
4.2.1	Режим контроля за доступом 384
4.2.2	Права доступа к функциям..... 384
4.2.3	Права доступа к данным..... 384
4.2.4	Структура файлов и условия доступа к ним..... 385
4.3	Отчетность 385
4.4	Контроль..... 386
4.5	Повторное использование объектов..... 387
4.6	Достоверность..... 387
4.6.1	Правила контроля за поступлением информации..... 387
4.6.2	Внутренняя передача данных..... 387
4.6.3	Целостность сохраненных данных 388
4.7	Надежность функционирования 388
4.7.1	Испытания..... 388
4.7.2	Программное обеспечение 388
4.7.3	Физическая защита..... 389
4.7.4	Прекращение электропитания..... 389
4.7.5	Перезапуск 389
4.7.6	Доступность данных 390
4.7.7	Многоцелевое использование 390
4.8	Обмен данными 390
4.8.1	Обмен данными с датчиком движения 390
4.8.2	Обмен данными с карточками тахографа 390
4.8.3	Обмен данными с внешним носителем (функция загрузки данных)..... 391
4.9	Криптографическая защита..... 391
5.	Определение механизмов защиты 392
6.	Минимальная эффективность механизмов защиты..... 392
7.	Степень надежности..... 292
8.	Обоснование 392

СОДЕРЖАНИЕ (продолжение)

	<u>Стр.</u>
Общие контрольные показатели защиты карточки тахографа	400
1. Введение	400
2. Сокращения, определения и источники	400
2.1 Сокращения	400
2.2 Определения	401
2.3 Источники	402
3. Назначение и характеристика изделия	402
3.1 Описание и способ эксплуатации карточки тахографа	402
3.2 Жизненный цикл карточек тахографа	403
3.3 Опасности	403
3.3.1 Конечные цели нарушителей защиты	403
3.3.2 Пути преодоления защиты	404
3.4 Цели защиты	404
3.5 Цели защиты в области информационных технологий	405
3.6 Технические, организационные и процедурные средства	406
4. Защитные функции	406
4.1 Соответствие профилям защиты	406
4.2 Идентификация и аутентификация пользователей	406
4.2.1 Идентификация пользователей	406
4.2.2 Аутентификация пользователей	407
4.2.3 Отрицательный результат аутентификации	407
4.3 Контроль за доступом	408
4.3.1 Режим контроля за доступом	408
4.3.2 Функции контроля за доступом	408
4.4 Отчетность	409
4.5 Контроль	410
4.6 Достоверность	410
4.6.1 Целостность сохраненных данных	410
4.6.2 Аутентификация основных данных	410
4.7 Надежность функционирования	410
4.7.1 Испытания	410
4.7.2 Программное обеспечение	411
4.7.3 Питание	411
4.7.4 Перезапуск	411
4.8 Обмен данными	411
4.8.1 Обмен данными с бортовым устройством	411
4.8.2 Экспорт данных на устройства, не являющиеся бортовыми устройствами (функция загрузки)	412
4.9 Криптографическая защита	412

СОДЕРЖАНИЕ (продолжение)

	<u>Стр.</u>
5. Определение механизмов защиты	413
6. Заявленная минимальная эффективность механизмов защиты.....	413
7. Степень надежности.....	413
8. Обоснование	413

О содержании настоящего подраздела

В настоящем подразделе содержится минимальный перечень обязательных контрольных показателей защиты датчиков движения, бортовых устройств и карточек тахографа.

В целях выработки контрольных показателей защиты соответствующих изделий, на основании которых им могут присваиваться сертификаты защиты, изготовители этих изделий должны по мере необходимости уточнять и дополнять соответствующую документацию, не изменяя и не удаляя при этом существующих определений опасностей, а также целей, процедурных средств и защитных функций.

Общие контрольные показатели ЗАЩИТЫ датчика движения

1. Введение

В настоящем документе приводится описание датчика движения с перечислением опасностей, которым он должен противостоять, и целей, на которые должна быть направлена его защита. В нем указаны необходимые для этого защитные функции, минимальный уровень заданной эффективности механизмов защиты и требуемая степень надежности при их разработке и аттестации.

Требования, о которых говорится в настоящем документе, сформулированы в основном тексте добавления 1В. В интересах ясности изложения некоторые контрольные показатели защиты дублируют положения основного текста добавления 1В. При отсутствии однозначного совпадения между каким-либо из контрольных показателей и соответствующим ему положением основного текста добавления 1В следует руководствоваться основным текстом добавления 1В.

Требования основного текста добавления 1В, для которых не определены контрольные показатели, защитными функциями не охватываются.

Определения опасностей, целей и процедурных средств, а также спецификации защитных функций снабжены индивидуальными индексами для более наглядной увязки с проектной и аттестационной документацией.

2. Сокращения, определения и источники

2.1 Сокращения

АИ	Аттестуемое изделие
БУ	Бортовое устройство
ЗФ	Защитная функция
ROM	Постоянная память (доступная только для чтения)

2.2 Определения

Цифровой тахограф	Контрольное устройство.
Устройство	Устройство, подключенное к датчику движения.
Данные о движении	Данные, которыми датчик обменивается с БУ, позволяющие определять скорость и пробег транспортного средства.
Физически разделенные	Физические детали датчика движения, установленные на транспортном средстве в разных местах, в отличие от компоненты физических деталей, сгруппированных внутри корпуса датчика.
Данные защиты	Конкретные данные, необходимые для обеспечения защитных функций (например, криптографические ключи).
Система	Технические средства, лица и организации, имеющие то или иное отношение к контрольному устройству.
Пользователь	Человек, пользующийся датчиком движения (за исключением случая "пользователь данных").
Пользовательские данные	Любые данные помимо данных о движении и данных защиты, регистрируемые и сохраняемые датчиком движения.

2.3 Источники

ITSEC	ИТСЕК Критерии оценки безопасности информационной технологии, 1991 год.
-------	---

3. Назначение и характеристика изделия

3.1 Описание и способ эксплуатации датчика движения

Датчик движения предназначен для установки на автотранспортных средствах. Он служит для получения и передачи на БУ криптозащищенных данных о движении, позволяющих определять скорость и пробег транспортного средства.

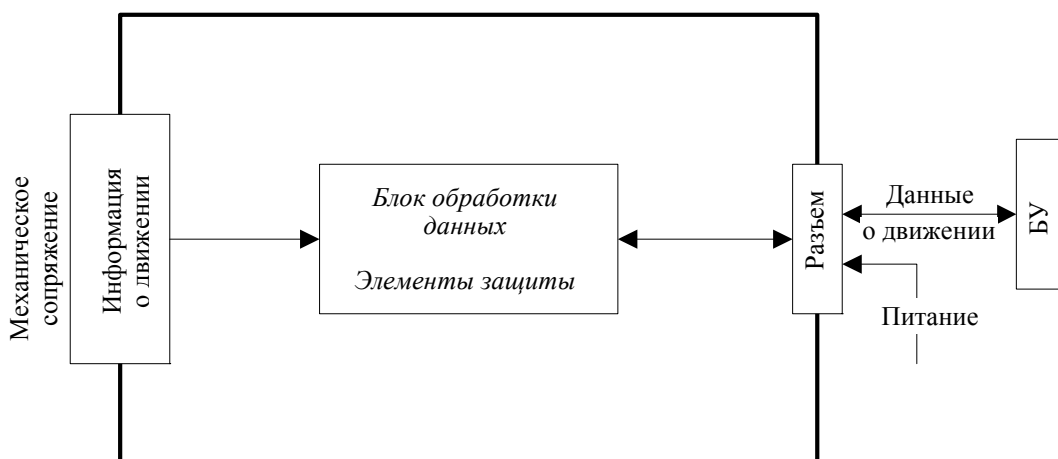
Датчик движения механически сопряжен с движущейся деталью транспортного средства, по движению которой может измеряться скорость транспортного средства или пройденное им расстояние. Он может располагаться в коробке передач или в любом другом месте на транспортном средстве.

В рабочем режиме датчик движения должен быть подключен к БУ.

В административных целях он также может подключаться к другому оборудованию (*по усмотрению изготовителя*).

Типичная схема датчика движения представлена ниже.

Рис. 1
Обобщенная схема датчика движения

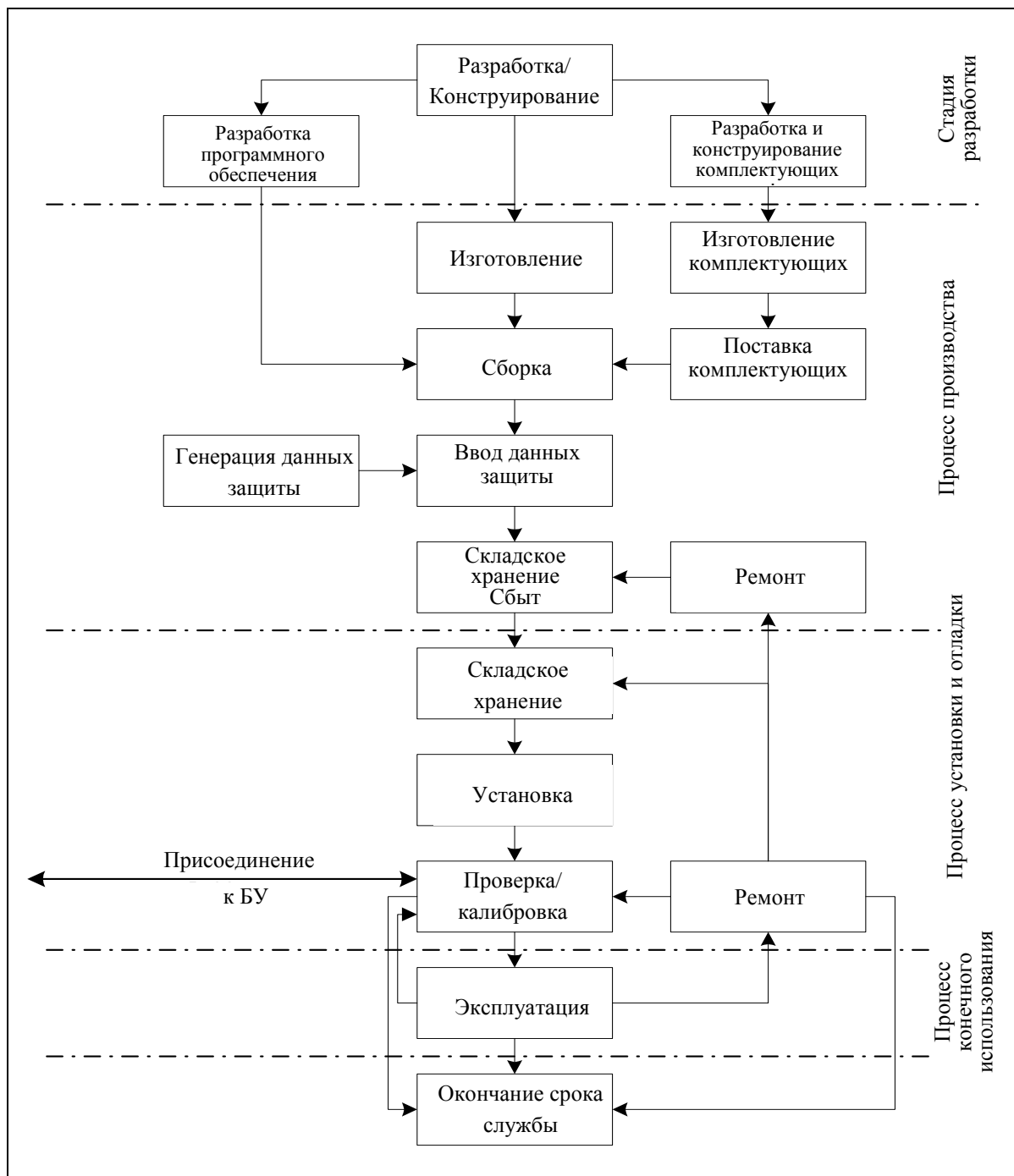


3.2 Жизненный цикл датчика движения

Схема жизненного цикла датчика движения представлена ниже.

Рис. 2

Обобщенная схема жизненного цикла датчика движения



3.3 Опасности

Настоящий пункт содержит описание опасностей, которым может подвергаться датчик движения.

3.3.1 Опасности, связанные с нарушением режима контроля за доступом

О: Доступ Пользователи могут пытаться получить доступ к не предназначенным для них функциям.

3.3.2 Опасности, связанные с конструкцией датчика

О: Сбои в работе Отказы аппаратуры, сбои в функционировании программного обеспечения или процедурах обмена данными могут привести к непредвиденным ситуациям и ослабить защиту датчика движения.

О: Испытания Защита датчика движения может быть нарушена в результате использования неотключенных тест-режимов или имеющихся "обходных путей" доступа.

О: Конструкция Пользователи могут пытаться незаконным путем добыть сведения о конструкции датчика – будь то у изготовителя (хищение, подкуп и т.п.) или путем инженерного анализа.

3.3.3 Опасности в процессе эксплуатации

О: Внешние_факторы Для преодоления защиты датчика движения пользователи могут пытаться использовать воздействие внешних факторов (термических, электромагнитных, оптических, химических, механических и т.д.).

О: Аппаратура Пользователи могут пытаться внести физические изменения в конструкцию датчика движения.

- О: Механический_источник_данных Пользователи могут пытаться нарушить механическое сопряжение датчика с ходовой частью (например, соединение с коробкой передач).
- О: Данные_о_движении Пользователи могут пытаться исказить данные о движении транспортного средства (подача добавочного или измененного сигнала, подавление сигнала, копирование и воспроизведение сигнала).
- О: Источник_питания Пользователи могут пытаться нейтрализовать защиту датчика движения путем изменения параметров тока в цепи питания (отключение, ослабление, усиление).
- О: Данные_защиты Пользователи могут пытаться получить несанкционированный доступ к данным защиты датчика в процессе генерации этих данных, их передачи или хранения аппаратурой.
- О: Программное_обеспечение Пользователи могут пытаться внести изменения в программное обеспечение датчика движения.
- О: Сохраненные_данные Пользователи могут пытаться изменить сохраненные данные (данные защиты или пользовательские данные).

3.4 Цели защиты

Основная цель защиты системы цифрового тахографа заключается в следующем:

- Ц: Основная Данные, необходимые контрольным органам для проверки, должны иметься в наличии и обеспечивать полный и точный учет деятельности контролируемых водителей и эксплуатации контролируемых транспортных средств в том, что касается продолжительности управления, периодов работы, готовности и отдыха, а также скоростного режима.

сервисных центрах или мастерских, пользующихся доверием и допущенных к таким работам.

C: Механическое_сопряжение Должны быть предусмотрены средства выявления попыток физического нарушения механического сопряжения датчика с ходовой частью (например, пломбы).

C: Регулярные_проверки Контрольное устройство должно регулярно проходить проверку и калибровку.

3.6.5 Правоприменительный контроль

C: Контроль Правоохранительный контроль должен осуществляться как на регулярной, так и на выборочной основе и включать контрольную проверку систем защиты.

3.6.6 Новые версии программного обеспечения

C: Новое_п/о Перед установкой на датчик движения новые версии программного обеспечения должны получить сертификат безопасности.

4. Защитные функции

4.1 Идентификация и аутентификация

UIA_101 При каждом взаимодействии с другими устройствами датчик движения должен иметь возможность идентифицировать подключенное устройство.

UIA_102 Идентификационные данные подключенного устройства состоят из:

- указания категории, к которой относится данное устройство, а именно:
 - БУ;
 - административные устройства;
 - прочие устройства;
- собственного идентификатора устройства (только для БУ).

- UIA_103 Идентификатор подключенного БУ состоит из номера официального утверждения данного образца БУ и серийного номера БУ.
- UIA_104 Датчик движения должен иметь возможность аутентифицировать любое подключенное к нему БУ или административное устройство:
- при подключении устройства;
 - при восстановлении подачи питания.
- UIA_105 Датчик движения должен иметь возможность периодически производить повторную аутентификацию БУ, к которому он подключен.
- UIA_106 Датчик движения должен выявлять и предотвращать использование скопированных и повторно воспроизводимых аутентификационных данных.
- UIA_107 После регистрации (*количество определяется изготовителем, но не должно превышать 20*) неудачных попыток аутентификации подряд защитные функции должны обеспечивать:
- генерацию контрольной записи о событии;
 - выдачу предупреждения на подключенное устройство;
 - продолжение экспорта данных о движении в незащищенном режиме.

