

Distr.: General
25 April 2017

Original: Russian only

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Рабочая группа по автомобильному транспорту

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

Пятнадцатая сессия

Женева, 12 июня 2017 года

Данный документ, представленный Европейской Комиссией, содержит добавление 7 к приложению IC к регламенту (ЕС) 2016/799.

RU

ПРИЛОЖЕНИЕ 7. ПРОТОКОЛЫ ЗАГРУЗКИ ДАННЫХ

СОДЕРЖАНИЕ

1. Введение	4
1.1. Область применения	4
1.2. Сокращения и обозначения	4
2. Загрузка данных из БУ	5
2.1. Процедура загрузки	5
2.2. Протокол загрузки данных	5
2.2.1 Структура сообщения	5
2.2.2 Типы сообщений	7
2.2.2.1 Запрос инициализации обмена данными (SID 81)	8
2.2.2.2 Положительный ответ: начало обмена данными (SID C1)	8
2.2.2.3 Запрос инициализ. диагност. сеанса (SID 10)	8
2.2.2.4 Положительный ответ: начало диагностики (SID 50)	8
2.2.2.5 Функция управления передачей данных (SID 87)	8
2.2.2.6 Положительный ответ: функция управления передачей данных (SID C7)	8
2.2.2.7 Запрос загрузки (SID 35)	8
2.2.2.8 Положительный ответ: запрос загрузки (SID 75)	8
2.2.2.9 Запрос передачи данных (SID 36)	8
2.2.2.10 Положительный ответ: передача данных (SID 76)	9
2.2.2.11 Запрос завершения передачи (SID 37)	9
2.2.2.12 Положит. ответ: запрос на завершение передачи (SID 77)	9
2.2.2.13 Запрос завершения обмена данными (SID 82)	9
2.2.2.14 Положительный ответ: конец обмена данными (SID C2)	9
2.2.2.15 Подтверждение приёма подсообщения (SID 83)	9
2.2.2.16 Отрицательный ответ (SID 7F)	9
2.2.3 Поток сообщений	10
2.2.4 Время	11
2.2.5 Обработка ошибок	11
2.2.5.1 Этап инициализации обмена данными	11
2.2.5.2 Этап обмена данными	12
2.2.6 Содержание ответного сообщения	15
2.2.6.1 Положительный ответ: передача обзорных данных	15
2.2.6.2 Положительный ответ: передача данных о действиях	17
2.2.6.3 Положительный ответ на запрос передачи данных о событиях и неисправностях	19
2.2.6.4 Положительный ответ: передача подробных данных о скорости	21
2.2.6.5 Положительный ответ: передача технических данных	22
2.3. Хранение файлов на ВН	23
3. Протокол загрузки данных с карточек тахографа	24
3.1. Область применения	24
3.2. Определения	24
3.3. Загрузка данных карточки	24
3.3.1 Процедура инициализации	24
3.3.2 Процедура для неподписанных файлов данных	25
3.3.3 Процедура для подписанных файлов данных	25
3.3.4 Процедура обнуления счётчика калибровок	26
3.4. Формат хранения данных	27
3.4.1 Введение	27
3.4.2 Формат файла	27
4. Загрузка данных с карточки тахографа через бортовое устройство	28

1. Введение

В настоящем приложении изложены процедуры различных вариантов загрузки данных на внешний носитель (ВН), а также протоколы, применение которых необходимо для правильной передачи данных и для обеспечения универсальной совместимости формата, в котором они загружаются, с тем чтобы любой контролёр имел возможность ознакомиться с этими данными и перед началом их анализа убедиться в их подлинности и целостности.

1.1. Область применения

На ВН могут загружаться данные:

- из бортового устройства при помощи подключённой к БУ специализированной программируемой аппаратуры (СПА),
- с карточки тахографа при помощи СПА, оснащённой устройством считывания карточек (IFD),
- с карточки тахографа через бортовое устройство путем подключения СПА к БУ.

Для целей контроля подлинности и целостности данных, сохраняемых на ВН, при загрузке они снабжаются подписью в соответствии с приложением 11 «Общие механизмы защиты». В состав загружаемой информации включаются идентификационные данные аппаратного источника (БУ или карточки) и соответствующие ему сертификаты безопасности (государства-члена и аппаратуры). Лицо, осуществляющее проверку данных, должно иметь собственный открытый криптографический ключ от надежного европейского поставщика.

DDP_001 Данные, загруженные за один сеанс загрузки, должны сохраняться на ВН в виде одного файла.

1.2. Сокращения и обозначения

В настоящем приложении используются следующие сокращения:

AID	Идентификатор приложения
ATR	Отклик на сигнал сброса
CS	Байт контрольной суммы
DF	Выделенный файл.
DS_	Диагностический сеанс
EF	Элементарный файл
ESM (ВН)	Внешний носитель
FID	Идентификатор файла (ИД файла)
FMT	Байт формата (первый байт в заголовке сообщения)
ICC	Карточка с интегральной схемой
IDE (СПА)	Специализированная программируемая аппаратура: аппаратура, используемая для загрузки данных на ВН (например, персональный компьютер)
IFD	Устройство интерфейса
KWP	Ключевой протокол 2000
LEN	Байт длины (последний байт в заголовке сообщения)
PPS	Выбор параметра протокола
PSO	Выполнение операции обеспечения безопасности
SID	Идентификатор функции
SRC	Байт адреса источника
TGT	Байт адреса приёмника
TLV	Значение длины метки
TREP	Ответный параметр передачи данных
TRTP	Параметр запроса передачи данных
VU (БУ)	Бортовое устройство

2. Загрузка данных из БУ

2.1. Процедура загрузки

Для загрузки данных из БУ оператору необходимо выполнить следующие действия:

- Ввести свою карточку тахографа в считывающее устройство БУ(*);
- Подсоединить СПА к выходному разъёму БУ;
- Установить канал связи между СПА и БУ;
- С помощью СПА выбрать данные для загрузки и передать запрос в БУ;
- Завершить сеанс загрузки.

(*) Ввод карточки инициирует подтверждение соответствующих прав доступа к функции загрузки и загружаемым данным. Однако данные также можно загружать с карточки водителя, введённой в одно из считывающих устройств БУ, если в другое считывающее устройство не вставлена никакая карточка другого типа.

2.2. Протокол загрузки данных

Протокол построен по принципу «ведущий-ведомый», при котором в роли ведущего выступает СПА, а в роли ведомого – БУ.

Структура сообщений, их типы и потоки, как правило, основываются на ключевом протоколе 2000 (KWP) (ISO 14230-2 Дорожные транспортные средства. Диагностические системы. Ключевой протокол 2000. Часть 2: Уровень канала передачи данных).

