ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р
(проект, первая редакция)

Автомобильные транспортные средства

ТАХОГРАФЫ ЦИФРОВЫЕ

Протоколы обмена информацией с автоматизированной информационной системой тахографического контроля

Настоящий проект стандарта не подлежит применению до его утверждения

Москва
Российский институт стандартизации
202_

ГОСТ Р
(проект, первая редакция)

Предисловие

1 РАЗРАБОТАН Ассоциацией по содействию безопасности автотранспортной деятельности «Тахографический Центр» и Федеральным государственным унитарным предприятием «Центральный ордена Трудового Красного Знамени научно-исследовательский автомобильный и автомоторный институт «НАМИ» (ФГУП «НАМИ»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 056 «Дорожный транспорт»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от _____202_ г. №_____

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru).

Содержание

Введение

В настоящем стандарте рассматривается протокол передачи сообщений для систем сбора и обработки тахографических данных на цифровых тахографах.

Тахограф устанавливает соединение с сервером – обработчиком тахографических данных (далее – ОТД), которому передает сообщения, предназначенные для систем сбора и обработки данных.

Взаимодействие тахографа с ОТД осуществляется по TCP/IP протоколу. Обмен сообщениями с содержательными данными выполняется по каналу защищенного обмена (далее – ЗОС).

Все криптографические операции в тахографе выполняются блоком СКЗИ тахографа (далее БТИ – блок тахографической информации).

Структура и состав содержательных данных сообщений, предназначенные для систем сбора и обработки данных, в настоящем стандарте не рассматриваются.

ГОСТ Р
(проект, первая редакция)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Автомобильные транспортные средства
ТАХОГРАФЫ ЦИФРОВЫЕ
Протоколы обмена информацией с автоматизированной информационной системой тахографического контроля

Motor vehicles. Digital tachographs. Protocols of information exchange with the automated information system of tachographic control.

Дата введения — — —

1 Область применения

Настоящий стандарт устанавливает протоколы обмена информацией цифрового тахографа, устанавливаемого на автомобильные транспортные средства (далее – АТС), с автоматизированной информационной системой тахографического контроля, а также требования к технологическому процессу сбора и обработки данных.

Настоящий стандарт не распространяется на контрольные устройства, устанавливаемые на АТС в соответствии с требованиями [1].

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 14443-3 – 2014 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 3: Инициализация и антиколлизия

П р и м е ч а н и е – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом

утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Сокращения

В настоящем стандарте использованы следующие сокращения:

БТИ – блок тахографической информации;

ДЦ – доверенный центр;

ЗОС – защищенный обмен сообщениями;

ОТД – обработчик тахографических данных;

ФБУ – Федеральное бюджетное учреждение «Росавтотранс»;

TCP (TCP/IP) – протокол передачи данных Transmission Control Protocol и Internet Protocol;

|| – символ конкатенации;

0x – префикс для указания шестнадцатеричного числа.

4 Основные положения

4.1 Формат сообщений протокола

Сообщение протокола состоит из заголовка фиксированной длины и тела в формате информационного TLV объекта, тэгом которого является код типа сообщения.

4.1.1 Формат заголовка

Заголовок сообщения имеет фиксированную длину, равную 37 байт.

Структура заголовка сообщения приведена в таблице 1.

Т а б л и ц а 1 – Структура заголовка сообщения

Смещение	Длина, байт	Значение/Описание
00	4	Фиксированная константа – Magic, 0x41544C53
04	1	Версия транспортного протокола, 0x07
05	4	Код/идентификатор системы сбора и обработки данных
09	16	Заводской номер БТИ – Part Number, байтовый массив
25	2	Длина тела сообщения
27	8	Контекст ОТД – ServerCTX, байтовый массив
35	2	CRC16 тела сообщения (см. приложение А)

4.1.1.1 Поле «Код/идентификатор системы сбора и обработки данных»

В заголовке сообщения указывается 4-х байтовый код/идентификатор системы сбора и обработки данных, которому предназначено сообщение. Структура кода представлена в таблице 2.

Т а б л и ц а 2 – Структура кода системы сбора и обработки данных

Поле	Тип	Длина, байт	Значение/Описание
Code	uInt_16	2	Код/идентификатор системы 0xA085 – код системы регистрации 0xA087 – код системы сбора и обработки данных ФБУ
RFU	-	2	0x0000

Также код/идентификатор системы сбора и обработки данных указывается в теле содержательного сообщения.

В заголовке сообщений для ОТД (0x30 - 0x38) 4 байта кода/идентификатора имеют нулевое значение.

В заголовке и теле содержательного сообщения (0x39) с данными для ОТД 4 байта кода/идентификатора имеют нулевое значение.

В заголовке и теле содержательных сообщений (0x39) для системы сбора и обработки данных 4 байта кода/идентификатора имеют не нулевое значение.

В заголовке сообщений (0x3A, 0x3B) для системы сбора и обработки данных 4 байта кода/идентификатора имеют не нулевое значение

4.1.1.2 Поле «Контекст ОТД» (ServerCTX)

Поле ServerCTX позволяет восстановить на ОТД контекст обработки поступающих данных от тахографа в случае разрыва TCP/IP соединения и последующего его восстановления.

При формировании сообщения (кроме запроса CONNECTREQUEST) поле ServerCTX инициализируется значением ServerCTX, полученным из последнего ответа от сервера.

Если после получения успешного ответа на запрос произошел разрыв TCP/IP соединения (или если нет ответов на запросы, что приводит к разрыву TCP/IP соединения), то тахограф заново подключается по TCP/IP к серверу и посылает следующее сообщение, со значением поля ServerCTX, полученного из последнего успешного ответа от сервера.

Сообщение CONNECTREQUEST формируется следующим образом:

1) поле ServerCTX для запроса CONNECTREQUEST заполняется байтами со значением 0x00 в следующих случаях:

- значение поля ServerCTX из последнего полученного успешного ответа от сервера неизвестно;

- интервал в обмене с ОТД больше 10 минут;

- по тем или иным причинам необходимо заново проинициализировать контекст обработки данных на ОТД;

2) в остальных случаях поле ServerCTX для запроса CONNECTREQUEST заполняется значением поля ServerCTX, взятого из последнего полученного успешного ответа от сервера.

4.1.2 Информационный объект TLV

Каждый объект TLV должен состоять из двух или трех последовательных полей: обязательного поля тега, обязательного поля длины и условного поля значения. Кодировка поля тэгов приведена в таблице 3.

Поле тега состоит из одиночного байта, кодирующего номер тега от 1 до 254. Значения '00' и 'FF' являются недействительными для поля тега.

Т а б л и ц а 3 – Кодировка поля тэгов

b8	b7	b6	b5	b4	b3	b2	b1	Описание
0	0	1	1	-	-	-	-	Сообщение. Структурированное кодирование, т.е. поле значения кодировано в TLV
0	0	0	1	-	-	-	-	Протокольные данные, передаваемые в сообщениях с содержательными данными
0	0	1	0	-	-	-	-	Открытые содержательные данные, передаваемые в сообщениях с содержательными данными
1	0	1	0	-	-	-	-	Зашифрованные содержательные данные, передаваемые в сообщениях с содержательными данными
0	0	0	0	-	-	-	-	Данные, передаваемые в сообщениях при установлении соединения и аутентификации
-	-	-	-	x	x	x	x	Номер тэга

Поле длины состоит из одного или большего числа последовательных байтов. Кодирование этих байтов должно соответствовать основным правилам кодирования ASN.1 и определению в таблице 4.

В коротком формате поле длины состоит из единичного байта, в котором бит 8 установлен в состояние 0, а биты с 7 по 1 кодируют число байтов в поле значения. Таким образом одним байтом может быть закодировано любое число от нуля до 127.