4.2 Контроль за доступом

Средства контроля за доступом обеспечивают возможность считывания, ввода или изменения информации в АИ только для уполномоченных на то лиц.

4.2.1 Режим контроля за доступом

АСС_101 Датчик движения должен обеспечивать контроль прав доступа к функциям и данным.

4.2.2 Права доступа к данным

АСС_102 Должна быть предусмотрена лишь однократная возможность сохранения идентификационных данных датчика движения (требование 078).

ACC_103 Датчик движения должен принимать и/или сохранять пользовательские данные только при их поступлении от аутентифицированных устройств.

ACC_104 Датчик движения должен обеспечивать соответствующий режим доступа к функциям считывания и сохранения данных защиты.

4.2.3 Структура файлов и условия доступа к ним

ACC_105 Структура файлов приложений и файлов данных и условия доступа к ним определяются в процессе изготовления и защищаются от любого последующего изменения или удаления.

4.3 Учет

ACT_101 В памяти датчика движения должны храниться идентификационные данные этого датчика (требование 077).

ACT_102 В памяти датчика движения должны храниться данные об установке (требование 099).

ACT_103 Должна быть предусмотрена возможность передачи учетных данных с датчика движения на аутентифицированные устройства по их запросу.

4.4 Контроль

AUD_101 Датчик движения должен генерировать контрольные записи о событиях, способных нарушить его защиту.

AUD_102 К событиям, затрагивающим защиту датчика движения, относятся:

- попытки преодоления защиты:
 - отрицательный результат аутентификации;
 - ошибка при проверке целостности сохраненных данных;
 - ошибка при внутренней передаче данных;
 - несанкционированное вскрытие корпуса;
 - умышленная порча оборудования;
- отказ датчика.

AUD_103 Надзорные записи должны включать следующие данные:

- дата и время события;
- тип события;
- идентификационные данные подключенного устройства.

Если необходимые данные отсутствуют, должно использоваться соответствующее обозначение по умолчанию (*определяется изготовителем*).

AUD_104 Генерируемые датчиком движения контрольные записи передаются на БУ в момент их генерации и могут также сохраняться в памяти датчика.

AUD_105 Если контрольные записи сохраняются в памяти датчика движения, то должно быть обеспечено хранение 20 таких записей даже после того, как емкость выделенной для них памяти будет исчерпана, с возможностью выдачи сохраненных записей на аутентифицированные устройства по их запросу.

4.5 Достоверность

4.5.1 Правила контроля за поступлением информации

ACR_101 Датчик движения должен воспринимать и обрабатывать данные о движении, поступающие только через устройства его механического сопряжения с ходовой частью.

4.5.2 Внутренняя передача данных

Требования настоящего пункта применяются лишь к датчикам движения, в которых используются физически разделенные компоненты.

ACR_102 Если между физически разделенными компонентами датчика движения передаются данные, то эти данные должны быть защищены от изменения.

ACR_103 При обнаружении ошибки передачи данных в процессе их внутренней передачи передача осуществляется повторно, а защитная функция (ЗФ) генерирует контрольную запись об этом событии.

4.5.3 Целостность сохраненных данных

ACR_104 Датчик движения должен проверять целостность хранящихся в его памяти пользовательских данных.

ACR_105 В случае ошибки при проверке неискаженности сохраненных пользовательских данных защитная функция генерирует надзорную запись.

4.6 Надежность функционирования

4.6.1 Испытания

RLB_101 Все команды, функции и контакты, предназначенные исключительно для тестирования датчика на стадии производства, перед выпуском готового изделия блокируются или удаляются. Возможность их восстановления для последующего использования должна быть исключена.

RLB_102 При включении, а также в процессе работы в обычном режиме датчик движения должен производить самопроверку для подтверждения того, что он функционирует нормально. При самопроверке датчика движения проверяются целостность данных защиты и хранящихся в памяти исполнимых команд (если они не сохранены в ROM).

RLB_103 В случае обнаружения внутренних неполадок в процессе самопроверки система защиты генерирует отчетную запись (сбой в работе датчика).

4.6.2 Программное обеспечение

RLB_104 Возможность анализа или отладки программного обеспечения датчика движения в полевых условиях должна быть исключена.

RLB_105 Данные, поступающие из внешних источников, не должны восприниматься в качестве исполнимых команд.

4.6.3 Физическая защита

RLB_106 Если конструкция датчика движения допускает вскрытие его корпуса, то датчик должен быть способен регистрировать любое такое вскрытие и сохранять эту способность даже при отключении от внешнего источника питания в течение как минимум шести месяцев. При этом ЗФ генерирует отчетную запись о данном событии (допускается возможность генерации и сохранения такой записи после возобновления питания).

Если конструкция датчика движения не предусматривает вскрытия корпуса, то она должна обеспечивать легкое обнаружение следов физического воздействия (например, при внешнем осмотре).

RLB_107 Датчик движения должен быть способен регистрировать конкретные (*определяемые заводом-изготовителем*) виды умышленной порчи оборудования.

RLB_108 В вышеупомянутых случаях ЗФ должна генерировать контрольную запись, а датчик движения должен: (*определяется заводом-изготовителем*).

4.6.4 Прекращение электропитания

RLB_109 Защита датчика движения не должна нарушаться при отключении от источника питания или при изменениях параметров тока в цепи питания.

4.6.5 Перезапуск

RLB_110 В случае прекращения питания, при досрочном прерывании текущей операции или при наступлении любых других условий, требующих перезапуска, датчик движения полностью перезапускается.

4.6.6 Доступность данных

RLB_111 Датчик движения должен предоставлять доступ к имеющимся ресурсам данных по мере необходимости, обеспечивать отсутствие неоправданных обращений к ресурсам и удалять ненужные данные.

4.6.7 Многоцелевое использование

RLB_112 Если датчик движения используется для других целей, помимо обеспечения работы тахографа, то все соответствующие приложения должны быть физически и/или логически отделены друг от друга. Данные защиты не должны быть общими для этих приложений. Одновременное выполнение более чем одной функции не допускается.

4.7 Обмен данными

DEX_101 Датчик движения выдает данные о движении транспортного средства на БУ с соответствующими атрибутами защиты, позволяющими БУ проверять их целостность и подлинность.

4.8 Криптографическая защита

Требования данного пункта применяются лишь в необходимых случаях в зависимости от используемых механизмов защиты и примененных заводом-изготовителем технических решений.

CSP_101 Любые криптографические операции, выполняемые датчиком движения, должны соответствовать заданному алгоритму при заданном размере ключа.

CSP_102 Если датчик движения генерирует криптографические ключи, то это должно делаться в соответствии с заданными алгоритмами генерации криптографических ключей при заданных размерах таких ключей.

CSP_103 Если датчик движения рассылает криптографические ключи, то это должно делаться в соответствии с установленными методами рассылки криптографических ключей.

CSP_104 Если датчик движения получает доступ к криптографическим ключам, то это должно соответствовать установленному порядку доступа к криптографическим ключам.

CSP_105 Если датчик движения уничтожает криптографические ключи, то это должно делаться в соответствии с установленными методами уничтожения криптографических ключей.

5. Определение механизмов защиты

Механизмы защиты, обеспечивающие выполнение защитных функций датчика движения, определяются заводами-изготовителями датчиков движения.

6. Минимальная эффективность механизмов защиты

Минимальная эффективность механизмов защиты датчика движения должна соответствовать **Высокому** уровню согласно определению, содержащемуся в [ITSEC].

7. Степень надежности

Степень надежности защиты датчика движения по системе ITSEC должна соответствовать уровню **E3** (согласно определению, содержащемуся в [ITSEC]).

8. Обоснование

В нижеследующей таблице приводится обоснование ЗФ с указанием:

- опасностей, для защиты от которых предназначены соответствующие ЗФ;
- связанных с информационными технологиями целей защиты, достижению которых способствуют соответствующие ЗФ.

	Опасности										ИТ-цели							
	Доступ	Сбои в работе	Испытания	Конструкция	Внешние_факторы	Аппаратная часть	Механическая_часть	Данные_о_движении	Питание	Данные_защиты	Программное_обеспечение	Сохраненные_данные	Доступ	Контроль	Аутентификация	Обработка	Надежность	Криптообмен_данными
Технические, организационные и процедурные средства																		
Разработка		x	x	x														
Изготовление			x	x														
Поставка						x					x	x						
Генерация данных защиты										x								
Передача данных защиты										x								
Утвержденные мастерские							x											
Механическое сопряжение							x											
Регулярная инспекция						x	x		x		x							
Правоприменительный контроль					x	x	x		x	x	x							
Новые версии п/о											x							
Защитные функции																		
Идентификация и аутентификация																		
UIA_101 Идентификация устройств	x						x					x		x				x

	Опасности										ИТ-цели							
	Доступ	Сбои в работе	Испытания	Конструкция	Внешние_факторы	Аппаратная часть	Механическая_часть	Данные_о_движении	Питание	Данные_защиты	Программное_обеспечение	Сохраненные_данные	Доступ	Контроль	Аутентификация	Обработка	Надежность	Криптообмен_данными
UIA_102 Идентификационные данные устройств	x											x		x				
UIA_103 Идент. данные БУ													x					
UIA_104 Аутентификация устройств	x						x					x		x				x
UIA_105 Повторная аутентификация	x						x					x		x				x
UIA_106 Нефальсифицируемая аутентификация	x						x					x		x				
UIA_107 Отрицательная аутентификация							x						x			x		
Контроль доступа																		
ACC_101 Режим контроля за доступом	x								x		x	x						
ACC_102 ID датчика движения											x	x						
ACC_103 Пользовательские данные											x	x						
ACC_104 Данные защиты									x		x	x						
ACC_105 Структура файлов и условия доступа	x								x		x	x						
Отчетность																		
ACT_101 Идент. данные датчика движения													x					
ACT_102 Данные о подключении													x					
ACT_103 Учетные данные													x					

	Опасности											ИТ-цели						
	Доступ	Сбои в работе	Испытания	Конструкция	Внешние_факторы	Аппаратная часть	Механическая_часть	Данные_о_движении	Питание	Данные_защиты	Программное_обеспечение	Сохраненные_данные	Доступ	Контроль	Аутентификация	Обработка	Надежность	Криптообмен_данными
RLB_110 Перезагрузка		x															x	
RLB_111 Доступность данных																x	x	
RLB_112 Многоцелевое использование																	x	
Обмен данными																		
DEX_101 Экспорт защищенных данных о движении							x											x
Криптозащита																		
CSP_101 Алгоритмы																	x	x
CSP_102 Генерация ключей																	x	x
CSP_103 Рассылка ключей																	x	x
CSP_104 Доступ к ключам																	x	x
CSP_105 Уничтожение ключей																	x	x

ОБЩИЕ КОНТРОЛЬНЫЕ ПОКАЗАТЕЛИ ЗАЩИТЫ БОРТОВОГО УСТРОЙСТВА

1. Введение

В настоящем документе приводится описание бортового устройства с перечислением опасностей, которым оно должно противостоять, и целей, на которые должна быть направлена его защита. В нем указаны необходимые в этой связи защитные функции, минимальный уровень заявленной эффективности механизмов защиты и требуемая степень надежности при их разработке и аттестации.

Требования, о которых говорится в настоящем документе, сформулированы в основном тексте добавления 1В. В интересах ясности изложения некоторые контрольные показатели защиты дублируют положения основного текста добавления 1В. При

отсутствии однозначного совпадения между каким-либо из контрольных показателей и соответствующим ему положением основного текста добавления 1В следует руководствоваться основным текстом добавления 1В.

Требования основного текста добавления 1В, для которых не определены контрольные показатели, защитными функциями не охватываются.

Определения опасностей, целей и процедурных средств, а также спецификации защитных функций снабжены индивидуальными индексами для более наглядной увязки с проектной и аттестационной документацией.

2. Сокращения, определения и источники

2.1 Сокращения

АИ Аттестуемое изделие

БУ Бортовое устройство

ЗФ Защитная функция

PIN Персональный идентификационный номер

ROM Постоянная память (доступная только для чтения)

2.2 Определения

Цифровой тахограф	Контрольное устройство.
Данные о движении	Данные, которыми БУ обменивается с датчиком движения, позволяющие определять скорость и пробег транспортного средства.
Физически разделенные компоненты	Физические детали бортового устройства, установленные на транспортном средстве в разных местах, в отличие от физических деталей, сгруппированных внутри корпуса БУ.
Данные защиты	Конкретные данные, необходимые для обеспечения защитных функций (например, криптографические ключи).
Система	Технические средства, лица и организации, имеющие то или иное отношение к контрольному устройству.
Пользователь	Под пользователями понимаются люди, использующие то или иное оборудование. В круг пользователей БУ обычно входят водители, контролеры, мастерские и предприятия.
Пользовательские данные	Любые данные помимо данных о движении и данных защиты, регистрируемые и сохраняемые БУ в соответствии с требованиями главы III.12.

2.3 Источники

ITSEC Критерии оценки безопасности информационной технологии ITSEC, 1991 год.

3. Назначение и характеристика изделия

3.1 Описание и способ эксплуатации бортового устройства

БУ предназначено для установки на автотранспортных средствах. Оно служит для регистрации, хранения, отображения, распечатки и выдачи на внешние устройства данных о деятельности водителей.

БУ соединено с датчиком движения, с которым оно обменивается данными о движении транспортного средства.

При взаимодействии с БУ пользователи идентифицируют себя с помощью карточек тахографа.

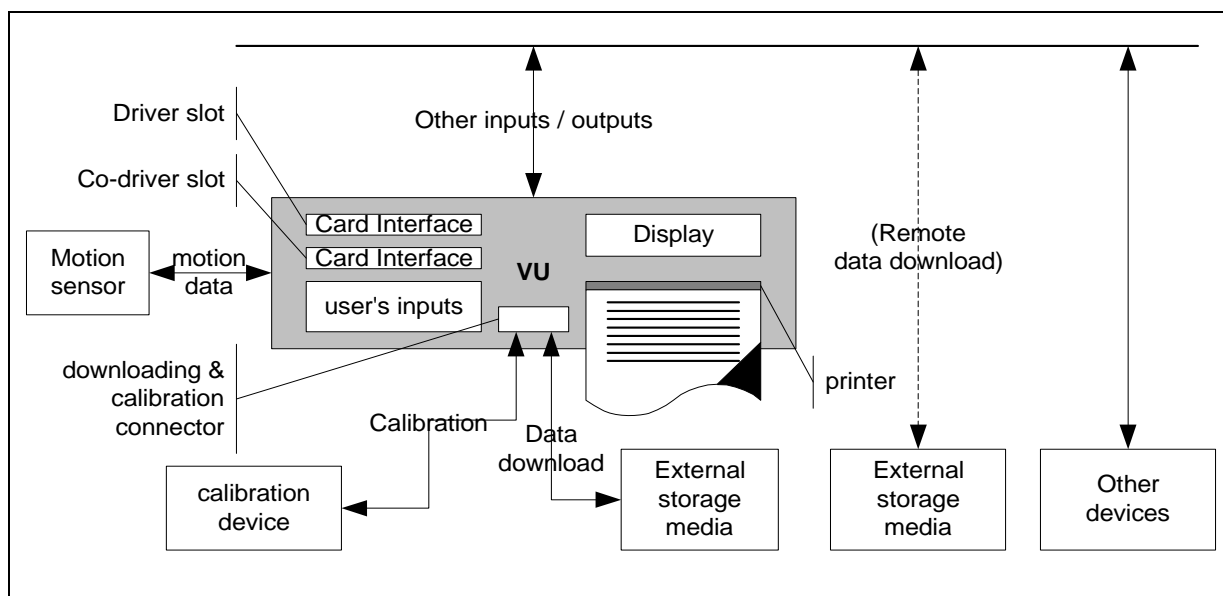
БУ регистрирует и сохраняет в своей памяти данные о деятельности пользователей; кроме того, данные о деятельности пользователей сохраняются им на карточках тахографа.