Уровень приложения, в принципе, опирается на действительную редакцию стандарта ISO 14229-1 (Дорожные транспортные средства. Диагностические системы. Часть 1: услуги диагностики, версия 6 от 22 февраля 2001 г.).

2.2.1 Структура сообщения

DDP_002 Все сообщения, которыми обмениваются СПА и БУ, форматируются в соответствии с трёхкомпонентной структурой:

- Заголовок, состоящий из байта формата (FMT), байта адреса приёмника (TGT), байта адреса источника (SRC) и в некоторых случаях также байта длины сообщения (LEN),
- Поле данных, образуемое байтом идентификатора функции (SID) и переменным числом байтов данных, включая необязательный байт диагностического сеанса (DS_) или необязательный байт параметра передачи (TRTP или TREP),
- Контрольная сумма, определяемая байтом контрольной суммы (CS).

Заголовок				Поле данных				Контрольн ая сумма	
FMT	TGT	SRC	LEN	SID	DATA	CS
4 байта				Макс. 255 байтов				1 байт	

Байты TGT и SRC указывают физические адреса получателя и отправителя сообщения. Их значения – F0 Hex для СПА и EE Hex для БУ.

Байт LEN представляет собой длину поля данных в сообщении.

Байт контрольной суммы представляет собой 8-битную сумму по модулю 256 всех байтов сообщения, за исключением самой контрольной суммы.

Определения байтов FMT, SID, DS_, TRTP и TREP приводятся далее в настоящем документе.

DDP_003 Если объём передаваемых в сообщении данных превышает длину поля данных, сообщение фактически высылается в виде нескольких подсообщений. Каждое подсообщение содержит заголовок, одни и те же байты SID и TREP, а также 2-байтовый счётчик подсообщений, указывающий порядковый номер данного подсообщения в общем сообщении. Чтобы обеспечить возможность обнаружения ошибок и отмены передачи, СПА подтверждает получение каждого подсообщения. СПА может принять подсообщение, запросить его повторную передачу, выдать БУ команду начать передачу заново или отменить её.

DDP_004 Если поле данных последнего подсообщения содержит ровно 255 байтов, к нему должно добавляться заключительное подсообщение с пустым (то есть содержащим только SID, TREP и счётчик подсообщений) полем данных, означающее конец сообщения.

Пример:

Заголово к	SID	TREP	Сообщение			CS
4 байта	Более 255 байтов					

Передаётся как:

Заголово к	SID	TREP	00	01	Подсообщение 1	CS
4 байта	255 байтов					

Заголово к	SID	TREP	00	02	Подсообщение 2	CS
4 байта	255 байтов					

...

Заголово к	SID	TREP	xx	yy	Подсообщение n	CS
4 байта	Менее 255 байтов					

или как:

Заголово к	SID	TREP	00	01	Подсообщение 1	CS
4 байта	255 байтов					

Заголово к	SID	TREP	00	02	Подсообщение 2	CS
4 байта	255 байтов					

...

Заголово к	SID	TREP	xx	yy	Подсообщение n	CS
4 байта	255 байтов					

Заголово к	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	Макс. 4 байта Заголовок				Макс. 255 байтов Данные			1 байт Контрольн ая сумма
	FMT	TGT	SRC	LEN	SID	DS_ TRTP	DATA	CS
СПА ->	<- БУ							
Запрос инициализации обмена данными	81	EE	F0		81			E0
Положительный ответ: начало обмена данными	80	F0	EE	03	C1		EA, 8F	9B
Запрос инициализ. диагност. сеанса	80	EE	F0	02	10	81		F1
Положительный ответ: начало диагностики	80	F0	EE	02	50	81		31
Функция управления передачей данных								
Проверка скорости передачи данных бодами (этап 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Положит. ответ: проверка скорости передачи бодами	80	F0	EE	02	C7		01	28
Скорость передачи данных бодами (этап 2)	80	EE	F0	03	87		02,03	ED
Запрос загрузки	80	EE	F0	0A	35		00,00,00,00, 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
Действия	80	EE	F0	06	36	02	Дата	CS
События и неисправности	80	EE	F0	02	36	03		99
Данные о скорости	80	EE	F0	02	36	04		9A
Технические данные	80	EE	F0	02	36	05		9B
Загрузка данных карточки	80	EE	F0	02	36	06	Считываю щее устройство	CS
Положит. ответ: передача данных	80	F0	EE	Len	76	TREP	Данные	CS
Запрос завершения передачи	80	EE	F0	01	37			96
Положит. ответ: запрос на завершение передачи	80	F0	EE	01	77			D6
Запрос прекращения обмена данными	80	EE	F0	01	82			E1
Положительный ответ: конец обмена данными	80	F0	EE	01	C2			21
Подтверждение приёма подсообщения	80	EE	F0	Len	83		Данные	CS
Отрицательные ответы								
Общее отклонение запроса	80	F0	EE	03	7F	Sid Req	10	CS
Услуга не поддерживается	80	F0	EE	03	7F	Sid Req	11	CS
Подфункция не поддерживается	80	F0	EE	03	7F	Sid Req	12	CS
Неверная длина сообщения	80	F0	EE	03	7F	Sid Req	13	CS
Недопустимые условия или ошибка очередн.	80	F0	EE	03	7F	Sid Req	22	CS
Нештатный запрос	80	F0	EE	03	7F	Sid Req	31	CS
Отказ в приёме загружаемых данных	80	F0	EE	03	7F	Sid Req	50	CS
Ожидается ответ	80	F0	EE	03	7F	Sid Req	78	CS
Данных нет	80	F0	EE	03	7F	Sid Req	FA	CS

Примечания:

- Sid Req = Sid соответствующего запроса.
- TREP = TRTP соответствующего запроса.
- Тёмный фон ячейки в таблице означает отсутствие передачи данных.
- Термин «upload» (загрузка со стороны СПА) используется для целей совместимости с ISO 14229. Он имеет тот же смысл, что и термин «download» (загрузка со стороны БУ).
- 2-байтные счётчики подсообщений, которые могут содержаться в сообщениях, в таблице не показаны.
- Считывающее устройство – это номер считывающего устройства: 1 (для карточки водителя) или 2 (для карточки второго водителя)
- Если номер считывающего устройства не указан, БУ выбирает устройство № 1, если в него вставлена карточка, а устройство № 2 выбирается, только если его конкретно выбрал пользователь.
-

2.2.2.1 Запрос инициализации обмена данными (SID 81)

DDP_005 Данное сообщение высылается СПА для установления канала обмена данными с БУ. Начальная скорость передачи данных во всех случаях составляет 9600 бод (до тех пор, пока она не будет изменена при помощи соответствующих функций управления передачей данных).