В длинном формате поле длины состоит из двух или более байтов.

Поля длины TLV объектов приведены в таблице 4.

Таблица 4 – Поля длины TLV объектов и правила кодирования

Диапазон	Байт	1 байт	2 байт	3 байт
От 0 до 127	1 байт	От '00' до 7F'	-	-
От 0 до 255	2 байта	'81'	От '00' до 'FF'	-
От 0 до 65535	3 байта	'82'	От '0000' до 'FFFF'	

Если поле длины равно нулю, то поле значения отсутствует, т.е. объект является пустым. В противном случае, если объект простой, поле значения состоит из последовательных байтов; если объект структурированный, поле значения состоит из набора простых TLV объектов.

4.1.3 Типы сообщений

Типы сообщений приведены в таблице 5.

Т а б л и ц а 5 – Типы сообщений

Тэг	Название	Примечание
0x30	CONNECTREQUEST	Выдается тахографом сразу после установления соединения
0x31	SERVERHELLO	Выдается сервером при установлении сессии или в качестве запроса на повторную аутентификацию
0x33	DENYSESSION	Выдается сервером в случае разрыва соединения и/или закрытия сессии ЗОС по инициативе сервера
0x34	CACERTREQUEST	Выдается тахографом, если у него нет сертификата ДЦ
0x35	CACERTCHAIN	Выдается сервером в ответ на CACERTREQUEST
0x36	INITSESSION	Выдается тахографом для динамической аутентификации
0x37	CONFIRMSESSION	Выдается сервером в ответ на успешную динамическую аутентификацию
0x39	MESSAGE	Зашифрованные сообщения, защищенные имитовставкой. (Данные в сообщении могут быть не зашифрованы)
0x3A*	PROMPT	Периодически выдается тахографом для согласования текущей частоты передачи запросов
0x3B*	SERVERREQUEST	Выдается сервером в ответ на PROMPT
* Опционально		

4.1.4 Формат тела сообщений

4.1.4.1 CONNECTREQUEST

Тэг 0x30, выдается тахографом сразу после установления соединения. Состоит из набора объектов TLV, приведенных в таблице 6.

Т а б л и ц а 6 – Набор объектов TLV, выдаваемых тахографом сразу после установления соединения

Тэг	Наименование	Длина, байт	Количество	Примечание
0x02	Server Address	n	0/1	Адрес (DNS-имя) сервера
0x03	Part Number	16	1	Заводской номер БТИ
0x04	KeyId	16	1	Идентификатор открытого ключа БТИ
0x05	Random	16	1	Случайное число БТИ
0x06	RFU	4	1	0x00000000

4.1.4.2 SERVERHELLO

Тэг 0x31, выдается сервером сразу после получения запроса на установление соединения или в ходе установленной сессии с целью проведения повторной динамической аутентификации. Состоит из набора объектов TLV, приведенных в таблице 7.

Т а б л и ц а 7 – Набор объектов TLV, выдаваемых сервером сразу после получения запроса на установление соединения или в ходе установленной сессии

Тэг	Наименование	Длина, байт	Количество	Примечание
0x01	Certificate	до 3000	1	Сертификат сервера
0x05	Random	16	1	Случайное число сервера

4.1.4.3 DENYSESSION

Тэг 0x33, выдается сервером в случае разрыва соединения, сессии ЗОС. Состоит из набора объектов TLV приведенных в таблице 8.

Т а б л и ц а 8 – Набор объектов TLV, выдаваемых сервером в случае разрыва соединения

Тэг	Наименование	Длина, байт	Количество	Примечание
0x09	ErrorCode	2	1	Код причины разрыва соединения.
0x0A	Description	0-n	1	Описание причины разрыва соединения (короткое сообщение)

4.1.4.4 CACERTREQUEST

Тэг 0x34, выдается тахографом, если у него нет открытого ключа ДЦ для проверки сертификата сервера. Сообщение содержит объекты TLV с идентификаторами ключей ДЦ известных БТИ (см. таблицу 9).

Т а б л и ц а 9 – Набор объектов TLV, выдаваемых тахографом, если у него нет открытого ключа ДЦ для проверки сертификата сервера

Тэг	Наименование	Длина, байт	Количество	Примечание
0x04	KeyId	16	1 и более	Идентификатор ключа ДЦ

4.1.4.5 CACERTCHAIN

Тэг 0x35, выдается сервером в ответ на сообщение тахографа - CACERTREQUES. Сообщение содержит объекты TLV с сертификатами ДЦ, составляющими цепочку сертификатов, которые необходимо передать в БТИ в том порядке, в каком они присланы сервером (см. таблицу 10).

Т а б л и ц а 10 – Набор объектов TLV, выдаваемых сервером в ответ на сообщение тахографа - CACERTREQUES

Тэг	Наименование	Длина, байт	Количество	Примечание
0x01	Certificate	до 3000	1 и более	Сертификат ДЦ (Передаются в том порядке, в котором должны быть переданы в БТИ на проверку)

4.1.4.6 INITSESSION

Тэг 0x36, выдается тахографом для динамической аутентификации. Состоит из набора объектов TLV, приведенных в таблице 11.

Т а б л и ц а 11 – Набор объектов TLV, выдаваемых тахографом для динамической аутентификации

Тэг	Наименование	Длина, байт	Количество	Примечание
0x01	Certificate	до 3000	1	Сертификат открытого ключа БТИ
0x05	Random	16	1	Случайное число БТИ
0x07	S	64	1	Криптограмма БТИ

4.1.4.7 CONFIRMSESSION

Тэг 0x37, выдается сервером в ответ на сообщение тахографа INITSESSION для динамической аутентификации (см. таблицу 12).

Т а б л и ц а 12 – Набор объектов TLV, выдаваемых сервером в ответ на сообщение тахографа INITSESSION

Тэг	Наименование	Длина, байт	Количество	Примечание
0x08	H	10	1	Текущее время сервера (4 байта) || Проверочная криптограмма сервера (6 байт)

4.1.4.8 PROMPT

Тэг 0x3A, периодически выдается тахографом для согласования текущей частоты передачи данных. Состоит из набора объектов TLV, приведенных в таблице 13:

Т а б л и ц а 13 – Набор объектов TLV, выдаваемых тахографом для согласования текущей частоты передачи данных

Тэг	Наименование	Длина, байт	Количество	Примечание
0x03	Part Number	16	0/1	Заводской номер БТИ
0x0B	Freq	4	1	Текущая частота передачи сообщений

4.1.4.9 SERVERREQUEST

Тэг 0x3B, выдается сервером в ответ на сообщение PROMPT. Состоит из набора объектов TLV, приведенных в таблице 14.

Т а б л и ц а 14 – Набор объектов TLV, выдаваемых сервером в ответ на сообщение тахографа PROMPT

Тэг	Наименование	Длина, байт	Количество	Примечание
0x03	Part Number	16	0/1	Заводской номер БТИ
0x0B	Freq	4	1	Текущая частота передачи сообщений
0x0C	ServerRequest	4	1	Код процедуры/уведомления, запрашиваемого сервером. В случае передачи фиксированного значения (например 0) тахограф считает, что необходимости в оперативном общении с сервером нет

4.1.4.10 MESSAGE

Тэг 0x39, выдается сервером и тахографом. Используется для передачи содержательных данных в открытом или зашифрованном виде. Состоит из набора объектов TLV, приведенных в таблице 15.