БУ способно отображать данные на дисплее, распечатывать их и передавать их на внешние устройства.

Операционная среда, в которой функционирует бортовое устройство, установленное на транспортном средстве, схематически показана на рисунке ниже.

Рис. 1

Операционная среда БУ



Счит. устройство карточки водителя			Другие входы/выходы			
Счит. устройство карточки 2-го водителя		Интерфейс карточки Интерфейс карточки	БУ	Дисплей	(Дистанционная загрузка данных)	
Датчик движения	Данные о движении	Ввод данных пользователем				
Загрузочный/калибровочный разъем		Калибровка	Загрузка данных		Печатающее устройство	
	Калибровочное устройство			Внешний носитель	Внешний носитель	Прочие устройства

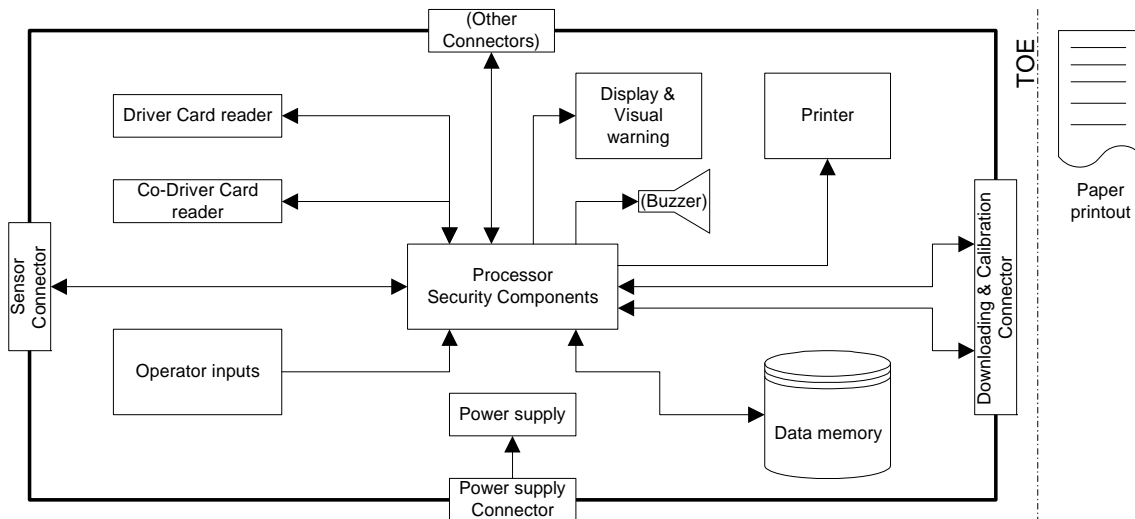
Общие характеристики БУ, описание его функций и режимов работы приводятся в главе II добавления 1В.

Конкретные требования к конструкции БУ изложены в главе III добавления 1В.

Типовая схема БУ представлена ниже.

Рис. 2

Типовая схема БУ (...) (не является обязательной)

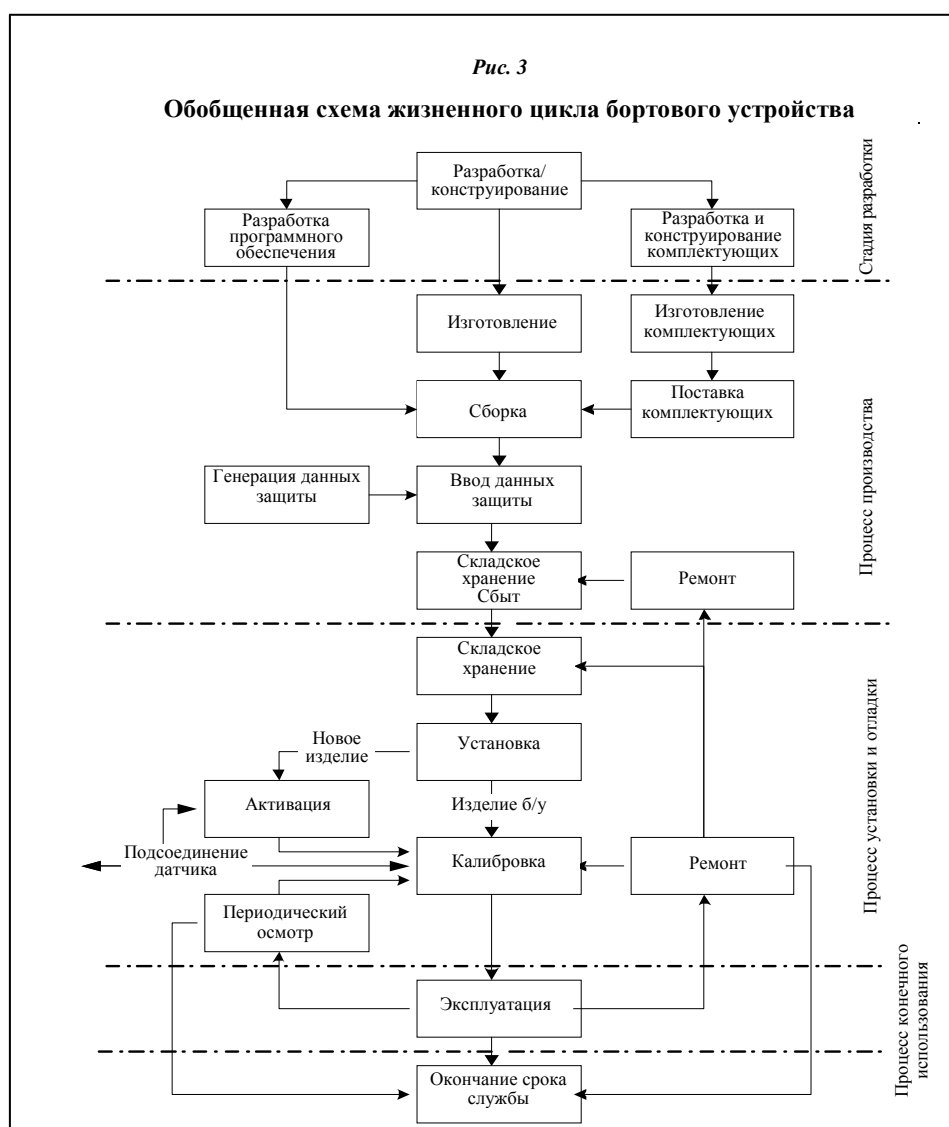


Разъем датчика	(Прочие разъемы)				Загрузочный/ калибровочный разъем	Аттестуемое изделие	Распечатка
	Счит. устройство карточки водителя		Дисплей и визуальные сигналы предупреждения	Печатающее устройство			
	Счит. устройство карточки 2-го водителя		(Звуковой сигнал)				
	Элементы защиты процессора						
	Ввод данных оператором	Питание		Запоминающее устройство для данных			
	Разъем цепи питания						

Следует иметь в виду, что хотя печатающее устройство является частью АИ, распечатанные им документы в состав АИ не входят.

3.2 Жизненный цикл бортового устройства

Типовая схема жизненного цикла БУ представлена ниже.



3.3 Опасности

Настоящий пункт содержит описание угроз, которым может подвергаться БУ.

3.3.1 Опасности, связанные с идентификационными данными и режимом контроля за доступом

О: Доступ

Пользователи могут пытаться получить доступ к не предназначенным для них функциям (например, водители - к функции калибровки).

О: Идентификационные_данные Пользователи могут пытаться воспользоваться другими идентификационными данными или вообще не использовать идентификационных данных.

3.3.2 Опасности, связанные с конструкцией устройства

О: Сбои в работе Отказы аппаратуры, сбои в функционировании программного обеспечения или процедурах обмена данными могут привести к непредвиденным ситуациям и ослабить защиту БУ.

О: Испытания Защита БУ может быть нарушена в результате использования неотключенных тест-режимов или имеющихся "обходных путей" доступа.

О: Конструкция Пользователи могут пытаться незаконным путем добыть сведения о конструкции устройства – будь то у изготовителя (хищение, подкуп и т.п.) или путем инженерного анализа.

3.3.3 Опасности в процессе эксплуатации

О: Параметры_калибровки Пользователи могут пытаться применять неверно откалиброванную аппаратуру (изменяя калибровочные данные или пользуясь организационными недосмотрами).

О: Обмен_данными_с_карточкой Пользователи могут пытаться внести изменения в данные в процессе их передачи между БУ и карточкой тахографа (подача добавочного или измененного сигнала, подавление сигнала, копирование и воспроизведение сигнала).

О: Часы Пользователи могут пытаться изменить показания встроенных часов.

О: Внешние_факторы Для преодоления защиты БУ пользователи могут пытаться использовать воздействие внешних

факторов (термических, электромагнитных, оптических, химических, механических и т.д.).

- О: Фальсификация_устройств Пользователи могут пытаться подключить к БУ фальсифицированные устройства (датчик движения, микропроцессорные карточки).
- О: Аппаратура Пользователи могут пытаться внести изменения в аппаратную часть БУ.
- О: Данные_о_движении Пользователи могут пытаться исказить данные о движении транспортного средства (подача добавочного или измененного сигнала, подавление сигнала, копирование и воспроизведение сигнала).
- О: Неактивированная_аппаратура Пользователи могут использовать неактивированную аппаратуру.
- О: Выходные_данные Пользователи могут пытаться внести изменения в выходные данные (при их распечатке, выводе на дисплей или загрузке на внешние устройства).
- О: Источник_питания Пользователи могут пытаться нейтрализовать защиту БУ путем изменения параметров тока в цепи питания (отключение, ослабление, усиление).
- О: Данные_защиты Пользователи могут пытаться получить несанкционированный доступ к данным защиты в процессе генерации этих данных, их передачи или хранения аппаратурой.
- О: Программное_обеспечение Пользователи могут пытаться внести изменения в программное обеспечение БУ.
- О: Сохраненные_данные Пользователи могут пытаться изменить сохраненные данные (данные защиты или пользовательские данные).

3.4 Цели защиты

Основная цель защиты системы цифрового тахографа заключается в следующем:

Ц: Основная
Данные, необходимые контрольным органам для проверки, должны иметься в наличии и обеспечивать полный и точный учет деятельности контролируемых водителей и эксплуатации контролируемых транспортных средств в том, что касается продолжительности управления, периодов работы, готовности и отдыха, а также скоростного режима.

Соответственно, цели защиты БУ, способствующие достижению вышеупомянутой основной цели, заключаются в следующем:

Ц: Основная (БУ)
Данные, подлежащие измерению, регистрации и последующей проверке контрольными органами, должны иметься в наличии и обеспечивать точный учет деятельности контролируемых водителей и эксплуатации контролируемых транспортных средств в том, что касается продолжительности управления, периодов работы, готовности и отдыха, а также скоростного режима.

Ц: Экспорт_данных (БУ)
БУ должно быть способно экспортировать данные на внешний носитель, обеспечивая при этом возможность проверки их целостности и подлинности.

3.5 Цели защиты в области информационных технологий

Конкретные цели защиты БУ в области ИТ, способствующие достижению главной цели защиты БУ, заключаются в следующем:

Ц: Доступ
БУ должно контролировать доступ пользователей к функциям и данным.

Ц: Отчетность	БУ должно обеспечивать сбор точных отчетных данных.
Ц: Надзор	БУ должно обеспечивать надзор за попытками преодоления защиты системы и отслеживать их связь с соответствующими пользователями.
Ц: Аутентификация	БУ должно производить аутентификацию пользователей и подключенных устройств (в случаях, когда необходим защищенный канал связи между устройствами).
Ц: Целостность	БУ должно защищать сохраненные данные от искажений.
Ц: Выходные_данные	БУ должно обеспечивать точное соответствие выходных данных тем данным, которые получены в результате измерений или хранятся в его памяти.
Ц: Обработка	БУ должно обеспечивать точность переработки вводимой информации в пользовательские данные.
Ц: Надежность	БУ должно функционировать надежно.
Ц: Защищенный_обмен_данными	БУ должно обеспечивать защиту данных, которыми оно обменивается с датчиком движения и карточками тахографа.

3.6 Технические, организационные и процедурные средства

В данном пункте излагаются технические, организационные и процедурные требования, связанные с защитой БУ.

3.6.1 Конструкция аппаратуры

С: Разработка	Разработчики БУ должны заботиться об обеспечении информационной безопасности при распределении функций на стадии конструирования.
---------------	---

С: Изготовление

Изготовители БУ должны заботиться об обеспечении информационной безопасности при распределении функций на стадии производства, а в процессе непосредственного изготовления БУ предохранять их от технического вмешательства, способного нарушить информационную защиту.

3.6.2 Поставка и активация аппаратуры

С: Поставка

Изготовители БУ, изготовители транспортных средств, сервисные центры и мастерские должны заботиться об обеспечении информационной безопасности на всех этапах работы с неактивированными БУ.

С: Активация

Изготовители транспортных средств, сервисные центры и мастерские должны, после установки БУ на транспортных средствах, активировать их до выхода транспортного средства из цеха, где произведена установка.

3.6.3 Генерация, передача и ввод данных защиты

С-3: Генерация_данных

Доступ к алгоритмам генерации данных защиты должны иметь только уполномоченные и пользующиеся доверием лица.

С-3: Перенос_данных_защиты

При генерации и передаче данных защиты, а также при их вводе в датчик движения должны соответствующим образом обеспечиваться конфиденциальность и целостность этих данных.

3.6.4 Выдача карточек

С: Доступ_к_карточкам

Карточки тахографа должны выдаваться только лицам, прошедшим соответствующий отбор.

- C: Единственность_карточки_водителя Водитель не может одновременно иметь более одной действительной карточки водителя.
- C: Учет_карточек Выдача карточек подлежит учету ("белые" и "черные" списки); "черные списки" должны использоваться при ревизионных проверках систем защиты.

3.6.5 Установка, калибровка и проверка контрольного устройства

- C: Утвержденные_мастерские Монтаж, калибровка и ремонт контрольных устройств должны производиться только в сервисных центрах или мастерских, пользующихся доверием и допущенных к таким работам.
- C: Регулярные_проверки Контрольное устройство должно регулярно проходить проверку и калибровку.
- C: Добросовестность_калибровки При калибровке контрольных устройств в утвержденных сервисных центрах или мастерских в эти устройства должны вводиться действительные параметры соответствующих транспортных средств.

3.6.6 Эксплуатация аппаратуры

- C: Добросовестность_водителей Водители должны соблюдать установленные правила и вести себя ответственно (пользоваться карточками водителя, правильно вводить данные о своей деятельности, когда эти данные вводятся вручную, и т.д.).

3.6.7 Правоприменительный контроль

- C: Контроль Правоприменительный контроль должен осуществляться как на регулярной, так и на

UIA_206 После регистрации (*количество определяется изготовителем, но не должно превышать 20*) неудачных попыток аутентификации подряд и/или после обнаружения несанкционированной (т.е. произведенной не в процессе калибровки контрольного устройства) замены датчика движения защитная функция должны обеспечивать:

- генерацию контрольной записи о событии;
- выдачу предупреждения пользователю;
- дальнейший прием и использование данных о движении, передаваемых датчиком движения, в незащищенном режиме.

4.1.2 Идентификация и аутентификация пользователей

UIA_207 БУ на постоянной основе избирательно отслеживает идентификационные данные двух пользователей по информации, считываемой с карточек тахографа, которые вводятся в считывающие устройства для карточек водителя и второго водителя.

UIA_208 Идентификационные данные пользователя состоят из:

- указания категории пользователя:
- ВОДИТЕЛЬ (карточка водителя),
- КОНТРОЛЕР (карточка контролера),
- МАСТЕРСКАЯ (карточка мастерской),
- ПРЕДПРИЯТИЕ (карточка предприятия),
- НЕТ ДАННЫХ (карточка не введена),
- идентификатора пользователя, который включает:
- код выдавшей карточку Договаривающейся стороны и номер карточки;
- параметр UNKNOWN, если НЕТ ДАННЫХ о том, к какой категории принадлежит пользователь.