2.2.2.2 Положительный ответ: начало обмена данными (SID C1)

DDP_006 Данное сообщение высылается БУ в качестве положительного ответа на запрос инициализации обмена данными. Оно включает в себя два байта ключей 'EA' и '8F', указывающие на поддержку данного протокола устройством, и заголовок с информацией о получателе, источнике и длине сообщения.

2.2.2.3 Запрос инициализ. диагност. сеанса (SID 10)

DDP_007 Сообщение с запросом инициализации диагностического сеанса высылается СПА, чтобы начать новый сеанс обмена диагностическими данными с БУ. Подфункция «default session» (81 Hex) указывает на то, что будет начат стандартный диагностический сеанс.

2.2.2.4 Положительный ответ: начало диагностики (SID 50)

DDP_008 Сообщение с положительным ответом на запрос инициализации диагностики высылает БУ, чтобы подтвердить начало диагностического сеанса.

2.2.2.5 Функция управления передачей данных (SID 87)

DDP_052 Функция управления передачей данных используется СПА для того, чтобы инициировать изменение скорости передачи данных бодами. Это происходит в два этапа. На первом этапе СПА предлагает изменение скорости передачи, указывая новую скорость. По получении от БУ положительного ответа СПА высылает БУ подтверждение изменения скорости (второй этап). Затем СПА переключается на новую скорость передачи данных. После получения подтверждения БУ изменяет скорость передачи данных в бодах на новую.

2.2.2.6 Положительный ответ: функция управления передачей данных (SID C7)

DDP_053 Положительный ответ о функции управления передачей данных высылается БУ в качестве положительного ответа на запрос регулировки канала обмена данными (первый этап). Следует обратить внимание на то, что ответ на запрос подтверждения не высылается (второй этап).

2.2.2.7 Запрос загрузки (SID 35)

DDP_009 Сообщение с запросом загрузки высылается СПА с целью указать БУ на необходимость загрузить данные. В соответствии с требованиями ISO 14229 в него должна включаться информация об адресе, объёме и формате запрашиваемых данных. Поскольку до загрузки данных СПА такой информацией не располагает, адрес ячейки памяти при этом устанавливается на 0, формат указывается как нешифрованный и без сжатия, а объём памяти задается максимальным.

2.2.2.8 Положительный ответ: запрос загрузки (SID 75)

DDP_010 Сообщение с положительным ответом на запрос загрузки высылается БУ с целью указать СПА на готовность БУ к загрузке данных. В соответствии с требованиями ISO 14229 в это сообщение включаются данные, указывающие СПА о том, что последующие положительные ответы на запросы передачи данных будут содержать максимум 00FF Hex байт.

2.2.2.9 Запрос передачи данных (SID 36)

DDP_011 Запрос передачи данных высылается СПА с целью указать БУ тип данных, которые должны быть загружены. Тип данных указывается однобайтовым параметром запроса передачи (TRTP).

Возможна передача шести типов данных:

- Обзор (TRTP 01),
- Деятельность на указанную дату (TRTP 02),
- События и неисправности (TRTP 03),
- Подробные данные о скоростном режиме (TRTP 04),
- Технические данные (TRTP 05),
- Загрузка данных с карточки (TRTP06).

DDP_054 В ходе сеанса загрузки СПА в обязательном порядке запрашивает передачу обзорных данных (TRTP 01), так как только при этом в загружаемом файле регистрируются сертификаты БУ (что создаёт возможность проверки цифровой подписи).

Во втором случае (TRTP 02) сообщение с запросом передачи данных включает в себя указание календарной даты (в формате TimeReal), данные за которую подлежат загрузке.

2.2.2.10 Положительный ответ: передача данных (SID 76)

DDP_012 Положительный ответ на запрос передачи данных высылается БУ по получении запроса передачи данных. Это сообщение содержит запрошенные данные и параметр ответа на запрос передачи (TREP), который соответствует TRTP запроса.

DDP055 В первом случае (TREP 01) БУ высылает данные, помогающие оператору СПА выбрать информацию, загрузку которой он желает продолжить. Сообщение содержит данные о:

- Сертификатах защиты,
- Идентификационных данных транспортного средства,
- Текущих дате и времени БУ,
- Самой ранней и самой поздней дате, данные за которую могут быть загружены из БУ,
- Наличии карточек в считывающих устройствах БУ,
- Предыдущей загрузке данных представителем предприятия,
- Блокировках, установленных предприятием,
- Предыдущих проверках.

2.2.2.11 Запрос завершения передачи (SID 37)

DDP_013 Сообщение о запросе завершения передачи высылается СПА с целью указать БУ на завершение сеанса загрузки.

2.2.2.12 Положит. ответ: запрос на завершение передачи (SID 77)

DDP_014 Положительный ответ на запрос завершения передачи данных высылается БУ в качестве подтверждения получения запроса завершения передачи.

2.2.2.13 Запрос завершения обмена данными (SID 82)

DDP_015 Данное сообщение высылается СПА для отключения канала обмена данными с БУ.

2.2.2.14 Положительный ответ: конец обмена данными (SID C2)

DDP_016 Положительный ответ на запрос завершения обмена данными высылается БУ в качестве подтверждения получения запроса завершения обмена данными.

2.2.2.15 Подтверждение приёма подсообщения (SID 83)

DDP_017 Подтверждение приёма подсообщения высылается СПА, подтверждая этим получение каждой части сообщения, передаваемого в виде ряда подсообщений. Поле данных содержит SID, полученный от БУ, и двухбайтовый код со следующими возможными значениями:

- MsgC +1 – подтверждение правильного приёма подсообщения номер MsgC.
Запрос от СПА к БУ на отправку следующего подсообщения
- MsgC – проблема приёма подсообщения номер MsgC.
Запрос от СПА к БУ на повторную отправку подсообщения.
- FFFF – запрос прекращения передачи сообщения.
Эта функция может использоваться СПА для прекращения по каким-либо причинам передачи сообщения от БУ.

Приём последнего подсообщения в сообщении (LEN < 255 байт) может подтверждаться любым из вышеуказанных кодов или оставаться без подтверждения.