Т а б л и ц а 15 – Набор объектов TLV, выдаваемых сервером и тахографом при обмене содержательными данными

Тэг	Наименование	Длина, байт	Количество	Примечание
0x20	Payload	до 4000	0 - если есть 0xA0 1 - если нет	Открытые содержательные данные. Если в сообщении нет содержательных данных, должен присутствовать это объект нулевой длины
0xA0	Payload_enc	до 4000	0 - если есть 0x20 1 - если нет	Зашифрованные содержательные данные. Если в сообщении нет содержательных данных, должен присутствовать это объект нулевой длины
0x10	SerialNo*	4	1	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	1	Номер последнего сообщения, полученного отправителем данного
0x12	RetransmitReq	1	0-1	Запрос повторной передачи данных предыдущего сообщения с кодом причины запроса
0x13	IDProcessingSys	4	0-1	Код/идентификатор системы сбора и обработки данных
0x14	VPProcessingSys	1	0-1	Версия протокола обмена с системой сбора и обработки данных
0x15	UTISerial	16(32)	0-1	Заводской (заводской и регистрационный) номер БТИ
0x1C	Diagnostic	1	0-1	Диагностические данные для сервера
0x1D	Priority	1	0-1	Уровень приоритета сообщения
0x1F	Source	1	1	Источник данных
0x1E	MAC	6	1	Имитовставка

4.1.4.10.1 Объект SerialNo

Тахограф ведет непрерывный учет сформированных сообщений. Каждому сформированному сообщению присваивается последовательный порядковый номер. При обрыве и восстановлении или установлении нового соединения нумерация продолжается.

Для сервера допускается ведение непрерывного учета сформированных ответных сообщений только в течение установленного соединения. Нумерация сохраняется при обрыве сессии с восстановлением и при повторной динамической аутентификации. При установлении нового соединения нумерация может начаться заново.

4.1.4.10.2 Объект Source

Сообщение содержит обязательный объект источника содержательных данных

сообщения.

В объекте источника содержательных данных сообщения сервер может передать запрос на передачу данных БТИ или тахографу.

Кодировка источника данных приведена в таблице 16.

Т а б л и ц а 16 – Кодировка источника данных в сообщении, передаваемом тахографом или сервером

b8-b5	b4	b3	b2	b1	Источник
0	0	0	0	x	0 – Данные блока/для блока тахографической информации 1 – Данные тахографа/для тахографа
0	0	0	1	0	Запрос сервера на передачу данных тахографу
0	0	1	0	0	Запрос сервера на передачу данных блоку тахографической информации
0	1	0	0	0	Устройства контроля состояния водителя

4.1.4.10.3 Объект Priority

Сообщение может содержать необязательный объект приоритета, имеющий значение от 0 до 255. Если в сообщении отсутствует объект приоритета, оно считается имеющим приоритет 0 (не приоритетно).

4.1.4.10.4 Объекты содержательных данных сообщения

Сообщение содержит обязательный объект с содержательными данными сообщения. Данные, подготовленные БТИ, тахографом или сервером передаются в открытом виде в объекте TLV с тэгом 0x20 или в зашифрованном виде в объекте TLV с тэгом 0xA0. Длина объекта не более 4000 байт

4.1.5 Формирование сообщения MESSAGE

При формировании сообщения выполняются следующие действия:

1) Формирование содержательных данных сообщения;

2) Формирование набора объектов TLV сообщения

3) Формирование тела сообщения: к полученному набору добавляется тэг(0x39) и длина;

4) Формирование сообщения: к телу сообщения добавляется заголовок и в таком виде сообщение передается на сервер/тахограф.

4.1.5.1 Формирование набора объектов TLV тела сообщения MESSAGE

4.1.5.1.1 Набор объектов TLV сообщения MESSAGE, подготовленного тахографом

Если данные для выгрузки присутствуют, тахограф формирует набор объектов TLV с открытыми – тэг 0x20 или зашифрованными – тэг 0xA0 содержательными данными, приведенными в таблице 17.

Т а б л и ц а 17 – Набор объектов TLV сообщения MESSAGE, сформированного тахографом

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload	до 4000	Содержательные данные, подготовленные БТИ
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения полученного отправителем данного или 0x00000000 для первого сообщения
0x13	IDProcessingSys	4	Код/идентификатор системы сбора и обработки данных
0x14	VPProcessingSys	1	Версия протокола обмена с системой сбора и обработки данных
0x15	UTISerial	16(32)	Заводской (заводской и регистрационный) номер БТИ
0x1C	Diagnostic	1	Диагностические данные для сервера
0x1F	Source	1	Источник данных: 0 – БТИ, 1 – тахограф. По умолчанию – 0
0x1E	MAC	6	Имитовставка

4.1.5.1.2 Набор объектов TLV сообщения MESSAGE, подготовленного сервером

Сервер формирует набор объектов TLV с подтверждением с открытыми – тэг 0x20 или зашифрованными – тэг 0xA0 данными, приведенными в таблице 18.

Т а б л и ц а 18 – Набор объектов TLV сообщения MESSAGE, сформированного сервером

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload/ Payload_enc	до 4000	Содержательные данные с подтверждением
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения полученного от тахографа
0x13	IDProcessingSys	4	Код/идентификатор системы сбора и обработки данных
0x14	VPProcessingSys	1	Версия протокола обмена с системой сбора и обработки данных
0x15	UTISerial	16(32)	Заводской (заводской и регистрационный) номер БТИ
0x1F	Source	1	Источник данных
0x1E	MAC	6	Имитовставка

4.1.5.2 Формирование тахографом сообщения MESSAGE осуществляется в следующем порядке:

1) Формируется набор объектов TLV без объекта содержательных данных и без объекта имитовставки.

Каждому сформированному набору присваивается порядковый номер. При обрыве и восстановлении или установлении нового соединения нумерация продолжается.

2) Формируется объект содержательных данных сообщений:

- если тахограф формирует сообщение с данными БТИ, объект содержательных данных Payload / Payload_enc формируется нулевой длины;

- если тахограф формирует сообщение с собственными данными, объект содержательных данных Payload/Payload_enc формируется с данными, подготовленными тахографом.

3) Сформированный набор объектов TLV передается БТИ в команде «Получение посылки для сервера».

4) Получив сформированный набор объектов TLV, БТИ выполняет следующие действия:

- если тип данных «данные подготовленные БТИ» и объект с тэгом содержательных данных пуст, формируются содержательные данные;

- если установлен признак шифрования, переданные или сформированные содержательные данные шифруются;

- значение объекта содержательных данных модифицируется в соответствии с выполненными операциями;

- вычисляется имитовставка на весь набор объектов тела сообщения и формируется объект имитовставки;

- переформированный набор объектов выдается в ответ на команду.

5) Формируется тело сообщения: к полученному набору объектов TLV добавляется тэг(0x39) и длина;

6) Формируется сообщение: к телу сообщения добавляется заголовок, после чего сообщение передается на сервер.

4.1.5.3 Разбор сообщения MESSAGE осуществляется в следующем порядке:

1) Из тела сообщения извлекается набор объектов TLV и проверяется его корректность.

В принятом с сервера сообщении должен содержаться объект SerialNo, содержащий последовательный номер сообщения, отправленного сервером и объект

Confirmed, содержащий последовательный номер полученного от тахографа сообщения.

2) Набор объектов TLV передается БТИ в команде «Передача подтверждения сервера».

3) Получив набор объектов TLV тела сообщения, БТИ выполняет следующие действия:

- отделяет объект имитовставки;

- выполняет проверку имитовставки;

- извлекает объект содержательных данных;

- извлекает шифротекст и выполняет расшифровывание, если установлен признак шифрования.

- выполняется регистрация подтверждения, если в объекте содержательных данных передается подтверждение получения данных БТИ, данные в ответ на команду не выдаются.