Пользователи, идентификатор которых содержит параметр UNKNOWN, могут быть опознаваемыми непосредственно или по косвенным признакам.

UIA_209 БУ должно аутентифицировать пользователей при вводе карточек.

UIA_210 БУ должно производить повторную аутентификацию пользователей:

- при возобновлении подачи питания;
- на периодической основе или после конкретных событий (*периодичность определяется изготовителем, но должна составлять более одного раза в сутки*).

UIA_211 Аутентификация производится путем подтверждения того, что введенная в устройство карточка является действительной карточкой тахографа и содержит данные защиты, которые могли быть получены только из системы. Процесс аутентификации является двусторонним и инициируется бортовым устройством.

UIA_212 В дополнение к вышеизложенному обязательным требованием является положительная аутентификация мастерских с помощью PIN-кода. PIN-код должен состоять не менее чем из 4 знаков.

Примечание. Если PIN-код передается на БУ с внешней аппаратуры, расположенной вблизи от БУ, то меры по защите конфиденциальности PIN-кода при передаче не требуются.

UIA_213 БУ должно выявлять и предотвращать использование скопированных и повторно воспроизводимых аутентификационных данных.

UIA_214 После регистрации 5 неудачных попыток аутентификации подряд защитная функция должна обеспечивать:

- генерацию контрольной записи о событии;
- выдачу предупреждения пользователю;
- отнесение пользователя к категории НЕТ ДАННЫХ и признание карточки недействительной (определение "z" и требование 007).

4.1.3 Идентификация и аутентификация предприятия при дистанционном подключении

Возможность дистанционного подключения предприятия не обязательна. Поэтому настоящий пункт применяется лишь в тех случаях, когда эта функция реализована.

UIA_215 При каждом взаимодействии с дистанционно подключенным предприятием БУ должно иметь возможность идентифицировать это предприятие.

UIA_216 Идентификационные данные предприятия, использующего дистанционное подключение, состоят из кода Договаривающейся стороны, которая выдала карточку предприятия, и номера карточки предприятия.

UIA_217 Экспорту каких-либо данных БУ в адрес дистанционно подключенного предприятия должна предшествовать положительная аутентификация этого предприятия бортовым устройством.

UIA_218 Аутентификация производится путем подтверждения того, что у предприятия имеется действительная карточка предприятия, содержащая данные защиты, которые могли быть получены только из системы.

UIA_219 БУ должно выявлять и предотвращать использование скопированных и повторно воспроизводимых аутентификационных данных.

UIA_220 После регистрации 5 неудачных попыток аутентификации подряд БУ должно обеспечивать:

- выдачу предупреждения дистанционно подключенному предприятию.

4.1.4 Идентификация и аутентификация административных устройств

Изготовителями БУ могут быть предусмотрены специальные устройства для выполнения дополнительных административных функций, связанных с БУ (таких, как установка обновлений программного обеспечения, перезагрузка данных защиты и т.п.). Настоящий пункт применяется лишь при наличии подобных устройств.

UIA_221 При каждом взаимодействии с административным устройством БУ должно иметь возможность идентифицировать это устройство.

UIA_222 Любому дальнейшему взаимодействию должна предшествовать успешная аутентификация административного устройства бортовым устройством.

UIA_223 БУ должно выявлять и предотвращать использование скопированных и повторно воспроизводимых аутентификационных данных.

4.2 Контроль за доступом

Средства контроля за доступом обеспечивают, чтобы возможность считывать, вводить или изменять информацию в АИ имели только санкционированные лица.

Следует иметь в виду, что хотя регистрируемые БУ пользовательские данные могут рассматриваться как чувствительные с точки зрения защиты личных данных или коммерческой тайны, конфиденциального характера они не носят. Поэтому

функциональное требование, касающееся прав доступа к считке этих данных (требование 011), не обеспечивается соответствующей защитной функцией.

4.2.1 Режим контроля за доступом

ACC_201 БУ должно обеспечивать учет и контроль прав доступа к функциям и данным.

4.2.2 Права доступа к функциям

ACC_202 БУ обеспечивает соблюдение правил выбора режима работы устройства (требования 006 - 009).

ACC_203 В рамках соответствующих режимов работы БУ обеспечивает соблюдение правил контроля за доступом к функциям (требование 010).

4.2.3 Права доступа к данным

ACC_204 БУ обеспечивает соблюдение правил доступа к функции сохранения идентификационных данных БУ (требование 076).

ACC_205 БУ обеспечивает соблюдение правил доступа к функции сохранения идентификационных данных подсоединенного к нему датчика движения (требования 079 и 155).

ACC_206 После активации БУ бортовое устройство обеспечивает, чтобы калибровочные данные могли вводиться в БУ и сохраняться в его памяти только тогда, когда устройство находится в режиме калибровки (требования 154 и 156).

ACC_207 После активации БУ бортовое устройство обеспечивает соблюдение правил доступа к функции сохранения и удаления калибровочных данных (требование 097).

ACC_208 После активации БУ бортовое устройство обеспечивает, чтобы данные корректировки времени могли вводиться в БУ и сохраняться в его памяти только тогда, когда устройство находится в режиме калибровки (данное требование не распространяется на незначительные корректировки времени, допустимые согласно требованиям 157 и 158).

АСС_209 После активации БУ бортовое устройство обеспечивает соблюдение правил доступа к функции сохранения и удаления данных корректировки времени (требование 100).

АСС_210 БУ должно обеспечивать соответствующий режим доступа к функциям считывания и сохранения данных защиты (требование 080).

4.2.4 Структура файлов и условия доступа к ним

АСС_211 Структура файлов приложений и файлов данных и условия доступа к ним определяются в процессе изготовления и защищаются от любого последующего изменения или удаления.

4.3 Отчетность

АСТ_201 БУ должно обеспечивать отчетность водителей о своей деятельности (требования 081, 084, 087, 105a, 105b, 109 и 109a).

АСТ_202 В БУ должны храниться неизменяемые идентификационные данные (требование 075).

АСТ_203 БУ должно обеспечивать отчетность мастерских о своей деятельности (требования 098, 101 и 109).

АСТ_204 БУ должно обеспечивать отчетность контролеров о своей деятельности (требования 102, 103 и 109).

АСТ_205 БУ должно регистрировать данные счетчика пробега (требование 090) и подробные данные о скоростном режиме (требование 093).

АСТ_206 БУ должно обеспечивать, чтобы пользовательские данные, имеющие отношение к требованиям 081 - 093 и 102 - 105b включительно, не изменялись после их сохранения, за исключением случаев, когда они становятся наиболее старыми из хранящихся в памяти данных и подлежат замене новыми данными.

ACT_207 БУ должно обеспечивать, чтобы данные, уже сохраненные на карточке тахографа, не изменялись бортовым устройством (требования 109 и 109a), за исключением случаев замены наиболее старых данных новыми данными (требование 110) и случая, о котором говорится в примечании к пункту 2.1 подраздела I.

4.4 Контроль

Контрольные функции необходимы только в связи с событиями, которые могут указывать на попытки вмешательства в работу устройства или нарушения его защиты. При обычном осуществлении пользовательских прав, даже имеющих отношение к защите, эти функции не требуются.

AUD_201 События, затрагивающие защиту БУ, регистрируются БУ вместе с соответствующими данными (требования 094, 096 и 109).

AUD_202 К событиям, затрагивающим защиту БУ, относятся:

- попытки нарушения защиты:
 - отрицательный результат аутентификации датчика движения;
 - отрицательный результат аутентификации карточки тахографа;
 - несанкционированная замена датчика движения;
 - ошибка при проверке целостности данных, введенных с карточки;
 - ошибка при проверке целостности сохраненных пользовательских данных;
 - ошибка внутренней передачи данных;
 - несанкционированное вскрытие корпуса;
 - умышленная порча оборудования;
- ошибка в данных о движении;
- перерыв в подаче питания;
- внутренние неполадки в БУ.

AUD_203 В БУ обеспечивается соответствующий режим хранения контрольных записей (требования 094 и 096).

AUD_204 Контрольные записи, генерированные датчиком движения, сохраняются в памяти БУ.

AUD_205 Должна быть предусмотрена возможность вывода контрольных записей на дисплей, их распечатки и загрузки на внешние устройства.

4.5 Повторное использование объектов

REU_201 БУ обеспечивает возможность повторного использования временно сохраненных объектов без недопустимой дополнительной передачи информации.

4.6 Достоверность

4.6.1 Правила контроля за поступлением информации

ACR_201 БУ должно обеспечивать, чтобы пользовательские данные, имеющие отношение к требованиям 081, 084, 087, 090, 093, 102, 104, 105, 105а и 109, принимались к обработке лишь при условии их поступления из следующих источников:

- данные о движении транспортного средства;
- часы реального времени, встроенные в БУ;
- параметры калибровки контрольного устройства;
- карточки тахографа;
- ввод данных пользователем.

ACR_201a БУ должно обеспечивать возможность ввода пользовательских данных, имеющих отношение к требованию 109а, только за период с момента последнего извлечения карточки до ввода карточки, находящейся в устройстве на данный момент (требование 050а).

4.6.2 Внутренняя передача данных

Требования настоящего пункта применяются лишь к тем БУ, в которых используются физически разделенные компоненты.

ACR_202 Если между физически разделенными компонентами БУ передаются данные, то эти данные должны быть защищены от изменения.

ACR_203 При обнаружении ошибки передачи данных в процессе их внутренней передачи передача осуществляется повторно, а ЗФ генерирует контрольную запись об этом событии.

4.6.3 Целостность сохраненных данных

ACR_204 БУ должно проверять целостность хранящихся в его памяти пользовательских данных.

ACR_205 В случае ошибки при проверке целостности сохраненных пользовательских данных ЗФ генерирует контрольную запись.

4.7 Надежность функционирования

4.7.1 Испытания

RLB_201 Все команды, функции и контакты, предназначенные исключительно для тестирования БУ на стадии производства, перед активацией БУ блокируются или удаляются. Возможность их восстановления для последующего использования должна быть исключена.

RLB_202 При включении, а также в процессе работы в обычном режиме БУ должно производить самопроверку для подтверждения того, что оно функционирует нормально. При самопроверке БУ проверяется целостность данных защиты и хранящихся в памяти исполнимых команд (если они не сохранены в ROM).

RLB_203 В случае обнаружения внутренних неполадок в процессе самопроверки ЗФ обеспечивает:

- генерацию отчетной записи (если устройство не находится в режиме калибровки) (внутренние неполадки в БУ);
- целостность сохраненных данных.

4.7.2 Программное обеспечение

RBL_204 Возможность анализа или отладки программного обеспечения активированного БУ в полевых условиях должна быть исключена.

RLB_205 Данные, поступающие из внешних источников, не должны восприниматься в качестве исполнимых команд.

4.7.3 Физическая защита

RLB_206 Если конструкция БУ допускает вскрытие его корпуса, то БУ, когда оно не находится в режиме калибровки, должно регистрировать любое такое вскрытие и сохранять эту способность даже при отключении от внешнего источника питания в течение как минимум шести месяцев. При этом ЗФ генерирует отчетную запись (допускается возможность генерации и сохранения такой записи после возобновления питания).

Если конструкция БУ не предусматривает вскрытия корпуса, то она должна обеспечивать легкое обнаружение следов физического воздействия (например, при внешнем осмотре).

RLB_207 После активации БУ должно производиться тестирование с целью выявления конкретных видов умышленной порчи оборудования (определяются изготовителем).

RLB_208 В случае обнаружения такой порчи оборудования ЗФ генерируют надзорную запись, а БУ (определяется изготовителем).

4.7.4 Прекращение электропитания

RLB_209 БУ должно регистрировать отклонения от номинальных параметров тока в цепи питания, в том числе отключения от источника питания.

RLB_210 В вышеупомянутых случаях ЗФ обеспечивает:

- генерацию надзорной записи (если устройство не находится в режиме калибровки);
- сохранение защищенности БУ;
- сохранение функций защиты не отключенных компонентов и процессов;
- целостность сохраненных данных.

4.7.5 Перезапуск

RLB_211 При перерыве в подаче питания, при досрочном прерывании текущей операции или при наступлении любых других условий, требующих перезапуска, БУ полностью перезапускается.

4.7.6 Доступность данных

RLB_212 БУ должно предоставлять доступ к имеющимся ресурсам данных по мере необходимости, обеспечивать отсутствие неоправданных обращений к ресурсам и предусматривать стирание ненужных данных.

RLB_213 БУ должно обеспечивать невозможность извлечения карточек до сохранения на них соответствующих данных (требования 015 и 016).

RLB_214 В указанном выше случае ЗФ генерирует контрольную запись о данном событии.

4.7.7 Многоцелевое использование

RLB_215 Если БУ используется для других целей, помимо функции тахографа, то все соответствующие приложения должны быть физически и/или логически отделены друг от друга. Данные защиты не должны быть общими для этих приложений. Одновременное выполнение более чем одной функции не допускается.

4.8 Обмен данными

В настоящем пункте рассматривается обмен данными между БУ и подключенными к нему устройствами.

4.8.1 Обмен данными с датчиком движения

DEX_201 БУ должно проверять целостность и подлинность данных о движении, импортируемых с датчика движения.

DEX_202 В случае обнаружения ошибки при проверке целостности или подлинности данных о движении ЗФ обеспечивает:

- генерацию контрольной записи;
- дальнейшее использование импортируемых данных.

4.8.2 Обмен данными с карточками тахографа

DEX_203 БУ должно проверять целостность и подлинность данных, импортируемых с карточек тахографа.

DEX_204 В случае обнаружения ошибки при проверке целостности или подлинности данных, поступающих с карточки, БУ:

- генерирует контрольную запись;
- не использует поступившие данные.

DEX_205 БУ экспортирует данные на микропроцессорные карточки тахографа с соответствующими атрибутами защиты, позволяющими карточке проверять их целостность и подлинность.

4.8.3 Обмен данными с внешним носителем (функция загрузки данных)

DEX_206 БУ генерирует информацию, подтверждающую происхождение данных, загружаемых на внешний носитель.

DEX_207 БУ обеспечивает возможность проверки получателем информации, подтверждающей происхождение загруженных данных.

DEX_208 БУ загружает данные на внешний носитель с соответствующими атрибутами защиты, позволяющими проверять целостность и подлинность загруженных данных.

4.9 Криптографическая защита

Требования данного пункта применяются лишь в необходимых случаях, в зависимости от используемых механизмов защиты и примененных изготовителем технических решений.

CSP_201 Любые криптографические операции, выполняемые БУ, должны соответствовать заданному алгоритму при заданном размере ключа.

CSP_202 Если БУ генерирует криптографические ключи, то это должно делаться в соответствии с заданными алгоритмами генерации криптографических ключей при заданных размерах таких ключей.

CSP_203 Если БУ рассылает криптографические ключи, то это должно делаться в соответствии с установленными методами рассылки ключей.

CSP_204 Если БУ получает доступ к криптографическим ключам, то это должно соответствовать установленному порядку доступа к криптографическим ключам.

CSP_205 Если БУ уничтожает криптографические ключи, то это должно делаться в соответствии с установленными методами уничтожения криптографических ключей.

5. Определение механизмов защиты

Обязательные механизмы защиты указаны в подразделе XI.

Все остальные механизмы защиты определяются изготовителями по их усмотрению.

6. Минимальная эффективность механизмов защиты

Минимальная эффективность механизмов защиты бортового устройства должна соответствовать "высокому" уровню согласно определению, содержащемуся в [ITSEC].

7. Степень надежности

Степень надежности защиты бортового устройства по системе ITSEC должна соответствовать уровню E3 (согласно определению, содержащемуся в [ITSEC]).

8. Обоснование

В нижеследующей таблице приводится обоснование ЗФ с указанием:

- опасностей, для защиты от которых предназначены соответствующие ЗФ;
- связанных с информационными технологиями целей защиты, достижению которых способствуют соответствующие ЗФ.