К ответам БУ, которые состоят из нескольких подсообщений, относятся:

- Положительный ответ: передача данных (SID 76)

2.2.2.16 Отрицательный ответ (SID 7F)

DDP_018 Сообщение с отрицательным ответом на те или иные из перечисленных выше запросов БУ высылает в

тех случаях, когда запрос не может быть выполнен. Поле данных сообщения содержит SID ответа (7F), SID запроса и код, указывающий причину отрицательного ответа. Могут использоваться следующие коды:

- 10 Общее отклонение запроса
Действие не может быть выполнено по причине, не входящей в число нижеперечисленных.
- 11 Услуга не поддерживается
Не опознан SID запроса.
- 12 Подфункция не поддерживается
Не опознан DS_ или TRTP запроса либо отсутствуют другие подсообщения для передачи.
- 13 Неверная длина сообщения
Получено сообщение неверной длины.
- 22 Недопустимые условия или ошибка очередности
Требуемая функция не активирована либо неверная очередность запросов.
- 31 Нештатный запрос
Значение параметра запроса (поле данных) недействительно.
- 50 Отказ в приёме загружаемых данных
Невозможно выполнить запрос (несоответствие режима работы БУ или внутренние неполадки в БУ).
- 78 Ожидается ответ
Запрошенная операция не может быть завершена своевременно; БУ не готов к приему нового запроса.
- FA данных нет
Запрошенный к передаче объект данных отсутствует в БУ (например, не введена карточка, ...).

2.2.3 Поток сообщений

При нормальной загрузке данных поток сообщений, как правило, выглядит следующим образом:

СПА		БУ
Запрос инициализации обмена данными	⇒ ⇐	Положительный ответ
Запрос инициализации функции диагностики	⇒ ⇐	Положительный ответ
Запрос загрузки	⇒ ⇐	Положительный ответ
Обзор запроса передачи данных	⇒ ⇐	Положительный ответ
Запрос передачи данных № 2	⇒ ⇐	Положительный ответ № 1 Положительный ответ № 2 Положительный ответ № m Положительный ответ (поле данных <255 байт)
Подтверждение приёма подсообщения № 1	⇒	
Подтверждение приёма подсообщения № 2	⇒	
Подтверждение приёма подсообщения № m	⇒	
Подтверждение приёма подсообщения (факультативно)	⇒	
...		
Запрос передачи данных № n	⇒ ⇐	Положительный ответ
Запрос завершения передачи	⇒ ⇐	Положительный ответ
Запрос прекращения обмена данными	⇒ ⇐	Положительный ответ

2.2.4 Время

DDP_019 Временные параметры для нормального режима работы указаны в таблице ниже:

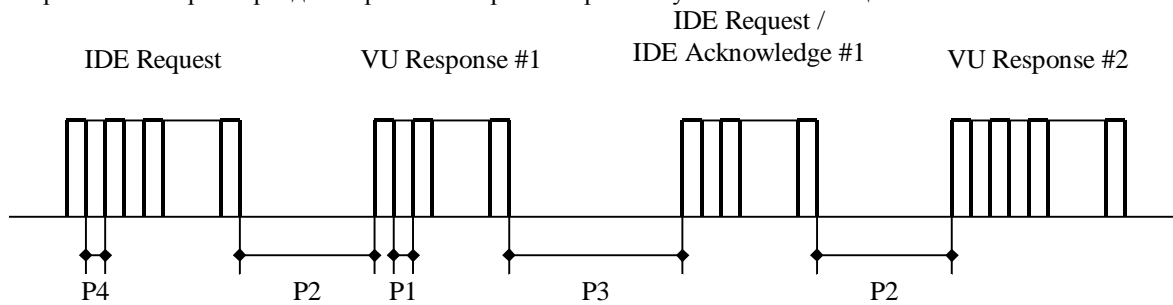


Рисунок 1 – Поток сообщений и временные параметры

Где:

P1 = Межбайтовый интервал для ответа БУ.

P2 = Время между окончанием запроса СПА и началом ответа БУ или между окончанием подтверждения СПА и началом следующего ответа БУ.

P3 = Время между окончанием ответа БУ и началом нового запроса СПА или между окончанием ответа БУ и началом подтверждения СПА, или между окончанием запроса СПА и началом нового запроса СПА при отсутствии ответа от БУ.

P4 = Межбайтовый интервал для запроса СПА.

P5 = Увеличенное значение P3 для загрузки данных с карточек.

Допустимые значения временных параметров приводятся в нижеследующей таблице (расширенный диапазон временных параметров протокола KWP для использования при физической адресации в целях ускорения передачи данных).

Время Параметр	Нижний предел Значение (мс)	Верхний предел Значение (мс)
P1	0	20
P2	20	1000 (*)
P3	10	5000
P4	5	20
P5	10	20 минут

(*) если БУ выдает отрицательный ответ с кодом, означающим «запрос получен правильно – ожидается ответ», это значение увеличивается до соответствующего верхнего предельного значения P3.

2.2.5 Обработка ошибок

При возникновении ошибки в процессе обмена сообщениями схема потока сообщений модифицируется в зависимости от того, каким из приборов обнаружена ошибка и каким сообщением она вызвана.

На рис. 2 и рис. 3 показаны процедуры обработки ошибок, соответственно, для БУ и для СПА.

2.2.5.1 Этап инициализации обмена данными

DDP_020 Если СПА обнаруживает ошибку синхронизации или ошибку в битовом потоке на стадии инициализации обмена данными, период ожидания СПА перед повторением запроса равняется P3 min.

DDP_021 Если БУ обнаруживает ошибку в очередности сообщений от СПА, оно не высылает ответа и ожидает нового сообщения с запросом инициализации обмена данными в течение периода, равного P3 max.

2.2.5.2 Этап обмена данными

На этой стадии можно выделить две разных области обработки ошибок:

1. БУ обнаруживает ошибку в передаче данных от СПА

DDP_022 БУ проверяет каждое полученное сообщение на ошибки синхронизации, ошибки в формате байтов (например, в стартовом и стоповом разрядах) и ошибки передачи кадров (неверное число полученных байтов, ошибки в байте контрольной суммы).

DDP_023 При обнаружении одной из вышеназванных ошибок БУ не высылает ответа и игнорирует поступившее сообщение.

DDP_024 БУ может обнаружить и другие ошибки в формате или содержании полученного сообщения (например, «сообщение не поддерживается»), даже если оно соответствует требованиям по длине и контрольной сумме; в подобном случае БУ высылает СПА отрицательный ответ с указанием характера ошибки.