- открытые данные выдаются в ответ на команду вместе с тегом и длиной, если в объекте содержательных данных передаются данные для тахографа.

4) Если при разборе тела сообщения обнаружена ошибка, тахограф должен выполнить процедуру обработки ошибки или повторить передачу данных в следующем по порядку сообщении.

4.2 Процедуры протокола

4.2.1 Инициализация обмена с сервером осуществляется при выполнении следующих условий:

1) обмен с сервером не инициализирован (обмен с сервером завершен, включение питания);

2) у тахографа есть необходимость в передаче информации в систему сбора и обработки данных.

Процедура включает следующие действия:

1) тахограф устанавливает TCP-соединение с сервером в соответствии с техническим регламентом (приложение Б);

2) тахограф выполняет процедуру открытия сессии ЗОС.

4.2.2 Завершение обмена с сервером выполняется в следующих случаях:

1) в случае разрыва соединения в соответствии с техническим регламентом (приложение Б):

- отсутствие обмена в пределах таймаута (≥ 595 с отсутствуют данные для передачи, нет ответа сервера);

- отсутствие TCP-соединение более 10 мин при попытке восстановления соединения после возникновения ошибки по TCP.

2) ошибка при открытии сессии ЗОС (ошибка аутентификации), ошибка ЗОС.

Процедура включает следующие действия:

- тахограф разрывает TCP-соединение;

-тахограф удаляет контекст обмена, хранящийся в оперативной памяти (сеансовые ключи, контекст ОТД (ServerCTX) и др.).

3) тахограф подает в БТИ команду «Завершение обмена с сервером».

4.2.3 Обмен сообщениями

После инициализации обмена с сервером обмен сообщениями выполняется в соответствии с техническим регламентом по приложению Б и протоколом сессии ЗОС (см. 4.4).

4.2.4 Обработка ошибок

В процессе обмена возможны следующие исключительные ситуации:

- разрыв TCP-соединение более 10 мин, то в этой ситуации выполняется процедура завершения обмена (см. 4.2.2);

- ошибка взаимодействия по TCP (разрыв TCP-соединение менее 595 с и другие), то в этой ситуации после восстановления соединения обмен продолжается в рамках ранее открытой сессии ЗОС (см. 4.4.2.2);

- ошибка аутентификации, то в этой ситуации выполняется процедура завершения обмена (см. 4.2.2);

- ошибка ЗОС (ошибка MAC, некорректный набор объектов TLV, превышен лимит использования сеансовых ключей), то в этой ситуации выполняется процедура повторной аутентификации (см. 4.4.4);

- ошибка взаимодействия с БТИ, то в этой ситуации выполняется процедура завершения обмена (раздел 4.2.2)

4.3 Открытие сессии защищенного обмена сообщениями

Процедура открытия сессии выполняется в рамках процедуры инициализации обмена с сервером или процедуры повторной аутентификации и включает следующие действия:

1) тахограф формирует и отправляет сообщение с запросом на открытие сессии ЗОС и получает от сервера ответное сообщение с подтверждением, в котором передается сертификат открытого ключа сервера;

2) если у тахографа нет ключей для проверки сертификата, тахограф формирует и отправляет сообщение с запросом сертификатов и получает ответное сообщение;

3) тахограф инициирует процедуру аутентификации с сервером. Тахограф формирует и отправляет сообщение с криптограммой и получает ответное сообщение с проверочной криптограммой сервера;

4) в случае успешной проверки криптограммы сервера сессия считается установленной и тахограф переходит к передаче подготовленных данных.

4.3.1 Схема открытия сессии приведена на рисунке 1.

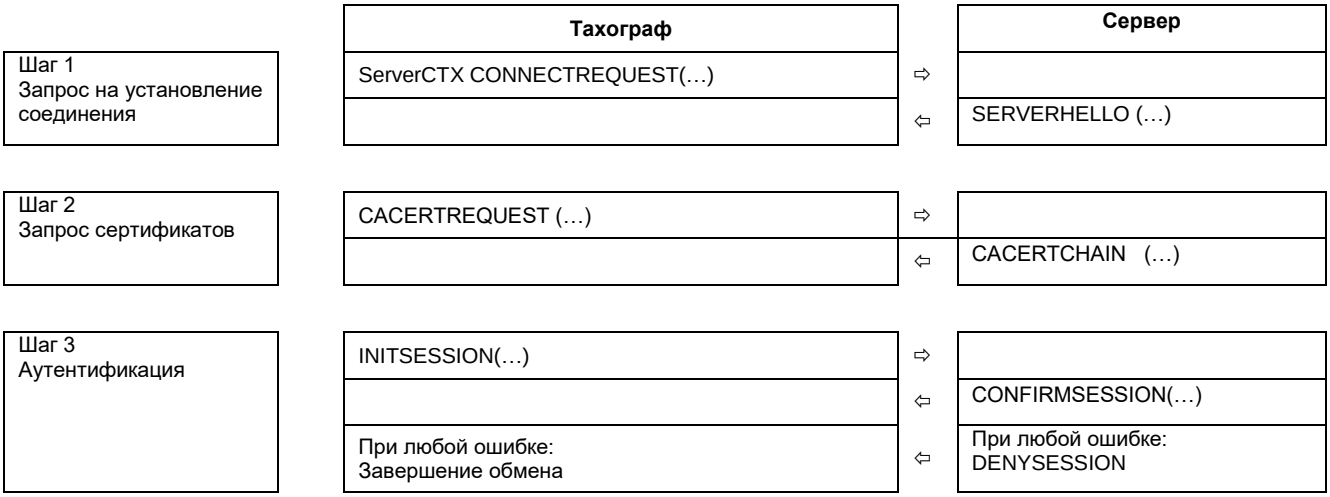

Рисунок 1 – Открытие сессии передачи тахографом подготовленных данных

4.3.2 Сценарий открытия сессии:

1) тахограф запрашивает у БТИ значение текущего состояния БТИ и статус выгрузки документов в команде «Запрос статуса БТИ».

Операции по выгрузке допустимы только в случае, если БТИ функционален.

2) тахограф формирует сообщение CONNECTREQUEST:

- считывает данные для передачи серверу (адрес (DNS-имя) сервера или другие идентификационные данные);

- запрашивает у БТИ данные активации БТИ в команде «Запрос данных активации БТИ». В ответ получает идентификационные данные БТИ, включая заводской номер БТИ;

- запрашивает у БТИ идентификаторы ключей. В ответ получает идентификатор ключа БТИ и идентификаторы ключей ДЦ известных БТИ;

- вырабатывает случайное число;

- формирует тело сообщения.

Тело сообщения CONNECTREQUEST приведено в таблице 19.

Т а б л и ц а 19 – Набор объектов TLV сообщения CONNECTREQUEST

Тэг	Наименование	Длина, байт	Количество	Примечание
0x02	Server Address	n	0/1	Адрес (DNS-имя) сервера
0x03	Part Number	16	1	Заводской номер БТИ
0x04	KeyId	16	1	Идентификатор открытого ключа БТИ
0x05	Random	16	1	Случайное число
0x06	RFU	4	1	0x00000000

3) тахограф формирует заголовок сообщения (см. 4.1.1) и передает сообщение CONNECTREQUEST серверу.

П р и м е ч а н и е – Если открытие сессии выполняется в рамках процедуры инициализации обмена, поле ServerCTX в заголовке заполняется байтами со значением 0x00. Если открытие сессии выполняется в рамках процедуры повторной аутентификации, поле заполняется значением поля ServerCTX, взятого из последнего полученного успешного ответа от сервера.

4) тахограф получает ответное сообщение SERVERHELLO.

Тело ответного сообщения SERVERHELLO приведено в таблице 20.