	Опасности														ИТ-цели														
	Доступ	Идент. данные	Сбои в работе	Испытания	Конструкция	Калибров. параметры	Обм. данными с карт.	Часы	Внешние факторы	Фальсиф. устройств	Аппаратная часть	Данные о движении	Не активировано	Выходные данные	Питание	(оставлено пустым)	Данные защиты	Прогр. обеспечение	Сохраненные данные	Доступ	Отчетность	Контроль	Аутентификация	Целостность	Вывод данных	Обработка	Надежность	Криптообм. данными	
Технические, организационные и процедурные средства																													
Разработка			x	x	x																								
Изготовление				x	x																								
Поставка													x																
Активация	x											x																	
Генерация данных защиты																	x												
Перенос данных защиты																	x												
Наличие карточки	x																												
Единственность карточки водителя	x																												
История карточки	x																												
Утвержденные мастерские						x	x																						
Регулярная инспекция Калибровка						x	x		x					x			x												
Добросовестные мастерские						x	x																						
Добросовестные водители	x																												
Правоприменительный контроль	x					x	x	x	x	x	x	x	x	x	x	x	x												
Новые версии п/о																		x											
Защитные функции																													
Идентификация и аутентификация																													
UIA_201 Идентификация датчика										x	x												x						x
UIA_202 Идент. данные датчика										x	x												x						
UIA_203 Аутентификация датчика										x	x												x						x

	Опасности															ИТ-цели												
	Доступ	Идент. данные	Сбой в работе	Испытания	Конструкция	Калибров. параметры	Обм. данными с карт.	Часы	Внешние факторы	Фальсиф. устройств	Аппаратная часть	Данные о движении	Не активировано	Выходные данные	Питание	(оставлено пустым)	Данные защиты	Прогр. обеспечение	Сохраненные данные	Доступ	Отчетность	Контроль	Аутентификация	Целостность	Вывод данных	Обработка	Надежность	Криптообм. данными
UIA_204									x	x												x						x
UIA_205									x	x												x						
UIA_206									x	x											x					x		
UIA_207	x	x							x											x		x						x
UIA_208	x	x							x											x		x						
UIA_209	x	x							x											x		x						x
UIA_210	x	x							x											x		x						x
UIA_211	x	x							x											x		x						
UIA_212	x	x				x	x													x		x						
UIA_213	x	x							x											x		x						
UIA_214	x	x							x												x							
UIA_215	x	x																		x		x						x
UIA_216	x	x																		x		x						
UIA_217	x	x																		x		x						x

	Опасности															ИТ-цели												
	Доступ	Идент. данные	Сбой в работе	Испытания	Конструкция	Калибров. параметры	Обм. данными с карт.	Часы	Внешние факторы	Фальсиф. устройств	Аппаратная часть	Данные о движении	Не активировано	Выходные данные	Питание	(оставлено пустым)	Данные защиты	Прогр. обеспечение	Сохраненные данные	Доступ	Отчетность	Контроль	Аутентификация	Целостность	Вывод данных	Обработка	Надежность	Криптообм. данными
ACC_209 Данные корректировки времени							x											x	x									
ACC_210 Данные защиты																	x	x	x									
ACC_211 Структура файлов и условия доступа	x				x												x	x	x									
Отчетность																												
ACT_201 Отчетность водителей																					x							
ACT_202 Идент. данные БУ																					x	x						
ACT_203 Отчетность мастерских																					x							
ACT_204 Отчетность контролеров																					x							
ACT_205 Отчетность о движении т/с																					x							
ACT_206 Изменение отчетных данных																		x					x				x	
ACT_207 Изменение отчетных данных																		x					x				x	

ОБЩИЕ КОНТРОЛЬНЫЕ ПОКАЗАТЕЛИ ЗАЩИТЫ КАРТОЧКИ ТАХОГРАФА

1. Введение

В настоящем документе приводится описание карточки тахографа с перечислением опасностей, которым она должна противостоять, и целей, на которые должна быть направлена ее защита. В нем указаны необходимые для этого защитные функции, минимальный уровень заданной эффективности механизмов защиты и требуемая степень надежности при их разработке и аттестации.

Требования, о которых говорится в настоящем документе, сформулированы в основном тексте добавления 1В. В интересах ясности изложения некоторые контрольные показатели защиты дублируют положения основного текста добавления 1В. При отсутствии однозначного совпадения между каким-либо из контрольных показателей и соответствующим ему положением основного текста добавления 1В следует руководствоваться основным текстом добавления 1В.

Требования основного текста добавления 1В, для которых не определены контрольные показатели, защитными функциями не охватываются.

Карточка тахографа представляет собой стандартную карточку со встроенной микросхемой, в которую введена специализированная прикладная программа тахографа, отвечающую современным требованиям в отношении функциональных возможностей и защиты микропроцессорных карточек. Соответственно, изложенные здесь контрольные показатели защиты касаются только дополнительных потребностей в защите, непосредственно связанных с функциями тахографа.

Определения опасностей, целей и процедурных средств, а также спецификации защитных функций снабжены индивидуальными индексами для более наглядной увязки с проектной и аттестационной документацией.

2. Сокращения, определения и источники

2.1 Сокращения

АИ Аттестуемое изделие

БУ Бортовое устройство

ЗФАИ Защитная функция АИ

- МП** Микропроцессор
(электронная схема, предназначенная для обработки и/или хранения данных),
ОС Операционная система
PIN Персональный идентификационный номер
РЗФ Режим защитных функций
ROM Постоянная память (доступная только для чтения)

2.2 Определения

Цифровой тахограф	Контрольное устройство.
Чувствительные данные	Данные, хранящиеся на карточке тахографа и нуждающиеся в защите от искажений, несанкционированных изменений и нарушений конфиденциальности (в части, касающейся данных защиты). К чувствительным данным относятся данные защиты и пользовательские данные.
Данные защиты	Конкретные данные, необходимые для обеспечения защитных функций (например, криптографические ключи).
Система	Технические средства, лица и организации, имеющие то или иное отношение к контрольному устройству.
Пользователь	Любой субъект (человек или внешнее электронное устройство) вне АИ, вступающий во взаимодействие с АИ.
Пользовательские данные	Чувствительные данные помимо данных защиты, хранящиеся на карточке тахографа. К пользовательским данным относятся идентификационные данные и данные о деятельности.
Идентификационные данные	Идентификационные данные включают идентификационные данные карточки и идентификационные данные держателя карточки.
Идентификационные данные карточки	Пользовательские данные, имеющие отношение к идентификации карточки, как это определено требованиями 190, 191, 192, 194, 215, 231 и 235.

Идентификационные данные держателя карточки	Пользовательские данные, имеющие отношение к идентификации держателя карточки, как это определено требованиями 195, 196, 216, 232 и 236.
Данные о деятельности	Данные о деятельности включают данные о деятельности держателя карточки, данные о событиях и неисправностях и данные о контрольных мероприятиях.
Данные о деятельности держателя карточки	Пользовательские данные, имеющие отношение к деятельности держателя карточки, как это определено требованиями 197, 199, 202, 212, 212а, 217, 219, 221, 226, 227, 229, 230а, 233 и 237.
Данные о событиях и отказах	Пользовательские данные, имеющие отношение к событиям или неисправностям, как это определено требованиями 204, 205, 207, 208 и 223.
Данные о контрольных мероприятиях	Пользовательские данные, имеющие отношение к правоприменительному контролю, как это определено требованиями 210 и 225.

2.3 Источники

ITSEC	Критерии оценки безопасности информационной технологии ITSEC, 1991 год.
IC PP	Smartcard Integrated Circuit Protection Profile - version 2.0 - issue September 1998. Registered at French certification body under the number PP/9806.
ES PP	Smart Card Integrated Circuit With Embedded Software Protection Profile - version 2.0 - issue June 99. Registered at French certification body under the number PP/9911.

3. Назначение и характеристика изделия

3.1 Описание и способ эксплуатации карточки тахографа

Карточка тахографа представляет собой карточку со встроенной микросхемой, соответствующую описанию, которое приводится в источниках [IC PP] и [ES PP], и несущую в себе прикладную программу для использования этой карточки совместно с контрольным устройством.

Основными функциями карточки тахографа являются:

- хранение идентификационных данных карточки и ее держателя. Эти данные используются бортовым устройством для идентификации держателя карточки, предоставления полагающегося ему доступа к функциям и данным и обеспечения отчетности держателя карточки о своих действиях;
- хранения данных о деятельности держателя карточки, данных о событиях и неисправностях и данных о контрольных мероприятиях, имеющих отношение к держателя карточки.

Таким образом, карточка тахографа предназначена для взаимодействия с бортовым устройством через его интерфейс для считки карточек. Она также может использоваться посредством любого считывающего устройства карт (например, подключенного к персональному компьютеру), через который можно получить полный доступ к любым пользовательским данным для их чтения.

На стадии конечного использования карточки тахографа (7-й этап "жизненного цикла", описание которого содержится в [ES PP]), бортовые устройства могут осуществлять только запись на нее пользовательских данных.

Требования к функциональным возможностям карточки тахографа изложены в основном тексте добавления 1В и в подразделе II.

3.2 Жизненный цикл карточек тахографа

Жизненный цикл карточек тахографа соответствует жизненному циклу карточек со встроенной микросхемой, описание которого приводится в [ES PP].

3.3 Опасности

Помимо перечисленных в [ES PP] и [IC PP] общих опасностей, актуальных для всех карточек со встроенной микросхемой, карточки тахографа могут подвергаться следующим опасностям:

3.3.1 Конечные цели нарушителей защиты

Конечной целью попыток преодоления защиты является изменение хранящихся в АИ пользовательских данных.

- О: Идент._данные Успешное изменение хранящихся в АИ идентификационных данных (таких, как тип карточки, срок ее действия или идентификационные данные держателя) создает возможность мошенничества при использовании АИ и ставит под серьезную угрозу достижение общих целей защиты системы.
- О: Данные_о_деят. Успешное изменение хранящихся в АИ данных о деятельности подрывает защиту АИ.
- О: Обмен_данными Успешное изменение (добавление, изъятие, искажение) данных о деятельности при их импорте или экспорте подрывает защиту АИ.

3.3.2 Пути преодоления защиты

Для преодоления защиты АИ могут использоваться следующие методы:

- несанкционированное получение сведений об устройстве аппаратной части и программного обеспечения АИ, и в первую очередь о его защитных функциях или данных защиты. Такие сведения могут быть получены в результате незаконного завладения материалами разработчика или изготовителя (путем хищения, подкупа и т.д.) или в результате непосредственного изучения АИ (физическое исследование, дедуктивный анализ и т.д.);
- использование слабых мест конструкции или технического исполнения АИ (инженерных просчетов, ошибок программного обеспечения, сбоев при передаче данных, отклонений в работе АИ, спровоцированных экстремальным воздействием внешних факторов, недостатков защитных функций – таких, как процедуры аутентификации, контроль за доступом к данным, криптографическая защита и т.д.);
- воздействие на АИ или его защитные функции с помощью физических, электрических или логических средств по отдельности или в сочетании друг с другом.

3.4 Цели защиты

Основная цель защиты всей системы цифрового тахографа заключается в следующем:

Ц: Основная
Данные, необходимые контрольным органам для проверки, должны иметься в наличии и обеспечивать полный и точный учет деятельности контролируемых водителей и эксплуатации контролируемых транспортных средств в том, что касается продолжительности управления, периодов работы, готовности и отдыха, а также скоростного режима.

Соответственно, основные цели защиты АИ, способствующие достижению вышеупомянутой основной цели, заключаются в следующем:

Ц: Идент._данные_карточки
АИ должно сохранять в неприкосновенности идентификационные данные карточки и идентификационные данные держателя карточки, введенные в память в процессе его персонализации.

Ц: Сохр._карточкой_данных_о_деят.
АИ должно сохранять в неприкосновенности пользовательские данные, введенные в память карточки бортовым устройством.

3.5 Цели защиты в области информационных технологий

Помимо перечисленных в [ES PP] и [IC PP] целей защиты, являющихся общими для всех карточек со встроенной микросхемой, реализации основных целей защиты АИ на стадии его конечного использования способствует достижение следующих специфических целей, связанных с информационными технологиями:

Ц: Доступ_к_данным
АИ должно предоставлять доступ к функции сохранения пользовательских данных только аутентифицированным бортовым устройствам.

Ц: Криптозащита_сообщений
АИ должно поддерживать протоколы и процедуры криптозащищенного обмена данными между карточкой и устройством считывания карточек, когда это необходимо для выполнения соответствующих функций.

3.6 Технические, организационные и процедурные средства

Технические, организационные и процедурные требования, направленные на защиту АИ, перечислены в [ES PP] и [IC PP] (разделы о целях защиты, связанных с операционной средой).

4. Защитные функции

В данном пункте конкретизируются некоторые из допустимых операций, такие как постановка функциональных задач или выбор [ES PP], и излагаются дополнительные функциональные требования к ЗФ.

4.1 Соответствие профилям защиты

CPP_301 АИ должно соответствовать [IC PP].

CPP_302 АИ должно соответствовать [ES PP], с учетом дальнейших уточнений.

4.2 Идентификация и аутентификация пользователей

Карточка должна идентифицировать устройство, в которое она введена, и распознавать, является ли это устройство аутентифицированным бортовым устройством. Допускается экспорт любых пользовательских данных с карточки на любое считывающее устройство; исключения составляют карточки контролера и карточки предприятия, идентификационные данные держателей которых могут экспортироваться только на аутентифицированные бортовые устройства (соответственно, появление имени контролера на дисплее или в распечатке служит доказательством того, что бортовое устройство не фальсифицировано).

4.2.1 Идентификация пользователей

Функциональная задача (FIA_UID.1.1) *Перечень действий со стороны ЗФАИ:* не требуются.

Функциональная задача (FIA_ATD.1.1) *Перечень атрибутов защиты:*

- **КАТЕГОРИЯ_ПОЛЬЗОВАТЕЛЕЙ:** БОРТОВОЕ_УСТРОЙСТВО,
НЕ_БОРТОВОЕ_УСТРОЙСТВО,

- **ID_ПОЛЬЗОВАТЕЛЯ:** Регистрационный номер транспортного средства (VRN) и код Договаривающейся стороны, где оно зарегистрировано (ID_ПОЛЬЗОВАТЕЛЯ известен только в случае, если КАТЕГОРИЯ ПОЛЬЗОВАТЕЛЕЙ = БОРТОВОЕ_УСТРОЙСТВО).

4.2.2 Аутентификация пользователей

Функциональная задача (FIA_UAU.1.1) Перечень действий со стороны ЗФАИ:

- карточка водителя и карточка мастерской: экспорт пользовательских данных с атрибутами защиты (функция загрузки данных с карточки);
- карточка контролера: экспорт пользовательских данных без атрибутов защиты помимо идентификационных данных держателя карточки.

UIA_301 Аутентификация бортового устройства осуществляется путем подтверждения наличия в нем данных защиты, которые могут быть получены только из системы.

Выбор (FIA_UAU.3.1 и FIA_UAU.3.2): блокировать.

Функциональная задача (FIA_UAU.4.1) Заданный(е) механизм(ы) аутентификации: любой механизм аутентификации.

UIA_302 Для карточки мастерской предусмотрен дополнительный механизм аутентификации, заключающийся в проверке PIN-кода (этот механизм предназначается для подтверждения бортовым устройством данных о личности держателя карточки, а не для защиты содержания карточки мастерской).

4.2.3 Отрицательный результат аутентификации

Ниже представлены функциональные задачи, определяющие реакцию карточки в каждом конкретном случае, когда аутентификация пользователя дает отрицательный результат.

Функциональная задача (FIA_AFL.1.1) Номер: 1, перечень событий в процессе аутентификации: аутентификация устройства считывания карточек.

Функциональная задача (FIA_AFL.1.2) *Перечень действий:*

- выдача предупреждения на подключенное устройство;
- занесение пользователя в категорию НЕ_БОРТОВОЕ_УСТРОЙСТВО.