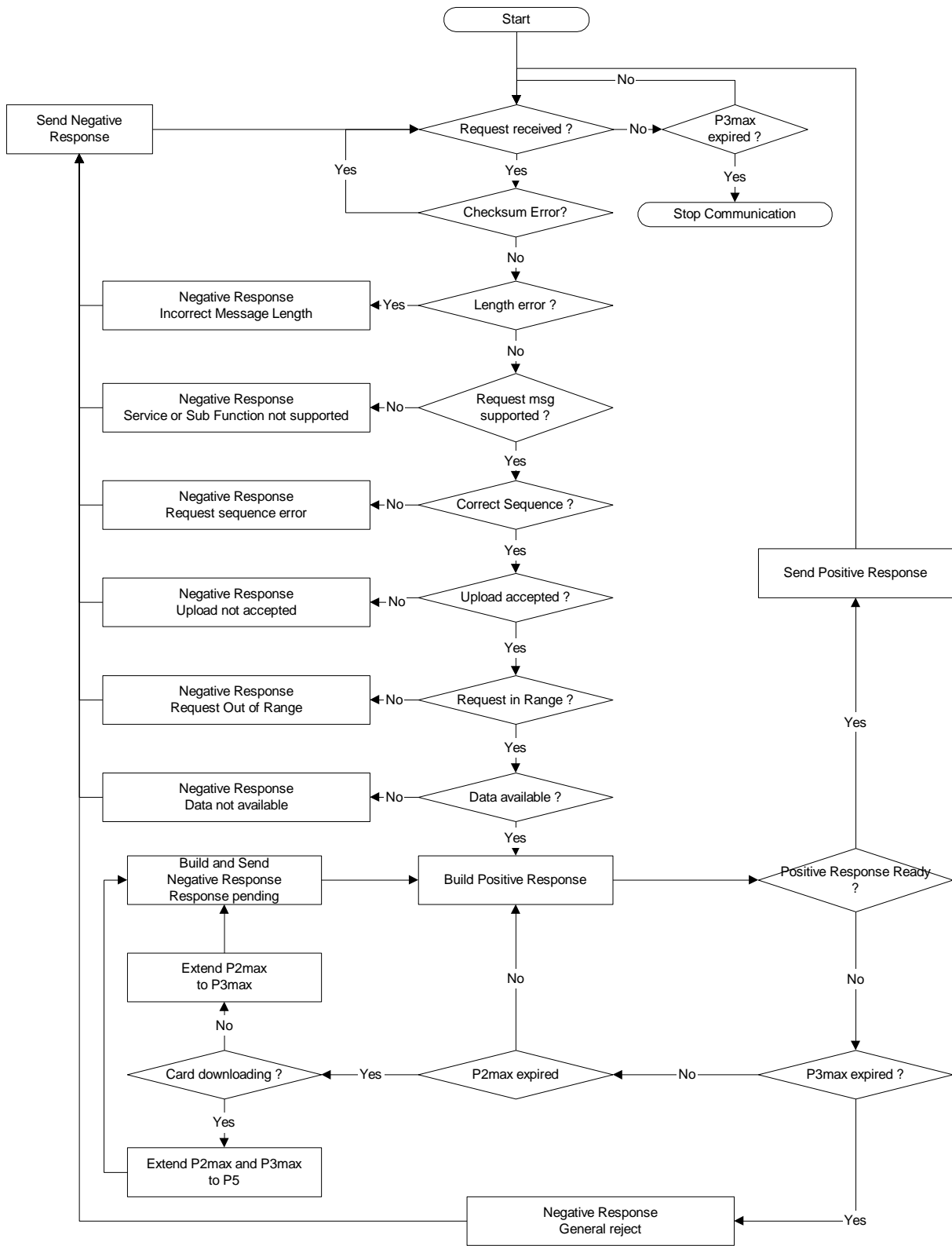


Рисунок 2 – Обработка ошибок в БУ

2. СПА обнаруживает ошибку в передаче данных из БУ.

DDP_025 СПА проверяет каждое полученное сообщение на ошибки синхронизации, ошибки в формате байтов (например, в стартовом и стоповом разрядах) и ошибки передачи кадров (неверное число полученных байтов, ошибки в байте контрольной суммы).

DDP_026 СПА проверяет поступающие сообщения на ошибки очерёдности, такие как сбои возрастания порядковых номеров подсообщений в последовательно поступающих сообщениях.

DDP_027 Если СПА обнаруживает ошибку или не получает от БУ ответа в течение периода, равного P2max, запрос высылается повторно, причём общее число передач ограничивается тремя. Для случаев обнаружения ошибок данного вида подтверждение приёма подсообщения рассматривается как запрос к БУ.

DDP_028 СПА ждёт хотя бы в течение периода, равного P3min, прежде чем начать каждую передачу; период ожидания измеряется с последнего вычисленного случая стоп-бита после обнаружения ошибки.