Таблица 20 – Набор объектов TLV сообщения SERVERHELLO

Тэг	Наименование	Длина, байт	Количество	Примечание
0x01	Certificate	до 3000	1	Сертификат сервера
0x05	Random	16	1	Случайное число сервера

Если полученное сообщение не SERVERHELLO, выполняется процедура завершения обмена (см. 4.2.2)

5) тахограф проверяет заголовок и структуру ответного сообщения. Если обнаружена ошибка, выполняется процедура завершения обмена (см. 4.2.2).

6) если открытие сессии выполняется в рамках процедуры инициализации обмена с сервером, тахограф подает в БТИ команду «Инициализация обмена с сервером».

7) тахограф извлекает из сообщения сертификат и передает его БТИ в команде «Предварительная проверка сертификата сервера».

БТИ:

- извлекает из сертификата поле CommonName;

- извлекает идентификатор ключа ДЦ для проверки сертификата и выполняет поиск ключа с идентификатором из сертификата в списке доверенных ключей ДЦ БТИ;

- выдает в ответ:

- итог поиска идентификатора ключа ДЦ, извлеченного из сертификата (ключ найден или ключ не найден);

- поле CommonName.

8) тахограф сравнивает CommonName с адресом (DNS-именем) сервера, использованным для установления соединения.

Если поле CommonName не совпадает с тем именем/адресом сервера, которое использовалось для установления соединения, выполняется процедура завершения обмена (см. 4.2.2).

9) если результат поиска – ключ известен БТИ, то переход к подпункту 13).

10) если результат поиска – ключ не известен БТИ, тахограф формирует сообщение CACERTREQUEST (см. 4.1.3.4), в которое включает идентификаторы ключей ДЦ, полученные от БТИ.

Тело сообщения CACERTREQUEST приведено в таблице 21.

Т а б л и ц а 21 – Набор объектов TLV сообщения CACERTREQUEST

Тэг	Наименование	Длина, байт	Примечание
0x04	Key ID	16	Идентификатор открытого ключа ДЦ для проверки сертификата БТИ
…	…..		…..
0x04	Key ID	16	Идентификатор открытого ключа ДЦ для проверки сертификата ДЦ

11) тахограф передает сообщение CACERTREQUEST серверу и получает ответное сообщение CACERTCHAIN с цепочкой сертификатов.

Тело ответного сообщения CACERTCHAIN приведено в таблице 22.

Т а б л и ц а 22 – Набор объектов TLV сообщения CACERTCHAIN

Тэг	Наименование	Длина, байт	Примечание
0x01	Certificate	до 3000	Сертификат ключа ДЦ для проверки следующего сертификата ДЦ
….		…..	
0x01	Certificate	до 3000	Сертификат ключа ДЦ для проверки сертификата сервера

Если не получено сообщение CACERTCHAIN, выполняется процедура завершения обмена (см. 4.2.2).

12) если получено сообщение CACERTCHAIN с цепочкой сертификатов, тахограф передает в БТИ сертификаты в том порядке, в каком они присланы сервером в команде «Проверка сертификата сервера».

Если проверка не успешна, выполняется процедура завершения обмена (см. 4.2.2).

13) тахограф передает в БТИ сертификат сервера, переданный в сообщении SERVERHELLO, в команде «Проверка сертификата сервера»;

Если проверка не успешна, выполняется процедура завершения обмена (см. 4.2.2).

14) если проверка успешна, запрашивает у БТИ сертификат БТИ в команде «Запрос сертификата ключа аутентификации БТИ»;

15) тахограф вызывает команду формирования криптограммы динамической аутентификации «Получение криптограммы БТИ», передавая туда случайное число, полученное от сервера в сообщении SERVERHELLO.

В ответ на команду БТИ выдает криптограмму и свое случайное число.

16) тахограф формирует сообщение INITSESSION (см. 4.1.3.6), в которое включает данные, полученные от БТИ.

Тело сообщения INITSESSION приведено в таблице 23.

Т а б л и ц а 23 – Набор объектов TLV сообщения INITSESSION

Тэг	Наименование	Длина, байт	Примечание
0x01	Certificate	до 3000	Сертификат открытого ключа БТИ
0x05	Random	16	Случайное число БТИ
0x07	S	80	Криптограмма

17) тахограф передает сообщение INITSESSION серверу и получает ответное сообщение CONFIRMSESSION

Тело ответного сообщения CONFIRMSESSION приведено в таблице 24.

Т а б л и ц а 24 – Набор объектов TLV сообщения CONFIRMSESSION

Тэг	Наименование	Длина, байт	Примечание
0x08	H	10	Текущее время сервера (4 байта) || Проверочная криптограмма сервера (6 байт)

Если не получено сообщение CONFIRMSESSION, выполняется процедура завершения обмена (см. 4.2.2).

18) если получено сообщение CONFIRMSESSION, тахограф вызывает команду «Проверка криптограммы сервера».

Если проверка не успешна, выполняется процедура завершения обмена (см. 4.2.2).

19) если проверка успешна, тахограф начинает выгрузку данных (см. 4.4.3.2).

4.4 Протокол сессии ЗОС

4.4.1 После открытия сессии тахограф отправляет на сервер подготовленные данные, в том числе:

- данные, которые были отправлены в ходе предыдущей сессии, но подтверждение не было получено до разрыва соединения;

- данные, которые были сформированы в период отсутствия связи.

4.4.2 Протокол сессии состоит из упорядоченного обмена сообщениями между тахографом и сервером в соответствии с техническим регламентом (приложение Б).

В ходе установленной сессии тахограф может отправлять на сервер следующие сообщения:

- защищенное имитовставкой сообщение MESSAGE, содержащие зашифрованные/открытые данные;

- сообщение CONNECTREQUEST, инициирующее повторную аутентификацию.

Сервер может отправлять тахографу в ответ на полученное сообщение:

- защищенное имитовставкой сообщение MESSAGE, содержащие зашифрованные/открытые данные (подтверждение);

- сообщение DENYSESSION о закрытии текущей сессии ЗОС.

4.4.2.1 Обмен указанными сообщениями осуществляется в следующем порядке:

1) Тахограф формирует и отправляет сообщение MESSAGE.

2) Сервер, получив сообщение, отправленное тахографом, отправляет ответное сообщение MESSAGE с подтверждением в соответствии с техническим регламентом (приложение Б).

Если при проверке сервером принятого сообщения тахографа не сошлась имитовставка или набор объектов TLV некорректен, сервер посылает сообщение DENYSESSION о закрытии сессии ЗОС (запрос на повторную аутентификацию).

3) Тахограф, после получения ответного сообщения от сервера (с подтверждением) формирует следующие сообщения с данными, на которые не получено подтверждение.

4) Если при проверке БТИ принятого сообщения сервера не сошлась имитовставка или набор объектов TLV некорректен, тахограф выполняет процедуру

обработки ошибки и посылает сообщение CONNECTREQUEST, инициирующее открытие новой сессии ЗОС (повторную аутентификацию).

5) Получив сообщение DENYSESSION, тахограф выполняет процедуру обработки ошибки и посылает сообщение CONNECTREQUEST, инициирующее открытие сессии ЗОС.

Схема обмена сообщениями приведена на рисунке 2.