Ниже представлены также функциональные задачи, определяющие реакцию карточки в случае, когда аутентификация посредством дополнительного механизма согласно UIA_302 дает отрицательный результат.

Функциональная задача (FIA_AFL.1.1) *Номер: 5, перечень событий в процессе аутентификации:* проверка PIN (карточка мастерской).

Функциональная задача (FIA_AFL.1.2) *Перечень действий:*

- выдача предупреждения на подключенное устройство;
- блокировка процедуры проверки PIN-кода таким образом, чтобы любой введенный после этого PIN-код отклонялся;
- возможность информирования последующих пользователей о причинах блокировки.

4.3 Контроль за доступом

4.3.1 *Режим контроля за доступом*

На стадии конечного использования карточки тахографа для нее предусмотрен единственный защитный режим контроля за доступом (SFP), обозначаемый как AC_SFP.

Функциональная задача (FDP_ACC.2.1) *Контроль за доступом SFP:* AC_SFP.

4.3.2 *Функции контроля за доступом*

Функциональная задача (FDP_ACF.1.1) *Контроль за доступом SFP:* AC_SFP.

Функциональная задача (FDP_ACF.1.1) *Заданная группа атрибутов защиты:*
КАТЕГОРИЯ_ПОЛЬЗОВАТЕЛЕЙ.

Функциональная задача (FDP_ACF.1.2) Правила, регулирующие доступ контролируемых субъектов к контролируемым объектам посредством контролируемых операций с контролируемыми объектами:

- **ОБЩЕЕ_ЧТЕНИЕ:** Пользовательские данные могут считываться с АИ любым устройством; исключение составляют идентификационные данные держателя карточки, считывать которые с карточки контролера или карточки предприятия может только **БОРТОВОЕ_УСТРОЙСТВО**.

- **СОХР._ИДЕНТ._ДАННЫХ:** Идентификационные данные могут быть сохранены только один раз, причем до завершения 6-й стадии жизненного цикла карточки. Возможность сохранения или изменения идентификационных данных кем-либо из пользователей на стадии конечного использования карточки исключается.

- СОХР._ДАННЫХ_О_ДЕЯТЕЛЬНОИ.:** Сохранять на АИ данные о деятельности может только **БОРТОВОЕ_УСТРОЙСТВО**.

- ОБНОВЛЕНИЕ_ПО:** Обновление программного обеспечения АИ пользователями не допускается.

- СТРУКТУРА_ФАЙЛОВ:** Структура файлов и условия доступа к ним определяются до завершения 6-й стадии жизненного цикла АИ и защищаются от любого последующего изменения или удаления кем-либо из пользователей.

4.4 Отчетность

АСТ_301 АИ должно содержать неизменяемые идентификационные данные.

АСТ_302 Должны быть указаны время и дата персонализации АИ. Возможность изменения этих данных должна быть исключена.

4.5 Контроль

АИ должно отслеживать события, свидетельствующие о потенциальном нарушении его защиты.

Функциональная задача (FAU_SAA.1.2) *Подмножество типовых событий, регистрируемых в надзорных целях:*

- отрицательный результат аутентификации держателя карточки (5 неправильных вводов PIN-кода подряд);
- ошибка самопроверки;
- ошибка при проверке целостности сохраненных данных;
- ошибка при проверке целостности вводимых данных о деятельности.

4.6 Достоверность

4.6.1 Целостность сохраненных данных

Функциональная задача (FDP_SDI.2.2) *Необходимые действия:* выдача предупреждения на подключенное устройство,

4.6.2 Аутентификация основных данных

Функциональная задача (FDP_DAU.1.1) *Перечень объектов или типов информации:* данные о деятельности.

Функциональная задача (FDP_DAU.1.2) *Перечень субъектов:* любые.

4.7 Надежность функционирования

4.7.1 Испытания

Выбор (FPT_TST.1.1): при включении, периодически в обычном режиме работы.

Примечание. "При включении" означает до исполнения команды (но не обязательно в ходе процедуры ответа на сигнал перезапуска).

RLB_301 Процедура самопроверки АИ включает проверку целостности любого программного обеспечения кроме хранящегося в ROM.

RLB_302 При обнаружении ошибки во время самопроверки ЗФАИ выдает предупреждение на подключенное устройство.

RLB_303 По окончании тестирования ОС все команды и функции, специально предназначенные для тестирования, блокируются или удаляются. Возможность снятия блокировки и повторного использования этих функций должна быть исключена. Команды, рассчитанные на использование в пределах какой-либо одной стадии жизненного цикла, должны быть полностью недоступными на других стадиях.

4.7.2 Программное обеспечение

RLB_304 Возможность анализа, отладки или изменения программного обеспечения АИ в полевых условиях должна быть исключена.

RLB_305 Данные, поступающие из внешних источников, не должны восприниматься в качестве исполнимых команд.

4.7.3 Питание

RLB_306 Защита АИ не должна нарушаться при отключении от источника питания или при изменениях параметров тока в цепи питания.

4.7.4 Перезапуск

RLB_307 При отключении питания (или при изменениях параметров тока в цепи питания) АИ, при досрочном прерывании текущей операции или при наступлении любых других условий, требующих перезапуска, АИ полностью перезапускается.

4.8 Обмен данными

4.8.1 Обмен данными с бортовым устройством

DEX_301 АИ проверяет целостность и подлинность данных, импортируемых с бортового устройства.

DEX_302 В случае ошибки при проверке целостности импортируемых данных АИ:

- выдает предупреждение устройству, с которого поступают данные;
- не использует импортируемые данные.

DEX_303 АИ экспортирует пользовательские данные на бортовое устройство с соответствующими атрибутами защиты, позволяющими бортовому устройству проверять целостность и подлинность полученных данных.

4.8.2 Экспорт данных на устройства, не являющиеся бортовыми устройствами (функция загрузки)

DEX_304 АИ должно быть способно генерировать информацию, подтверждающую происхождение данных, загружаемых на внешний носитель.

DEX_305 АИ должно быть способно обеспечивать возможность проверки получателем информации, подтверждающей происхождение загруженных данных.

DEX_306 АИ должно быть способно загружать данные на внешний носитель с соответствующими атрибутами защиты, позволяющими проверять целостность загруженных данных.

4.9 Криптографическая защита

CSP_301 Если ЗФАИ генерирует криптографические ключи, то это должно делаться в соответствии с заданными алгоритмами генерации криптографических ключей при заданных размерах таких ключей. Генерируемые криптографические сеансовые ключи должны быть пригодными для использования ограниченное количество раз (*количество определяется изготовителем, но не должно превышать 240*).

CSP_302 Если ЗФАИ рассылает криптографические ключи, то это должно делаться в соответствии с установленными методами рассылки криптографических ключей.

5. Определение механизмов защиты

Обязательные механизмы защиты указаны в подразделе XI.

Все остальные механизмы защиты определяются изготовителем АИ по собственному усмотрению.

6. Заявленная минимальная эффективность механизмов защиты

Минимальная эффективность механизмов защиты карточки тахографа должна соответствовать "**Высокому**" уровню согласно определению, содержащемуся в [ITSEC].

7. Степень надежности

Степень надежности защиты карточки тахографа по системе ITSEC должна соответствовать уровню **E3** согласно определению, содержащемуся в [ITSEC].

8. Обоснование

В следующей таблице приводится обоснование дополнительных ЗФ с указанием:

- опасностей, для защиты от которых предназначены соответствующие ЗФ;
- связанных с информационными технологиями целей защиты, достижению которых способствуют соответствующие ЗФ.

ПОДРАЗДЕЛ XI
ОБЩИЕ МЕХАНИЗМЫ ЗАЩИТЫ
СОДЕРЖАНИЕ

	<u>Стр.</u>
1. Общие положения	416
1.1 Источники	416
1.2 Условные обозначения и сокращенные термины	417
2. Криптографические системы и алгоритмы	418
2.1 Криптографические системы	418
2.2 Криптографические алгоритмы	419
2.2.1 Алгоритм RSA	419
2.2.2 Хеш-алгоритм	419
2.2.3 Алгоритм шифрования данных	419
3. Ключи и сертификаты	420
3.1 Генерация и рассылка ключей	420
3.1.1 Генерация и рассылка ключей RSA	420
3.1.2 Испытательные ключи RSA	422
3.1.3 Ключи датчиков движения	422
3.1.4 Генерация и рассылка сеансовых ключей T-DES	423
3.2 Ключи	423
3.3 Сертификаты	423
3.3.1 Содержание сертификатов	423
3.3.2 Выдаваемые сертификаты	427
3.3.3 Проверка и расшифровка сертификатов	428
4. Механизм взаимной аутентификации	429
5. Механизмы обеспечения конфиденциальности, целостности и аутентификации данных при их передаче между БУ и карточками	432
5.1 Криптозащищенный обмен сообщениями	432
5.2 Обработка ошибок при криптозащищенном обмене сообщениями	435
5.3 Алгоритм расчета криптографических контрольных сумм	435
5.4 Алгоритм расчета криптограмм для защиты конфиденциальности ОД	436
6. Механизмы цифровой подписи при загрузке данных	437
6.1 Генерация подписей	437
6.2 Проверка подписей	438

1. Общие положения

Настоящий подраздел содержит конкретные указания относительно механизмов защиты, обеспечивающих:

- взаимную аутентификацию БУ и карточек тахографа, включая согласование сеансовых ключей;
- конфиденциальность, целостность и аутентификацию данных, передаваемых между БУ и карточками тахографа;
- целостность и аутентификацию данных, загружаемых с БУ и сохраняемых на внешнем носителе;
- целостность и аутентификацию данных, загружаемых с карточек тахографа и сохраняемых на внешнем носителе.

1.1 Источники

При подготовке настоящего подраздела использовались следующие источники:

SHA-1 National Institute of Standards and Technology (NIST). *FIPS Publication 180-1 : Secure Hash Standard*. April 1995.

PKCS1 RSA Laboratories. *PKCS # 1 : RSA Encryption Standard*. Version 2.0. October 1998.

TDES National Institute of Standards and Technology (NIST). *FIPS Publication 46-3 : Data Encryption Standard*. Draft 1999.

TDES-OP ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998.

ISO/IEC 7816-4 Информационные технологии. Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 4. Межотраслевые команды обмена данными. Издание первое, 1995 год + Поправка 1, 1997 год.

ISO/IEC 7816-6 Информационные технологии. Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 6. Элементы межотраслевых данных для обмена информацией. Издание первое, 1996 год + Поправка 1, 1998 год.

ISO/IEC 7816-8 Информационные технологии. Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 8. Межотраслевые команды обеспечения защиты. Издание первое, 1999 год.

ISO/IEC 9796-2 Информационные технологии. Методы защиты. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы с использованием хеш-функции. Издание первое, 1997 год.

ISO/IEC 9798-3 Информационные технологии. Методы защиты. Механизмы аутентификации объектов. Часть 3. Аутентификация объектов посредством алгоритма шифрования с открытым ключом. Издание второе, 1998 год.

ISO 16844-3 Транспорт дорожный. Тахографические системы. Часть 3. Интерфейс датчика движения.

1.2 Условные обозначения и сокращенные термины

В настоящем подразделе используются следующие условные обозначения и сокращенные термины:

(K_a, K_b, K_c)	набор ключей, используемый в рамках алгоритма тройного шифрования данных;
CA	(CO) сертификационный орган;
CAR	указатель сертификационного органа;
CC	(KКС) криптографическая контрольная сумма;
CG	криптограмма;
CH	заголовок команды;
CHA	полномочия держателя сертификата;
CHR	указатель держателя сертификата;
D()	расшифровка с помощью DES;
DE	элемент данных;
DO	(ОД) объект данных;
d	закрытый ключ в криптосистеме RSA, закрытая экспонента;
e	открытый ключ в криптосистеме RSA, открытая экспонента;
E()	шифрование с помощью DES;
EQT	аппаратура;
Hash()	значение хеш-функции, результат хеширования;
Hash	хеш-функция;
KID	идентификатор ключа;
Km	ключ TDES: ключ верхнего уровня, определение которого содержится в ISO 16844-3;
Km_{VU}	ключ TDES, вводимый в бортовые устройства;
Km_{WC}	ключ TDES, вводимый в карточки мастерских;
m	репрезентативный параметр сообщения, целое число от 0 до $n-1$;

n	ключ криптосистемы RSA, модуль;
PB	заполняющие байты;
PI	байт индикации заполнения (используется в криптограммах для обеспечения конфиденциальности объектов данных);
PV	простое значение;
s	репрезентативный параметр подписи, целое число от 0 до $n-1$;
SSC	(СИС) счетчик исходящих сообщений;
SM	(КЗОС) криптозащищенный обмен сообщениями;
TCBC	режим сцепления криптоблоков при тройном шифровании данных;
TDEA	алгоритм тройного шифрования данных;
TLV	"метка-длина-значение";
VU	(БУ) бортовое устройство;
X.C	сертификат, выданный сертификационным органом пользователю X;
X.CA	сертификационный орган пользователя X;
X.CA.PK \circ 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 сертификационным 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 ее защиты от искажений при пользовательских операциях обмена данными между бортовыми устройствами и карточками тахографа и для обеспечения в необходимых случаях конфиденциальности данных, передаваемых между бортовым устройством и карточкой тахографа.

2.2 Криптографические алгоритмы

2.2.1 Алгоритм RSA

CSM_003 Алгоритм RSA полностью выражается следующими соотношениями:

$$\begin{aligned} X.SK[m] &= s = m^d \bmod n \\ X.PK[s] &= m = s^e \bmod n \end{aligned}$$

Более всестороннее описание функции RSA можно найти в источниках [PKCS1]. При вычислениях по методу RSA в качестве открытой экспоненты, e , выбирается целое число в пределах от 3 до $n-1$, удовлетворяющее условию $\text{gcd}(e, \text{lcm}(p-1, q-1)) = 1$.

2.2.2 Хеш-алгоритм

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 трех функциональных уровнях, которые образуют следующую иерархию:

- европейский уровень,
- уровень Договаривающихся сторон,
- аппаратный уровень.

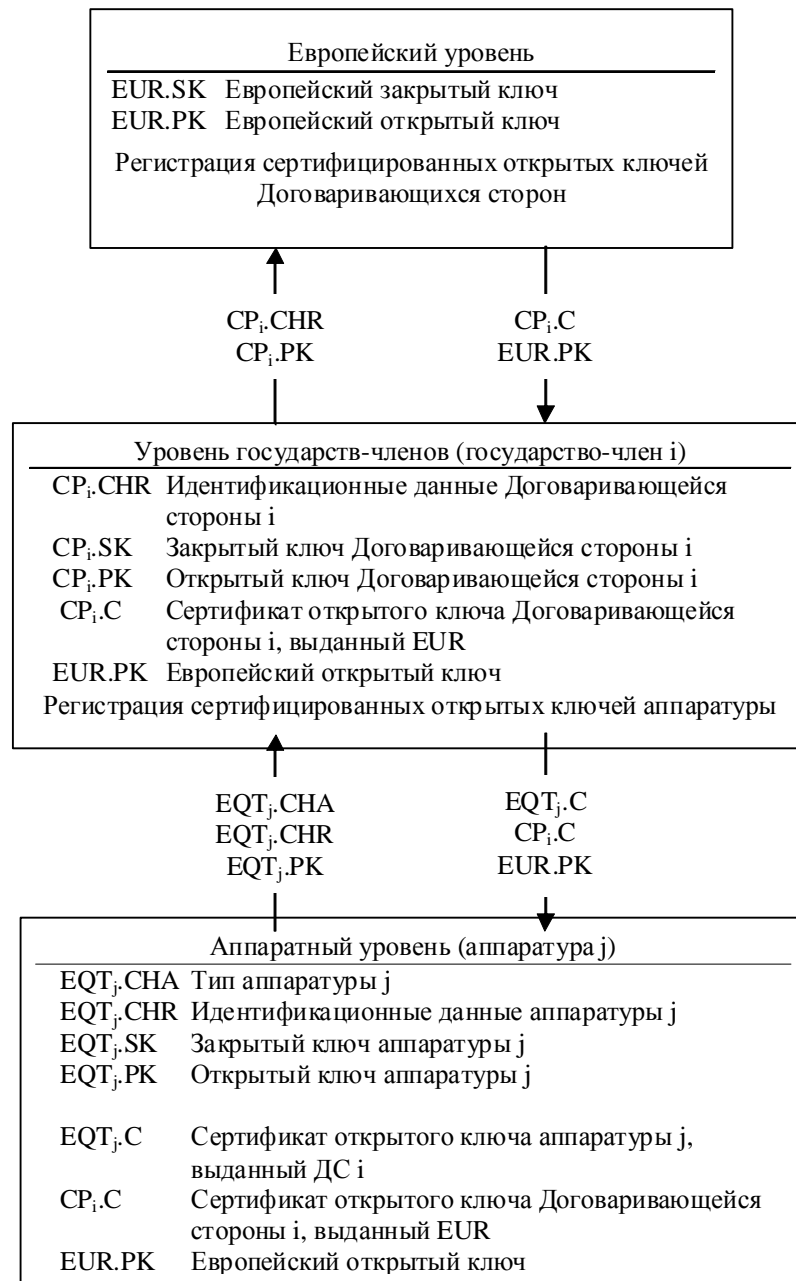
CSM_007 На европейском уровне генерируется единая пара общеевропейских ключей (EUR.SK и EUR.PK). Закрытый европейский ключ служит для сертификации открытых ключей Договаривающихся сторон. Все сертифицируемые ключи подлежат регистрации. Эти функции выполняет пользующийся международным признанием европейский сертификационный орган.