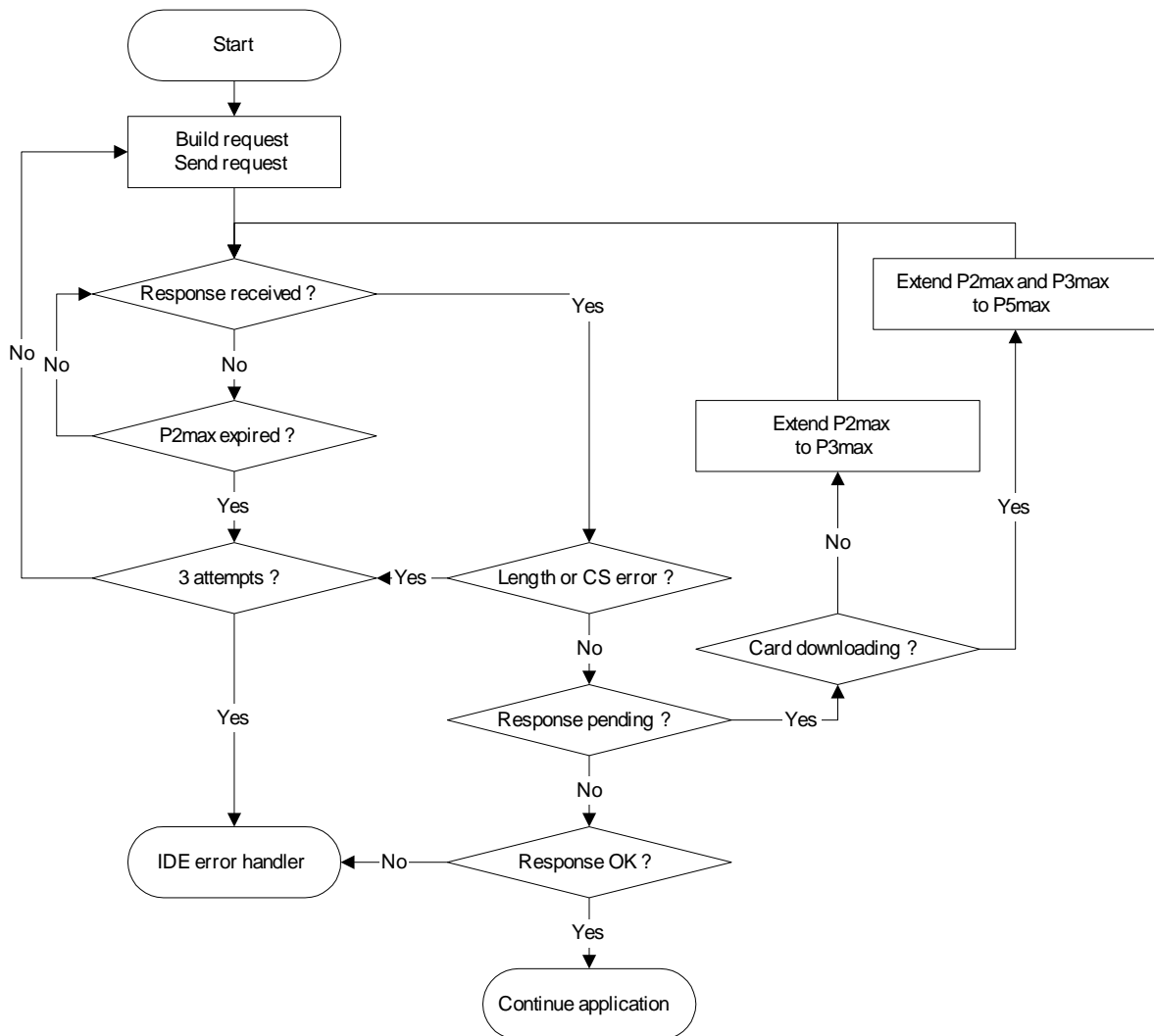


Рисунок 3 – Обработка ошибок в СПА

2.2.6 Содержание ответного сообщения

В данном пункте указано содержание полей данных различных сообщений с положительным ответом.

Элементы данных определены в словаре данных в приложении 1.

Примечание: При загрузке данных второго поколения каждый элемент данных высшего уровня представлен массивом записей, даже если в его состав входит лишь одна запись. Массив записей начинается с заголовка; данный заголовок содержит тип записи, размер записи и число записей. В нижеследующих таблицах массивы записей называются «...RecordArray» (с заголовком).

2.2.6.1 Положительный ответ: передача обзорных данных

DDP_029 В поле данных сообщения «Положительный ответ на запрос передачи обзорных данных» включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 01 Hex, с соответствующим выделением и нумерацией подсообщений:

Структура данных первого поколения

Элемент данных	Комментарий
MemberStateCertificate VUCertificate	Сертификаты защиты БУ
VehicleIdentificationNumber VehicleRegistrationIdentification	Идентификационные данные транспортного средства
CurrentDateTime VuDownloadablePeriod	Текущие дата и время БУ Период, за который могут быть загружены данные
CardSlotsStatus VuDownloadActivityData	Тип карточек, вставляемых в БУ Предыдущая загрузка данных из БУ
VuCompanyLocksData	Все хранящиеся блокировки, установленные предприятием. Если раздел не заполнен, высылается только noOfLocks = 0.
VuControlActivityData	Все сохранённые в БУ контрольные записи. Если раздел не заполнен, высылается только noOfControls = 0.
Signature	Подпись RSA для всех данных (кроме сертификатов), от VehicleIdentificationNumber до последнего байта последней VuControlActivityData.

Структура данных второго поколения

Элемент данных	Комментарий
----------------	-------------

MemberStateCertificateRecordArray
VUCertificateRecordArray
VehicleIdentificationNumberRecordArray
VehicleRegistrationNumberRecordArray
CurrentDateTimeRecordArray
VuDownloadablePeriodRecordArray
CardSlotsStatusRecordArray
VuDownloadActivityDataRecordArray
VuCompanyLocksRecordArray
VuControlActivityRecordArray
SignatureRecordArray

Сертификат государства-члена
Сертификат БУ
Идентификационные данные транспортного средства
Регистрационный номер транспортного средства
Текущие дата и время БУ
Период, за который могут быть загружены данные
Тип карточек, вставляемых в БУ
Предыдущая загрузка данных из БУ
Все хранящиеся блокировки, установленные предприятием. Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.
Все сохранённые в БУ контрольные записи. Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.
Подпись ЕСС всех предшествующих данных, кроме сертификатов.

2.2.6.2 Положительный ответ: передача данных о действиях

DDP_030 В поле данных сообщения «Положительный ответ на запрос передачи данных о действиях» включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 02 Hex, с соответствующим выделением и нумерацией подсообщений:

Структура данных первого поколения

Элемент данных	Комментарий
TimeReal	Дата загрузки
OdometerValueMidnight	Показания счётчика пробега на конец суток, к которым относятся загружаемые данные
VuCardIWData	<p>Информация о циклах ввода/извлечения карточек.</p> <ul style="list-style-type: none"> – Если в разделе нет данных, высылается только <code>noOfVuCardIWRecords = 0</code>. – Если внутри периода, охватываемого записью <code>VuCardIWRecord</code>, находится отметка 00:00 часов (карточка введена накануне) или 24:00 часа (карточка извлечена на следующий день), эта запись в полном объёме включается в данные за оба дня.
VuActivityDailyData	Состояние считывающего устройства на 00:00 часов и изменения в деятельности водителей, зарегистрированные в течение суток, к которым относятся загружаемые данные.
VuPlaceDailyWorkPeriodData	Информация о географических пунктах, зарегистрированная в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылается только <code>noOfPlaceRecords = 0</code> .
VuSpecificConditionData	Данные об особых условиях, зарегистрированные в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылается только <code>noOfSpecificConditionRecords = 0</code> .
Signature	Подпись RSA для всех данных от TimeReal до последнего байта последней записи особого условия.

Структура данных второго поколения:

Элемент данных	Комментарий
DateOfDayDownloadedRecordArray	Дата загрузки
OdometerValueMidnightRecordArray	Показания счётчика пробега на конец суток, к которым относятся загружаемые данные
VuCardIWRecordArray	<p>Информация о циклах ввода/извлечения карточек.</p> <ul style="list-style-type: none"> – Если раздел не содержит данных, высылается заголовок массива с noOfRecords = 0. – Если внутри периода, охватываемого записью VuCardIWRecord, находится отметка 00:00 часов (карточка введена накануне) или 24:00 часа (карточка извлечена на следующий день), эта запись в полном объёме включается в данные за оба дня.
VuActivityDailyRecordArray	Состояние считывающего устройства на 00:00 часов и изменения в деятельности водителей, зарегистрированные в течение суток, к которым относятся загружаемые данные.
VuPlaceDailyWorkPeriodRecordArray	Информация о географических пунктах, зарегистрированная в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.
VuGNSSCDRecordArray	Местоположение транспортного средства по ГНСС, где непрерывное время вождения достигает значения, кратного трём часам. Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.
VuSpecificConditionRecordArray	Данные об особых условиях, зарегистрированные в течение суток, к которым относятся загружаемые данные. Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.
SignatureRecordArray	Подпись ЕСС всех предшествующих данных.