	Тахограф		Сервер
1	Выдача данных MESSAGE(n, Data_n)	⇨	
		⇦	Передача квитанции MESSAGE(m, ack_ Data_n _m)
2	Выдача данных MESSAGE(n+1, Data_n+1)	⇨	
		⇦	Передача квитанции MESSAGE(m+1, ack_ Data_n+1 _m+1)
3	Выдача данных MESSAGE(n+2, Data_n+2)	⇨	
		⇦	Передача квитанции MESSAGE(m+2, ack_ Data_n+2 _m+2)
…	…	⇨	
		⇦	…
q	Выдача данных MESSAGE(n+q, Data_n+q)	⇨	
		⇦	Передача квитанции MESSAGE(m+q, ack_ Data_n+q _m+q)
	При ошибке ЗОС: Повторная аутентификация	⇦	При любой ошибке: DENYSESSION(…)

Рисунок 2 – Схема обмена сообщениями тахографа и сервера

4.4.2.2 Схема обмена после устранения ошибки взаимодействия по TCP приведена на рисунке 3.

	Тахограф		Сервер
Шаг 1 Продолжение обмена	ServerCTX≠ 0 MESSAGE(…)	⇨	
		⇦	а) Если сессия восстановлена (восстановлен контекст обработки поступающих данных, ошибки ЗОС отсутствуют) MESSAGE(…)
Шаг 2а) Продолжение обмена	MESSAGE(…)	⇨	
		⇦	MESSAGE(…)
Шаг 2б) Запрос повторной аутентификации		⇦	б) Если восстановление невозможно, DENYSESSION(…)

Рисунок 3 – Схема обмена сообщениями тахографа и сервера после обработки ошибки

4.4.3 Процедура выгрузки данных из тахографа

4.4.3.1 Выгрузка данных осуществляется в следующем порядке:

- тахограф формирует сообщение с объектом Payload/Payload_enc, содержащими данные БТИ или тахографа, с объектом SerialNo, содержащим порядковый номер

сообщения, с объектом Confirm, содержащим номер последнего принятого сообщения сервера и с объектом Source, содержащим источник данных;

- получив сообщение, отправляемое тахографом, сервер немедленно отправляет ответное сообщение с объектом SerialNo, содержащим порядковый номер сообщения, с объектом Confirm, содержащим номер принятого сообщения тахографа, с объектом Source и с объектом Payload/Payload_enc, содержащим подтверждение или запрос повторной передачи;

- при получении от сервера запроса повторной передачи данных тахограф формирует сообщение с данными, на которые не были получены подтверждения;

- при получении сообщения от сервера с подтверждением тахограф формирует следующие сообщение с данными БТИ или данными тахографа, если есть данные для передачи.

4.4.3.2 Сценарий выгрузки данных, подготовленных БТИ:

1) Тахограф считывает из БТИ значение текущего состояния БТИ (команда «Запрос статуса БТИ»);

2) Тахограф проверяет состояние БТИ. Если данные для выгрузки отсутствуют, завершение процедуры, повторное выполнение пункта через 2 минуты;

3) Если данные для выгрузки присутствуют, тахограф инкрементирует номер сообщения и формирует набор объектов TLV с объектом содержательных данных нулевой длины и без объекта имитовставки (таблица 25);

Т а б л и ц а 25 – Набор объектов TLV, формируемого тахографом, с объектом содержательных данных нулевой длины и без объекта имитовставки

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload/ Payload_enc	00	Содержательные данные
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения полученного отправителем данного или 0x00000000 для первого сообщения
…	…	…	…
0x1C	Diagnostic	1	Диагностические данные для сервера
0x1F	Source	1	Источник данных

4) Тахограф передает в БТИ сформированный набор объектов TLV в команде «Получение посылки для сервера» и получает в ответ набор объектов TLV с

содержательными данными (открытыми – тэг 0x20 или зашифрованными – тэг 0xA0) и объектом имитовставки, приведенным в таблице 26;

Т а б л и ц а 26 – Набор объектов TLV, сформированного БТИ

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload/ Payload_enc	до 4000	Данные БТИ
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения полученного отправителем данного или 0x00000000 для первого сообщения
..	..	..	..
0x1C	Diagnostic	1	Диагностические данные для сервера
0x1F	Source	1	Источник данных
0x1E	MAC	6	Имитовставка

5) Тахограф формирует сообщение MESSAGE (тэг 0x39 с данными, полученными от БТИ и заголовок);

6) Тахограф передает сообщение серверу и получает ответное сообщение;

7) Тахограф проверяет заголовок и структуру ответного сообщения, если обнаружена ошибка тахограф должен выполнить процедуру обработки ошибки (см. 4.2.4);

8) Тахограф передает в БТИ полученный набор объектов TLV в команде «Передача подтверждения сервера». Если команда выполнена успешно, то тахограф переходит к выгрузке следующего пакета данных, подготовленных БТИ.

9) Если от БТИ получен ответ с кодом ошибки, тахограф должен выполнить процедуру обработки ошибки (см. 4.2.4).

4.4.3.3 Сценарий выгрузки данных, подготовленных тахографом:

1) Если присутствуют данные, подготовленные тахографом, тахограф инкрементирует номер сообщения и формирует набор объектов TLV с объектом содержательных данных, подготовленных тахографом и без объекта имитовставки в соответствии с таблицей 27.

Т а б л и ц а 27 – Набор объектов TLV, формируемых тахографом, с объектом содержательных данных и без объекта имитовставки

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload/ Payload_enc	до 4000	Содержательные данные
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения полученного отправителем данного или 0x00000000 для первого сообщения
…	…	…	…
0x1C	Diagnostic	1	Диагностические данные для сервера
0x1F	Source	1	Источник данных

2) Тахограф передает в БТИ сформированный набор объектов TLV в команде «Получение посылки для сервера» и получает в ответ набор объектов TLV с содержательными данными (открытыми – тэг 0x20 или зашифрованными – тэг 0xA0) и объектом имитовставки, приведенным в таблице 28.

Т а б л и ц а 28 – Набор объектов TLV, подготовленного БТИ по команде «Получение посылки для сервера»

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload/ Payload_enc	до 4000	Данные, подготовленные тахографом
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения полученного отправителем данного или 0x00000000 для первого сообщения
…	…	…	…
0x1C	Diagnostic	1	Диагностические данные для сервера
0x1F	Source	1	Источник данных
0x1E	MAC	6	Имитовставка

3) Тахограф формирует соо бщение MESSAGE (тэг 0x39 с данными и заголовок);

4) Тахограф передает сообщение серверу и получает ответное сообщение;

5) Тахограф проверяет заголовок и структуру ответного сообщения, если обнаружена ошибка, то тахограф должен выполнить процедуру обработки ошибки (см. 4.2.4);

6) Тахограф передает в БТИ полученный набор объектов TLV в команде «Передача подтверждения сервера» (тип данных – данные сервера для тахографа). Если команда выполнена успешно, то тахограф переходит к формированию тела следующего сообщения;

7) Если от БТИ получен ответ с кодом ошибки, тахограф должен выполнить процедуру обработки ошибки (см. 4.2.4).

4.4.4 Повторная аутентификация

Сервер может потребовать от тахографа проведения повторной аутентификации.

Для повторной аутентификации сервер посылает сообщение DENYSESSION.

Тахограф также может потребовать от сервера проведения повторной аутентификации, послав сообщение CONNECTREQUEST. В заголовке сообщения поле ServerCTX заполняется значением поля ServerCTX, взятого из последнего полученного успешного ответа от сервера.

4.4.4.1 Схема запроса повторной аутентификации сервером приведена на рисунке 4.

	Тахограф		**Сервер**
Шаг1	MESSAGE (…)	⇨	
		⇦	DENYSESSION(…)
Шаг 2 Открытие сессии	ServerCTX ≠ 0 CONNECTREQUEST (…)	⇨	
		⇦	SERVERHELLO(…)
	CACERTREQUEST (…)	⇨	
		⇦	CACERTCHAIN (…)
	INITSESSION (…)	⇨	
		⇦	CONFIRMSESSION(…)
	При любой ошибке: Завершение обмена	⇦	При любой ошибке: DENYSESSION(…)
Шаг 3	Продолжение обмена на новых ключах MESSAGE(…)	⇨	
		⇦	Продолжение обмена на новых ключах MESSAGE(…)

Рисунок 4 – Обмен сообщениями при запросе сервером повторной аутентификации

4.4.4.2 Схема запроса повторной аутентификации тахографом приведена на рисунке 5.