CSM_008 На уровне Договаривающихся сторон генерируется по паре ключей (CP.SK и CP.PK) для каждой Договаривающейся стороны. Открытые ключи Договаривающихся сторон сертифицируются европейским сертификационным органом. Закрытый ключ Договаривающейся стороны используется для сертификации открытых ключей, вводимых в соответствующие аппаратные средства (бортовые устройства и карточки тахографа). Все сертифицируемые открытые ключи подлежат регистрации с указанием аппаратуры, для которой они предназначены. Эти функции выполняет сертификационный орган Договаривающейся стороны. Договаривающаяся сторона может регулярно изменять свою пару ключей.

CSM_009 На аппаратном уровне генерируется единая пара ключей (EQT.SK и EQT.PK), вводимых в каждое устройство. Открытый ключ аппаратного уровня сертифицируется сертификационным органом Договаривающейся стороны. Эти функции могут выполняться изготовителями аппаратуры, предприятиями, персонализирующими аппаратуру, или соответствующими органами Договаривающихся сторон. Данная пара ключей служит для аутентификации, создания цифровых подписей и шифрования данных.

CSM_010 При генерации, транспортировке (если она необходима) и хранении закрытых ключей должен соблюдаться 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 пару общеевропейских испытательных ключей и не менее двух пар испытательных ключей для Договаривающихся сторон, открытые ключи которых сертифицируются закрытым испытательным ключом общеевропейского уровня. При испытаниях, проводимых с целью официального утверждения типовых образцов, в испытываемую аппаратуру изготовителями вводятся испытательные ключи, сертифицированные одним из вышеупомянутых испытательных ключей Договаривающихся сторон.

3.1.3 Ключи датчиков движения

При генерации, транспортировке (если она необходима) и хранении трех ключей TDES, о которых говорится ниже, должен соблюдаться надлежащий режим конфиденциальности.

В целях обеспечения совместимости с контрольными устройствами, соответствующими стандарту ISO 16844, европейский сертификационный орган и сертификационные органы Договаривающихся сторон 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 Договаривающихся сторон европейский сертификационный орган высылает им эти ключи с соблюдением надлежащих процедур защиты.

CSM_037 Сертификационные органы Договаривающихся сторон:

- используют ключ K_m для шифрования показаний датчиков движения в соответствии с указаниями изготовителей этих датчиков (определение данных, подлежащих шифрованию ключом K_m , дается в стандарте ISO 16844-3);
- с соблюдением надлежащих процедур защиты высылают $K_{m_{VU}}$ заводам-изготовителям бортовых устройств для ввода в эти устройства;

- обеспечивают ввод KmWC во все карточки мастерских (запись SensorInstallationSecData в элементарном файле Sensor_Installation_Data) при персонализации карточек.

3.1.4 Генерация и рассылка сеансовых ключей T-DES

CSM_012 Бортовые устройства и карточки тахографа в рамках процесса взаимной аутентификации генерируют необходимые данные и обмениваются ими в целях составления единого сеансового ключа для тройного шифрования по системе DES. Для сохранения конфиденциальности этого обмена данными используется криптографическая защита RSA.

CSM_013 Составленный ключ используется при всех последующих операциях криптозащищенного обмена сообщениями. Он перестает действовать по окончании текущего сеанса (извлечение или перезагрузка карточки) и/или после 240-го использования (однократное использование ключа = передача на карточку одного криптозащищенного сообщения-команды и получение соответствующего ответа).

3.2 Ключи

CSM_014 Ключи RSA (независимо от уровня) имеют следующую длину: модуль n - 1024 бита, открытая экспонента e - до 64 бит, закрытая экспонента d - 1024 бита.

CSM_015 Ключи DES для тройного шифрования имеют вид (K_a, K_b, K_a) , где K_a и K_b - независимые ключи длиной 64 бита. Биты контроля по четности не задаются.

3.3 Сертификаты

CSM_016 Сертификаты открытых ключей RSA должны быть "не содержащими самоописания" сертификатами с возможностью "проверки по карточке" (см. ISO/IEC 7816-8).

3.3.1 Содержание сертификатов

CSM_017 Сертификаты открытых ключей RSA состояются из следующих данных в следующем порядке:

Данные	Формат	Байты	Пояснение
CPI	ЦЕЛОЕ ЧИСЛО	1	Идентификатор профиля сертификата (в данной версии – "01")
SAR	ОКТЕТНАЯ СТРОКА	8	Указатель сертификационного органа
SNA	ОКТЕТНАЯ СТРОКА	7	Полномочия владельца сертификата
EOV	TimeReal	4	Дата истечения срока действия сертификата. Может не указываться; в этом случае поле заполняется байтами "FF".
CHR	ОКТЕТНАЯ СТРОКА	8	Указатель держателя сертификата
<i>n</i>	ОКТЕТНАЯ СТРОКА	128	Открытый ключ (модуль)
<i>e</i>	ОКТЕТНАЯ СТРОКА В	8	Открытый ключ (открытая экспонента)
		164	

Примечания:

1. "Идентификатор профиля сертификата" (CPI) определяет конкретную структуру сертификата, используемого в целях аутентификации. Он может применяться аппаратурой в качестве внутреннего идентификатора для вызова соответствующего списка заголовков, заключающего в себе описание конкатенации (последовательности) элементов данных, из которых состоит сертификат.

Такой список заголовков, отражающий содержание сертификата, выглядит следующим образом:

'4D'	'16'	'5F 29'	'01 '	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Расширенная метка списка заголовков	Длина списка заголовков	Метка CPI	Длина CPI	Метка CAR	Длина CAR	Метка CHA	Длина CHA	Метка EOY	Длина EOY	Метка CHR	Длина CHR	Метка открытого ключа (генерируется)	Длина последующих объектов данных	Метка модуля	Длина модуля	Метка открытой экспоненты	Длина открытой экспоненты

2. "Указатель сертификационного органа" (CAR) служит для обозначения сертификационного органа, выдавшего сертификат; таким образом, этот элемент данных может использоваться одновременно с идентификатором ключа сертификационного органа для указания на принадлежащий данному органу открытый ключ (информацию о соответствующих кодах см. ниже, в пункте, посвященном идентификаторам ключей).
3. "Полномочия держателя сертификата" (CHA) – указание на объем прав, предоставляемых сертификатом. Оно включает идентификатор приложения тахографа и тип аппаратуры, для которой предназначен сертификат (соответствует элементу данных EquipmentType; для Договаривающейся стороны используется значение "00").
4. "Указатель держателя сертификата" (CHR) предназначен для однозначной идентификации держателя данного сертификата; таким образом, этот элемент данных может использоваться одновременно с идентификатором ключа субъекта для указания на принадлежащий держателю сертификата открытый ключ.
5. Идентификаторы ключей позволяют однозначно идентифицировать держателя сертификата или сертификационный орган. Они кодируются следующим образом:

5.1 Аппаратура (БУ или карточка):

Данные	Серийный номер аппаратуры	Дата	Тип	Изготовитель
Длина	4 байта	2 байта	1 байт	1 байт
Значение	Целое число	мм гг VCD-код	Определяется изготовителем	Код изготовителя

Когда речь идет о бортовом устройстве, его изготовитель, запрашивая сертификаты, не обязательно должен знать идентификационные данные аппаратуры, в которую будут вводиться соответствующие ключи.

Если эти идентификационные данные изготовителю известны, то он направляет их вместе с открытым ключом на сертификацию в сертификационный орган своей Договаривающейся стороны. Выданный в результате сертификат будет содержать идентификационные данные аппаратуры, и изготовителю 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 аппаратуры изготовителю не известны, то он должен снабдить каждую заявку на сертификат индивидуальным обозначением и сообщить это обозначение вместе с открытым ключом сертификационному органу своей Договаривающейся стороны на предмет сертификации. В выданном сертификате будет указано индивидуальное обозначение заявки. После ввода ключа в аппаратуру изготовитель должен информировать сертификационный орган своей Договаривающейся стороны 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	Изготовитель
Длина	4 байта	2 байта	1 байт	1 байт
Значение	Целое число	мм гг VCD-код	'FF'	Код изготовителя

5.2 Сертификационный орган:

Данные	Идентификационные данные органа	Серийный номер ключа	Дополнительная информация	Идентификатор
Длина	4 байта	1 байт	2 байта	1 байт
Значение	1-байтовый числовой код страны 3-байтовый буквенно-числовой код страны	Целое число	Дополнительный код (определяется серт. органом). Если не указан – "FF FF"	"01"

Серийный номер ключа позволяет отличать друг от друга различные ключи Договаривающейся стороны в случае смены ею своего ключа.

6. Сторона, проверяющая сертификат, должна по косвенным признакам распознавать 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 приложения A.4) и сопровождаемую "указателем сертификационного органа".

$$X.C = X.CA.SK['6A' \parallel C_r \parallel Hash(Cc) \parallel 'BC'] \parallel C_n \parallel X.CAR$$

При содержании сертификата

$$= Cc = \quad C_r \quad \parallel \quad C_n$$

106 байт 58 байт

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, должна по косвенным признакам определить алгоритм, использованный сертификационным органом для подписания сертификата.

4. Данному сертификату соответствует следующий список заголовков:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Метка сертификата CV (генерируется)	Длина последующих объектов данных	Метка подписи	Длина подписи	Метка остатка	Длина остатка	Метка CAR	Длина CAR

3.3.3 Проверка и расшифровка сертификатов

Процесс проверки и расшифровки сертификатов заключается в проверке подписи согласно стандарту ISO/IEC 9796-2, извлечении содержания сертификата, получении из него соответствующего открытого ключа ($X.PK = X.CA.PK \circ X.C$) и подтверждении действительности сертификата.

CSM_019 Этот процесс состоит из следующих этапов:

Проверка подписи и извлечение содержания:

- из $X.C$ извлекаются $Sign$, C_n' и CAR' :

$$X.C = \begin{array}{c} Sign \\ 128 \text{ байт} \end{array} \parallel \begin{array}{c} C_n' \\ 58 \text{ байт} \end{array} \parallel \begin{array}{c} CAR' \\ 8 \text{ байт} \end{array}$$

- из указателя CAR' выбирается открытый ключ соответствующего сертификационного органа (если он не выбран до этого иным способом);
- с помощью открытого ключа сертификационного органа расшифровывается содержание $Sign$: $Sr' = X.CA.PK [Sign]$;
- проверяется Sr' (начальными символами должны быть "6A", конечными – "BC");
- вычисляются C_r' и H' по формуле:

$$S_r' = \begin{array}{c} '6A' \\ 106 \text{ байт} \end{array} \parallel \begin{array}{c} C_r' \\ 20 \text{ байт} \end{array} \parallel \begin{array}{c} H' \\ 20 \text{ байт} \end{array} \parallel \begin{array}{c} 'BC' \end{array}$$

- извлекается 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:

- если применимо, проверяется дата истечения срока действия сертификата, извлекаемая из С'.

Извлечение из С' и сохранение открытого ключа, идентификатора ключа, полномочий держателя сертификата и даты истечения срока его действия:

- X.PK = $n || e$
- X.KID = CHR
- X.CHA = CHA
- X.EOV = EOV

4. Механизм взаимной аутентификации

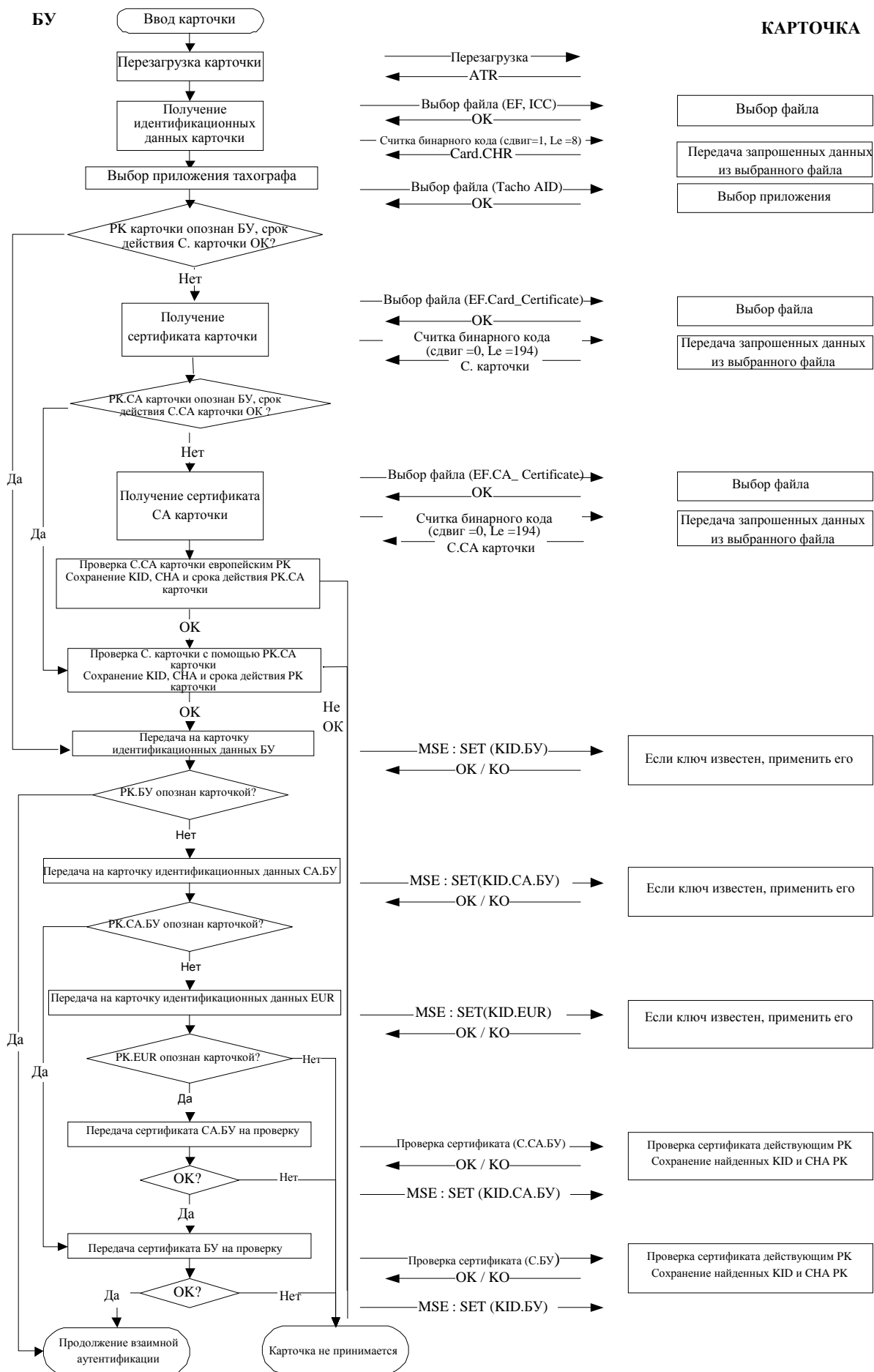
В основу механизма взаимной аутентификации карточек и БУ положен следующий принцип:

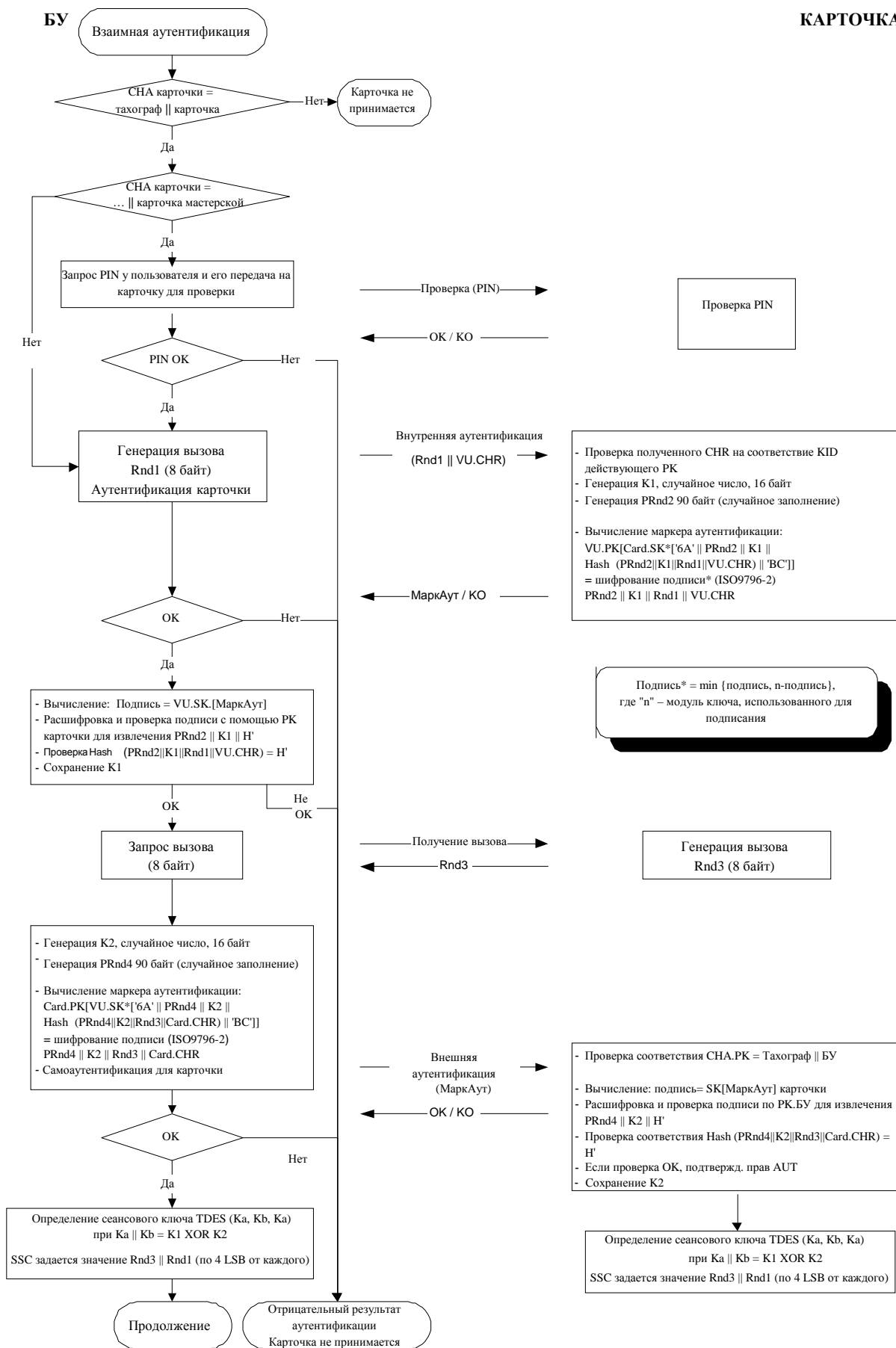
Каждая сторона должна доказать другой наличие у нее действительной пары ключей, открытый ключ которой сертифицирован сертификационным органом Договаривающейся стороны, имеющим в свою очередь сертификат, выданный европейским сертификационным органом.

Доказательством служит подписание закрытым ключом случайной последовательности цифр, полученной от другой стороны, которая при проверке подписи должна восстановить из нее ту же последовательность цифр.

Данный механизм запускается со стороны БУ при вводе карточки в считывающее устройство. 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. подраздел II)):





5. Механизмы обеспечения конфиденциальности, целостности и аутентификации данных при их передаче между БУ и карточками

5.1 Криптозащищенный обмен сообщениями

CSM_021 Неискаженность 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 высылаемым 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, высылаемых в виде команды, учитываются заголовок команды и все содержащиеся в ней объекты данных (\Rightarrow CLA = '0C', причем все эти объекты данных при их формировании снабжаются метками, 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 криптозащищенном обмене сообщениями команды и ответы имеют структуру, показанную ниже.

Используемые здесь объекты данных представляют собой часть набора ОД для криптозащищенного обмена сообщениями, описание которого приводится в ISO/IEC 7816-4:

Метка	Мнемокод	Значение
'81'	T _{PV}	Простое значение: данные без кодировки BER-TLV (защищаются с помощью ККС)
'97'	T _{LE}	Значение L _e в незащищенной команде (защищается с помощью ККС)
'99'	T _{SW}	Информация о состоянии (защищается с помощью ККС)
'8E'	T _{CC}	Криптографическая контрольная сумма
'87'	T _{PCG}	Байт индикации заполнения Криптограмма (Простое значение без кодировки BER-TLV)

Если незащищенная пара "команда-ответ" выглядит следующим образом:

Заголовок команды	Текст команды
CLA INS P1 P2	[поле L _c] [Поле данных] [поле L _e]
четыре байта	L байт, обозначаемые как байты от B ₁ до B _L

Текст ответа	Концевая метка ответа
[Поле данных]	SW1 SW2
L _r байт данных	два байта

то соответствующая ей криптозащищенная пара "команда-ответ" имеет следующий вид:

Криптозащищенная команда:

Заголовок команды (CH)	Текст команды										
CLA INS P1 P2	[Новое поле L _c]	[Новое поле данных]									[Новое поле L _e]
'0C'	Длина нового поля данных	T _{PV}	L _{PV}	PV	T _{LE}	L _{LE}	L _e	T _{CC}	L _{CC}	CC	'00'
		'81'	L _c	Поле данных	'97'	'01'	L _e	'8E'	'04'	CC	

Данные, учитываемые в контрольной сумме = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB, где

PB = заполняющие байты (80 .. 00) согласно стандартам ISO-IEC 7816-4 и ISO 9797 (метод 2).

Объекты данных PV и LE присутствуют лишь в случаях, когда незащищенная команда содержит соответствующие данные.

Криптозащищенный ответ:

1. Если поле данных ответа не является пустым, но не нуждается в защите конфиденциальности:

Текст ответа						Концевая метка ответа
[Новое поле данных]						Новые SW1 SW2
T _{PV}	L _{PV}	PV	T _{CC}	L _{CC}	CC	
'81'	L _r	Поле данных	'8E'	'04'	CC	

Данные, учитываемые в контрольной сумме = T_{PV} || L_{PV} || PV || PB

2. Если поле данных ответа не является пустым и нуждается в защите конфиденциальности:

Текст ответа						Концевая метка ответа
[Новое поле данных]						Новые SW1 SW2
T _{PI CG}	L _{PI CG}	PI CG	T _{CC}	L _{CC}	CC	
'87'		PI CG	'8E'	'04'	CC	

Информация, передаваемая в виде криптограммы: данные без кодировки BER-TLV и заполняющие байты.

Данные, учитываемые в контрольной сумме = T_{PI CG} || L_{PI CG} || PI CG || PB

3. Если поле данных ответа оставлено пустым:

Текст ответа						Концевая метка ответа
[Новое поле данных]						Новые SW1 SW2
T _{SW}	L _{SW}	SW	T _{CC}	L _{CC}	CC	
'99'	'02'	Новые SW1 SW2	'8E'	'04'	CC	

Данные, учитываемые в контрольной сумме = T_{SW} || L_{SW} || SW || PB

5.2 Обработка ошибок при криптозащищенном обмене сообщениями

CSM_026 Когда карточка тахографа обнаруживает ошибку КЗОС при расшифровке команды, она возвращает соответствующие байты состояния, не используя КЗОС. В соответствии со стандартом ISO/IEC 7816-4 для указания на ошибки КЗОС предусматриваются следующие байты состояния:

'66 88': несоответствие криптографической контрольной суммы;

'69 87': отсутствие ожидаемых объектов данных КЗОС;

'69 88': неверные объекты данных КЗОС.

CSM_027 Если карточкой тахографа возвращены байты состояния без ОД КЗОС или с неверным ОД КЗОС, то БУ должно прервать сеанс обмена данными.

5.3 Алгоритм расчета криптографических контрольных сумм

CSM_028 Криптографические контрольные суммы вычисляются на основе алгоритма аутентификации сообщений retail-MAC в соответствии с ANSI X9.19 и системой DES:

- начальный этап: в качестве первого контрольного блока у₀ используется E(K_a, SSC);
- последующие этапы: на основе K_a рассчитываются контрольные блоки у₁, .. , у_n;

- заключительный этап: по последнему контрольному блоку u_n рассчитывается криптографическая контрольная сумма: $E(K_a, D(K_b, u_n))$,

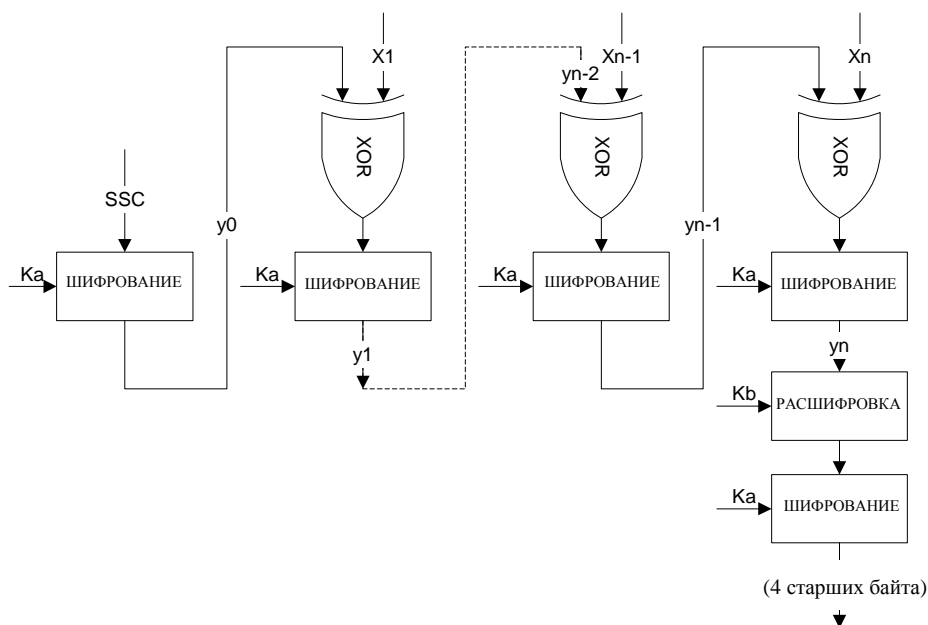
где $E()$ означает шифрование по системе DES, а $D()$ – расшифровка по системе DES.

Передаче подлежат четыре старших байта криптографической контрольной суммы.

CSM_029 В ходе процедуры согласования ключей счетчику исходящих сообщений (SSC) задаются следующие начальные значения: Initial SSC: Rnd3 (4 младших байта) || Rnd1 (4 младших байта).

CSM_030 Счетчик исходящих сообщений увеличивается на 1 единицу перед каждым вычислением MAC (кода аутентификации сообщения) (т.е. для первой команды значение SSC составляет Initial SSC + 1, а для первого ответа – Initial SSC + 2).

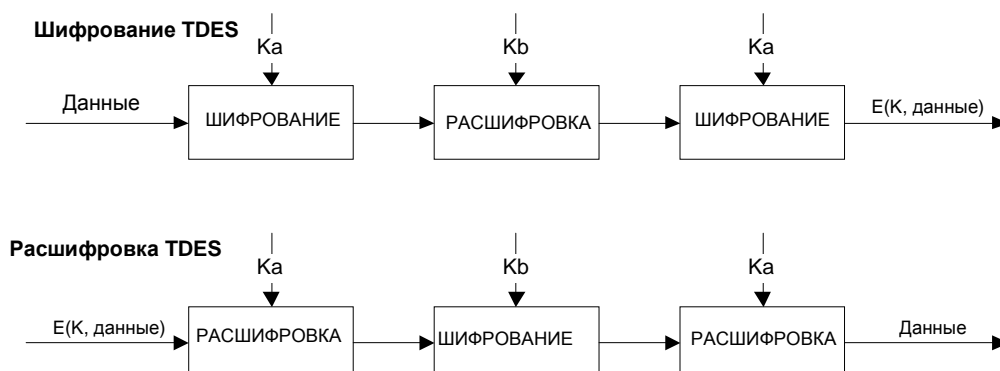
Способ вычисления retail-MAC изображен на диаграмме ниже.



5.4 Алгоритм расчета 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], причем в качестве блока начальной величины используется нуль-вектор.

Применение ключей TDES показано на следующей диаграмме.



6. Механизмы цифровой подписи при загрузке данных

CSM_032 Данные, полученные из того или иного аппаратного источника (БУ или карточки) за один сеанс загрузки, сохраняются специализированной программируемой аппаратурой (СПА) в виде одного физического файла данных. Этот файл должен заключать в себе сертификаты CP_i.C и EQT.C. Файл содержит цифровые подписи блоков данных в соответствии с указанным в подразделе VII (Протоколы загрузки данных).

CSM_033 Цифровые подписи загружаемых данных создаются по схеме, предполагающей добавление информации, которая позволяет при желании производить считку загруженных данных в нерасшифрованном виде.

6.1 Генерация подписей

CSM_034 Подписи данных генерируются аппаратурой согласно схеме подписи с соответствующим добавлением, которая определена в цитируемом источнике [PKCS1], при помощи хеш-функции SHA-1:

$$\text{Подпись} = \text{EQT.SK}[\text{'00'} \parallel \text{'01'} \parallel PS \parallel \text{'00'} \parallel \text{DER}(\text{SHA-1}(\text{данные}))]$$

PS = Заполняющая октетная строка со значением 'FF', до общей длины 128.

$\text{DER}(\text{SHA-1}(M))$ – кодированное представление идентификатора алгоритма хеш-функции и значения хеш-функции в виде величины стандарта ASN.1 типа DigestInfo (правила однозначного шифрования):

‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’||‘05’||‘00’||‘04’||‘14’||значение хеш-функции.

6.2 Проверка подписей

CSM_035 Проверка подписей загружаемых данных производится согласно схеме подписи с соответствующим добавлением, которая определена в цитируемом источнике [PKCS1], при помощи хеш-функции SHA-1.

Проверяющей стороне должен быть известен европейский открытый ключ EUR.PK, который она должна получить из независимого (и пользующегося доверием) источника.

В нижеследующей таблице представлен протокол, в соответствии с которым СПА после ввода в нее карточки контролера может проверять целостность загруженных данных, сохраненных на ВН (внешнем носителе). Для расшифровки цифровых подписей используется карточка контролера. В этом случае данная функция не обязательно должна быть предусмотрена в СПА.

Аппаратура, с помощью которой были загружены и подписаны подлежащие анализу данные, обозначена буквами EQT.