2.2.6.3 Положительный ответ на запрос передачи данных о событиях и неисправностях

DDP_031 В поле данных сообщения «Положительный ответ на запрос передачи данных о событиях и неисправностях» включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 03 Hex, с соответствующим выделением и нумерацией подсообщений:

Структура данных первого поколения

Элемент данных	Комментарий
VuFaultData	Записи о всех неисправностях, зарегистрированные или происходящие в БУ. Если раздел не заполнен, высылается только noOfVuFaults = 0.
VuEventData	Все события (кроме превышения скорости), зарегистрированные или происходящие в БУ. Если раздел не заполнен, высылается только noOfVuEvents = 0.
VuOverSpeedingControlData	Данные, относящиеся к последнему контролю за превышениями скорости (при отсутствии данных – значение по умолчанию).
VuOverSpeedingEventData	Все сохранённые в БУ события превышения скорости. Если раздел не заполнен, высылается только noOfVuOverSpeedingEvents = 0.

VuTimeAdjustmentData
Signature

<p>Вся сохранённая в БУ информация о корректировках времени (кроме производимых в процессе общей калибровки).</p> <p>Если раздел не заполнен, высылается только noOfVuTimeAdjRecords = 0.</p>
<p>Подпись RSA для всех данных от noOfVuFaults до последнего байта последней записи о корректировке времени</p>

Структура данных второго поколения:

Элемент данных
VuFaultRecordArray
VuEventRecordArray
VuOverSpeedingControlDataRecordArray
VuOverSpeedingEventRecordArray
VuTimeAdjustmentRecordArray
VuTimeAdjustmentGNSSRecordArray
SignatureRecordArray

Комментарий
<p>Записи о всех неисправностях, зарегистрированные или происходящие в БУ.</p> <p>Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.</p>
<p>Все события (кроме превышения скорости), зарегистрированные или происходящие в БУ.</p> <p>Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.</p>
<p>Данные, относящиеся к последнему контролю за превышениями скорости (при отсутствии данных – значение по умолчанию).</p>
<p>Все сохранённые в БУ события превышения скорости.</p> <p>Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.</p>
<p>Вся сохранённая в БУ информация о корректировках времени (кроме производимых в процессе общей калибровки).</p> <p>Если раздел не заполнен, высылается заголовок массива с noOfRecords = 0.</p>
<p>Подпись ECC всех предшествующих данных.</p>

2.2.6.4 Положительный ответ: передача подробных данных о скорости

DDP_032 В поле данных сообщения «Положительный ответ на запрос передачи подробных данных о скорости» включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 04 Hex, с соответствующим выделением и нумерацией подсообщений:

Структура данных первого поколения

Элемент данных
VuDetailedSpeedData
Signature

Комментарий

Вся сохранённая в БУ подробная информация о скоростном режиме (один блок данных о скорости за каждую минуту движения транспортного средства) 60 значений скорости в минуту (одно в секунду)

Подпись RSA для всех данных от поOfSpeedBlocks до последнего байта последней записи блока данных о скорости.

Структура данных второго поколения:

Элемент данных
VuDetailedSpeedBlockRecordArray
SignatureRecordArray

Комментарий

Вся сохранённая в БУ подробная информация о скоростном режиме (один блок данных о скорости за каждую минуту движения транспортного средства) 60 значений скорости в минуту (одно в секунду)

Подпись ECC всех предшествующих данных.

2.2.6.5 Положительный ответ: передача технических данных

DDP_033 В поле данных сообщения «Положительный ответ на запрос передачи технических данных» включаются перечисленные ниже данные в порядке, соответствующем нижеуказанному, при SID 76 Hex и TREP 05 Hex, с соответствующим выделением и нумерацией подсообщений:

Структура данных первого поколения

Элемент данных	Комментарий
VuIdentification	
SensorPaired	
VuCalibrationData	Все сохранённые в БУ записи калибровки.
Signature	Подпись RSA для всех данных от VuManufacturerName последнего байта последней записи VuCalibrationRecord.

Структура данных второго поколения:

Элемент данных
VuIdentificationRecordArray
VuSensorPairedRecordArray
VuSensorExternalGNSSCoupledRecordArray
VuCalibrationRecordArray
VuCardRecordArray
VuITSConsentRecordArray
VuPowerSupplyInterruptionRecordArray
SignatureRecordArray

Комментарий

Все пары MS, сохранённые в БУ
Все данные о подключении внешнего устройства ГНСС, хранящиеся в БУ
Все сохранённые в БУ записи калибровки.
Все сохранённые в БУ данные ввода карточек.
Подпись ECC всех предшествующих данных.

2.3. Хранение файлов на ВН

DDP_034 В случаях, когда сеанс загрузки данных включает в себя передачу данных с БУ, СПА сохраняет в виде одного физического файла все данные, полученные от БУ в ходе сеанса загрузки в сообщениях типа «Положительный ответ на запрос передачи данных». Сохраняемые данные не включают в себя заголовки сообщений, счётчики подсообщений, пустые подсообщения и контрольные суммы, но включают SID и TREP (при наличии нескольких подсообщений – только для первого подсообщения).

3. Протокол загрузки данных с карточек тахографа

3.1. Область применения

В настоящем пункте изложен порядок прямой загрузки данных с карточки тахографа на СПА. СПА не является частью защищённой среды; поэтому процедура аутентификации между карточкой и СПА не предусмотрена.

3.2. Определения

Сеанс загрузки данных: Каждая загрузка данных с ICC. Сеанс включает в себя всю процедуру, от перезапуска карточки считывающим устройством до деактивации ICC (т.е. извлечения или новой перезагрузки карточки).

Файл подписанных данных: Файл из ICC. Файл передаётся на IFD в текстовой форме. В ICC происходит хеширование и подпись файла, а подпись передаётся в IFD.