	Тахограф		**Сервер**
Шаг1 Открытие сессии	ServerCTX ≠ 0 CONNECTREQUEST(…)	⇨	
		⇦	SERVERHELLO(…)
	CACERTREQUEST (…)	⇨	
		⇦	CACERTCHAIN(…)
	INITSESSION (…)	⇨	
		⇦	CONFIRMSESSION(…)
	При любой ошибке: Завершение обмена	⇦	При любой ошибке: DENYSESSION(…)
Шаг 2	Продолжение обмена на новых ключах MESSAGE(…)	⇨	
		⇦	Продолжение обмена на новых ключах MESSAGE(…)

Рисунок 5 – Обмен сообщениями при запросе тахографом повторной аутентификации

Приложение А
(справочное)

Справочник вычисления CRC16 и используемых тегов при обмене данными тахографа и сервера

А.1 Вычисление CRC16

Алгоритм идентичен CRC-A по ГОСТ Р ИСО/МЭК 14443-3-2014, за исключением стартового значения CRC (CRC_IV). CRC_IV = 0xA56C (байтовая последовательность: 0x6CA5).

Пример

Стартовое значение: CRC_IV = 0x6CA5

Входные данные: Input = 0x0A123456

Результат: CRC16 = 0x4832

А.2 Используемые тахографом и сервером Тэги при обмене данными приведены в таблице А.1.

Т а б л и ц а А.1 – Теги, используемые тахографом и сервером при обмене данными

Тэг	Наименование	Длина, байт	Примечание
Сообщения			
0x30	CONNECTREQUEST	-	Выдается тахографом сразу после установления соединения
0x31	SERVERHELLO	-	Выдается сервером при установлении сессии в ответ на CONNECTREQUEST или в качестве запроса на повторную аутентификацию
0x33	DENYSESSION	-	Выдается сервером в случае отказа установления/восстановления сессии
0x34	CACERTREQUEST	-	Выдается тахографом если у него нет ключа ДЦ
0x35	CACERTCHAIN	-	Выдается сервером в ответ на CACERTREQUEST
0x36	INITSESSION	-	Выдается тахографом для динамической аутентификации
0x37	CONFIRMSESSION	-	Выдается сервером в ответ на успешную динамическую аутентификацию
0x39	MESSAGE	-	Зашифрованные сообщения, защищенные имитовставкой
0x3A	PROMPT	-	Периодически выдается тахографом для согласования текущей частоты передачи запросов

Продолжение таблицы А.1

Тэг	Наименование	Длина, байт	Примечание
0x3B	SERVERREQUEST	-	Выдается сервером в ответ на PROMPT
0x31, 0x38. 0x3C-0x3E	RFU	-	Зарезервировано
Простые тэги для передачи данных в сообщениях при установлении соединения и аутентификации			
0x01	Certificate	до 3000	Сертификат
0x02	Server Address	до 199	Адрес (DNS-имя) сервера и другие идентификационные данные
0x03	Part Number	16	Заводской номер БТИ
0x04	KeyId	16	Идентификатор(ы) ключа проверки сертификата
0x05	Random	16	Случайное число
0x07	S	64	Криптограмма аутентификации БТИ
0x08	H	10	Текущее время сервера (4 байта) || Проверочная криптограмма сервера (6 байт)
0x09	ErrorCode	2	Код причины разрыва соединения
0x0A	Description	0-n	Описание причины разрыва соединения (короткое сообщение)
0x0B	Freq	4	Текущая частота передачи сообщений, с
0x0C	ServerRequest	4	Код процедуры/уведомления, запрашиваемого сервером. В случае передачи фиксированного значения, например 0, тахограф считает, что необходимости в оперативном общении с сервером нет
0x06, 0x0D-0x0F	RFU	-	Зарезервировано
Простые тэги для передачи протокольных данных в сообщениях с содержательными данными (MESSAGE)			
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения, полученного отправителем данного

Окончание таблицы А.1

0x12	RetransmitReq	0	Запрос повторной передачи данных предыдущего сообщения
0x13	IDProcessingSys	4	Код/идентификатор системы сбора и обработки данных
0x14	VPProcessingSys	1	Версия протокола обмена с системой сбора и обработки данных
0x15	UTISerial	16(32)	Заводской (заводской и регистрационный) номер БТИ
0x16-0x1B	RFU	-	Зарезервировано
0x1C	Diagnostic	1	Диагностические данные для сервера
0x1D	Priority	1	Уровень приоритета сообщения
0x1F	Source	1	Источник данных
Простой тэг для передачи имитовставки			
0x1E	MAC	6	Имитовставка вычисляется на все тэги в сообщении
Составные тэги для передачи содержательных данных			
0x20	Payload	n	Открытые данные, передаваемые в сообщении
0xA0	Payload_enc	n	Зашифрованные данные, передаваемые в сообщении

Приложение Б
(обязательное)

Технический регламент взаимодействия тахографов с ОТД по TCP/IP

Б.1 Установка TCP соединения.

В случае если у тахографа есть необходимость в передаче информации в ОТД или тестирования канала связи:

а) тахограф начинает процедуру TCP подключения. При неудачной попытке соединения выполняется процедура обработки ошибок (см. Б.4);

б) тестирование канала связи допускается при включении устройства и не чаще, чем один раз в час.

Б.2 Общие положения TCP соединения:

а) общий таймаут на TCP соединение (TCP_INACTIVITY_TO), по которому не передаются пользовательские данные в любом направлении – 595 с.;

б) при отсутствии передачи данных в течение 595 с, ОТД разрывает TCP соединение (см. Б3) и закрывает сессию ЗОС.

в) любая передача пользовательских данных обнуляет таймер TCP_INACTIVITY_TO;

г) минимальный таймаут на ожидание любого ответа от сервера на этапе установки ЗОС (SEC_CONN_INIT_READ_TO) – 5 с;

д) после открытия сессии ЗОС, тахограф посылает запросы в ОТД и получает ответы по каналу ЗОС. Время ожидания ответа от процессинга (SEC_CONN_DATA_RSP_READ_TO) – не менее 33 с.

Б.3 Управление разрывом TCP соединения:

а) если установленным TCP и ЗОС соединением тахограф не пользуется в течение TCP_INACTIVITY_TO, то тахограф должен сам инициировать разрыв TCP соединения со своей стороны, и не устанавливать нового соединения, если нет необходимости в этот момент передачи данных/запросов в ОТД (или тестирования канала связи);

Примечание – После разрыва соединения, тахограф должен выполнить процедуру завершения обмена с сервером.

б) если соединение было принудительно разорвано со стороны ОТД, и у тахографа нет необходимости в этот момент передаче данных/запросов в ОТД, то тахограф не должен инициировать восстановление TCP соединения;

в) если у тахографа есть необходимость в передаче информации, то ситуация с ошибкой передачи данных по TCP соединению в пределах TCP_INACTIVITY_TO трактуется как ошибка взаимодействия и дальше тахограф должен следовать процедуре обработки ошибок, изложенной в Б.4.

Б.4 Процедура обработки ошибок:

а) после возникновения ошибки по TCP, тахограф делает паузу в 3 с и пытается повторно (до трех раз) установить TCP соединение, с паузой в 3 с между попытками.