3.3. Загрузка данных карточки

DDP_035 Процесс загрузки данных с карточки тахографа состоит из следующих этапов:

- Загрузка общей информации, записанной на карточке в элементарных файлах ICC и IC. Эта информация не является обязательной и не защищена цифровой подписью.
- Загрузка элементарных файлов Card_Certificate (или CardSignCertificate) и CA_Certificate. Эта информация не защищена цифровой подписью. Вышеуказанные файлы загружаются в обязательном порядке при каждом сеансе загрузки.
- Загрузка элементарных файлов данных других приложений (в Tachograph_DF и Tachograph_G2_DF, если уместно), за исключением EF Card_Download. Эта информация защищена цифровой подписью.
- При каждом сеансе загрузки обязательно загружаются как минимум элементарные файлы Application_Identification и ID.
 - При загрузке данных с карточки водителя в обязательном порядке загружаются также следующие элементарные файлы:
 - Events_Data,
 - Faults_Data,
 - Driver_Activity_Data,
 - Vehicles_Used,
 - Places,
 - GNSS_Places (если уместно),
 - Control_Activity_Data,
 - Specific_Conditions.
- При загрузке данных с карточки водителя обновляется дата LastCardDownload в элементарном файле Card_Download,
- При загрузке данных с карточки мастерской сбрасывается счётчик калибровки в элементарном файле Card_Download.
- При загрузке данных с карточки мастерской элементарный файл EF Sensor_Installation_Data не загружается.

3.3.1 Процедура инициализации

DDP_036 IDE иницирует следующую последовательность:

Карточка	Направление	IDE / IFD	Значение / Примечания
	←	Перезагрузка аппаратного обеспечения	
ATR	⇒		

Для переключения на более высокую скорость передачи данных, если она поддерживается ICC, можно использовать PPS.

3.3.2 Процедура для неподписанных файлов данных

DDP_037 Процедура загрузки элементарных файлов ICC, IC, Card_Certificate (или CardSignCertificate) и CA_Certificate выглядит следующим образом:

Карточка	Направление	IDE / IFD	Значение / Примечания
	←	Select File	Выбор файла по идентификаторам
OK	⇒		
	←	Read Binary	Если файл содержит больше данных, чем позволяет объём буфера считывателя или карточки, команду следует повторять до тех пор, пока не будет прочитан весь файл.
File Data OK	⇒	Сохранение данных на ВН	в соответствии с 3.4 Формат хранения данных

Примечание 1: перед выбором элементарного файла Card_Certificate (или CardSignCertificate) необходимо выбрать приложение тахографа (выбор по AID).

Примечание 2: выбор и чтение файла также могут выполняться в один приём при помощи команды Read Binary с коротким идентификатором EF.

3.3.3 Процедура для подписанных файлов данных

DDP_038 Для каждого из нижеперечисленных файлов, загружаемых вместе с соответствующей подписью, применяется следующая процедура:

Карточка	Направление	IDE / IFD	Значение / Примечания
	↵	Select File	
OK	⇒		
	↵	Perform Hash of File	Рассчитывает хеш-функцию по данным, содержащимся в выбранном файле, на основе хеш-алгоритма в соответствии с приложением 11. Эта команда не является ISO-командой.
Расчёт и временное хранение хеш-функции файла			
OK	⇒		
	↵	Read Binary	Если файл содержит больше данных, чем может сохранить буфер считывателя или карточки, команду следует повторять до тех пор, пока не будет прочитан весь файл.
File Data OK	⇒	Сохранение полученных данных на ВН	в соответствии с 3.4 Формат хранения данных
	↵	PSO: Compute Digital Signature	
На основе временно сохраненной хеш-функции выполняется защитная операция генерирования цифровой подписи			
Signature OK	⇒	Данные приобщаются к данным, сохраненным на ВН ранее	в соответствии с 3.4 Формат хранения данных

Примечание: выбор и чтение файла также могут выполняться в один приём при помощи команды Read Binary с коротким идентификатором EF. В подобных случаях EF можно выбрать и прочитать до применения команды Perform Hash of File.

3.3.4 Процедура обнуления счётчика калибровок

DDP_039 Для обнуления счетчика NoOfCalibrationsSinceDownload в элементарном файле EF Card_Download, хранящемся на карточке мастерской, применяется следующая процедура:

Карточка	Направление	IDE / IFD	Значение / Примечания
	↵	Select File EF Card_Download	Выбор файла по идентификаторам
OK	⇒		
	↵	Update Binary NoOfCalibrationsSinceDownload = '00 00'	
Обнуляется значение загрузок данных карточки			
OK	⇒		

Примечание: выбор и обновление файла также могут выполняться в один приём при помощи команды Update Binary с коротким идентификатором EF.

3.4. Формат хранения данных

3.4.1 Введение

DDP_040 Загружаемые данные хранятся с соблюдением следующих условий:

- Данные сохраняются транспарентно. Это означает, что последовательность байтов, а также последовательность битов внутри каждого байта переносимых с карточки данных должна при их сохранении оставаться неизменной;
- Все файлы, загружаемые с карточки за один сеанс загрузки, сохраняются на ВН в виде одного файла.

3.4.2 Формат файла

DDP_041 Формат файла представляет собой конкатенацию нескольких объектов TLV.

DDP_042 Меткой EF является FID с добавлением „00“.

DDP_043 Меткой подписи EF является FID файла с добавлением „01“.

DDP_044 Значение длины состоит из двух байтов. Им определяется число байтов в поле значений. Значение „FF FF“ в поле длины резервируется для последующего использования.

DDP_045 Если файл не загружается, никакая информация о нём сохранению не подлежит (т.е. не сохраняется ни метка, ни нулевой параметр длины).

DDP_046 В качестве объекта TLV, следующего непосредственно за объектом TLV с данными файла, сохраняется подпись.

Определение	Значение	Длина
FID (2 байта) „00“	Метка EF (FID)	3 байта
FID (2 байта) „01“	Метка подписи EF (FID)	3 байта
xx xx	Поле длины значения	2 байта

Пример данных в файле, загруженном на ВН:

Метка:	Длина	Значение
00 02 00	00 11	Данные EF ICC
c1 00 00	00 c2	Данные EF Card_Certificate
		...
05 05 00	0A 2E	Данные EF Vehicles_Used
05 05 01	00 80	Подпись EF Vehicles_Used

4. Загрузка данных с карточки тахографа через бортовое устройство

DDP_047 БУ должно обеспечивать возможность загрузки данных с введённой в него карточки водителя на подключённую СПА.

DDP_048 Для инициализации данного режима СПА направляет БУ сообщение «Запрос передачи данных, загружаемых с карточки» (см. 2.2.2.9).

DDP_049 После этого БУ файл за файлом загружает с карточки все имеющиеся на ней данные в соответствии с протоколом загрузки, который определён в пункте 3, и передаёт все полученные таким образом данные на СПА в соответствующем формате TLV (см. 3.4.2), заключённые внутри сообщения «Положительный ответ: передача данных».

DDP_050 СПА извлекает данные карточки из сообщения «Положительный ответ: передача данных» (освобождая их от всех заголовков, SID, TREP, счётчиков подсообщений и контрольных сумм) и сохраняет их в одном физическом файле, как указано в пункте 2.3.

DDP_051 Затем БУ при необходимости обновляет содержание файла Control_Activity_Data или Card_Download на карточке водителя.