б) в случае невозможности подключения после трех попыток, тахограф разрывает соединение, делает паузу (RECONNECT_WAIT_TO) в 30 + random (1...60) с и если у тахографа есть необходимость в передаче информации в ОТД, то снова выполняет попытку подключения (см.Б.1). Если подключение по TCP/IP успешно, то тахограф продолжает обмен в соответствии с Б.2.

Примечание – После разрыва соединения тахограф должен выполнить процедуру завершения обмена с сервером.

Библиография

[1] Европейское соглашение, касающееся работы экипажей транспортных средств, производящих международные автомобильные перевозки (ЕСТР), и Протокол о подписании. Заключено в г. Женева 01.07.1970 г. (в ред. поправки № 6 от 20.09.2010).

УДК 629.3.01 ОКС 43.040.10

Ключевые слова: автомобильные транспортные средства, тахографы цифровые, протоколы обмена, информационная система, контроль

Генеральный директор ФГУП «НАМИ» Ф.Л. Назаров

Заместитель генерального директора
по техническому регулированию
ФГУП «НАМИ» С.А. Аникеев

Директор Центра «Стандартизация и
идентификация» ФГУП «НАМИ» П.Г. Шачнев

Президент Ассоциации
«Тахографический центр» А.Б. Архангельский

Нормоконтроль:
Начальник Управления «Стандартизация»
Центра «Стандартизация и
идентификация» ФГУП «НАМИ» Е.Е. Бобылева

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р
(проект, первая редакция)

Автомобильные транспортные средства

ТАХОГРАФЫ ЦИФРОВЫЕ

Протоколы обмена информацией с автоматизированной информационной системой тахографического контроля

Настоящий проект стандарта не подлежит применению до его утверждения

Москва
Российский институт стандартизации
202_

ГОСТ Р
(проект, первая редакция)

Предисловие

1 РАЗРАБОТАН Ассоциацией по содействию безопасности автотранспортной деятельности «Тахографический Центр» и Федеральным государственным унитарным предприятием «Центральный ордена Трудового Красного Знамени научно-исследовательский автомобильный и автомоторный институт «НАМИ» (ФГУП «НАМИ»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 056 «Дорожный транспорт»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от _____202_ г. №_____

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru).

Содержание

Введение

В настоящем стандарте рассматривается протокол передачи сообщений для систем сбора и обработки тахографических данных на цифровых тахографах.

Тахограф устанавливает соединение с сервером – обработчиком тахографических данных (далее – ОТД), которому передает сообщения, предназначенные для систем сбора и обработки данных.

Взаимодействие тахографа с ОТД осуществляется по TCP/IP протоколу. Обмен сообщениями с содержательными данными выполняется по каналу защищенного обмена (далее – ЗОС).

Все криптографические операции в тахографе выполняются блоком СКЗИ тахографа (далее БТИ – блок тахографической информации).

Структура и состав содержательных данных сообщений, предназначенные для систем сбора и обработки данных, в настоящем стандарте не рассматриваются.

ГОСТ Р
(проект, первая редакция)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Автомобильные транспортные средства
ТАХОГРАФЫ ЦИФРОВЫЕ
Протоколы обмена информацией с автоматизированной информационной системой тахографического контроля

Motor vehicles. Digital tachographs. Protocols of information exchange with the automated information system of tachographic control.

Дата введения — — —

1 Область применения

Настоящий стандарт устанавливает протоколы обмена информацией цифрового тахографа, устанавливаемого на автомобильные транспортные средства (далее – АТС), с автоматизированной информационной системой тахографического контроля, а также требования к технологическому процессу сбора и обработки данных.

Настоящий стандарт не распространяется на контрольные устройства, устанавливаемые на АТС в соответствии с требованиями [1].

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 14443-3 – 2014 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 3: Инициализация и антиколлизия

П р и м е ч а н и е – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом

утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Сокращения

В настоящем стандарте использованы следующие сокращения:

БТИ – блок тахографической информации;

ДЦ – доверенный центр;

ЗОС – защищенный обмен сообщениями;

ОТД – обработчик тахографических данных;

ФБУ – Федеральное бюджетное учреждение «Росавтотранс»;

TCP (TCP/IP) – протокол передачи данных Transmission Control Protocol и Internet Protocol;

|| – символ конкатенации;

0x – префикс для указания шестнадцатеричного числа.

4 Основные положения

4.1 Формат сообщений протокола

Сообщение протокола состоит из заголовка фиксированной длины и тела в формате информационного TLV объекта, тэгом которого является код типа сообщения.

4.1.1 Формат заголовка

Заголовок сообщения имеет фиксированную длину, равную 37 байт.

Структура заголовка сообщения приведена в таблице 1.

Т а б л и ц а 1 – Структура заголовка сообщения

Смещение	Длина, байт	Значение/Описание
00	4	Фиксированная константа – Magic, 0x41544C53
04	1	Версия транспортного протокола, 0x07
05	4	Код/идентификатор системы сбора и обработки данных
09	16	Заводской номер БТИ – Part Number, байтовый массив
25	2	Длина тела сообщения
27	8	Контекст ОТД – ServerCTX, байтовый массив
35	2	CRC16 тела сообщения (см. приложение А)

4.1.1.1 Поле «Код/идентификатор системы сбора и обработки данных»

В заголовке сообщения указывается 4-х байтовый код/идентификатор системы сбора и обработки данных, которому предназначено сообщение. Структура кода представлена в таблице 2.

Т а б л и ц а 2 – Структура кода системы сбора и обработки данных

Поле	Тип	Длина, байт	Значение/Описание
Code	uInt_16	2	Код/идентификатор системы 0xA085 – код системы регистрации 0xA087 – код системы сбора и обработки данных ФБУ
RFU	-	2	0x0000

Также код/идентификатор системы сбора и обработки данных указывается в теле содержательного сообщения.

В заголовке сообщений для ОТД (0x30 - 0x38) 4 байта кода/идентификатора имеют нулевое значение.

В заголовке и теле содержательного сообщения (0x39) с данными для ОТД 4 байта кода/идентификатора имеют нулевое значение.

В заголовке и теле содержательных сообщений (0x39) для системы сбора и обработки данных 4 байта кода/идентификатора имеют не нулевое значение.

В заголовке сообщений (0x3A, 0x3B) для системы сбора и обработки данных 4 байта кода/идентификатора имеют не нулевое значение

4.1.1.2 Поле «Контекст ОТД» (ServerCTX)

Поле ServerCTX позволяет восстановить на ОТД контекст обработки поступающих данных от тахографа в случае разрыва TCP/IP соединения и последующего его восстановления.

При формировании сообщения (кроме запроса CONNECTREQUEST) поле ServerCTX инициализируется значением ServerCTX, полученным из последнего ответа от сервера.

Если после получения успешного ответа на запрос произошел разрыв TCP/IP соединения (или если нет ответов на запросы, что приводит к разрыву TCP/IP соединения), то тахограф заново подключается по TCP/IP к серверу и посылает следующее сообщение, со значением поля ServerCTX, полученного из последнего успешного ответа от сервера.

Сообщение CONNECTREQUEST формируется следующим образом:

1) поле ServerCTX для запроса CONNECTREQUEST заполняется байтами со значением 0x00 в следующих случаях:

- значение поля ServerCTX из последнего полученного успешного ответа от сервера неизвестно;

- интервал в обмене с ОТД больше 10 минут;

- по тем или иным причинам необходимо заново проинициализировать контекст обработки данных на ОТД;

2) в остальных случаях поле ServerCTX для запроса CONNECTREQUEST заполняется значением поля ServerCTX, взятого из последнего полученного успешного ответа от сервера.

4.1.2 Информационный объект TLV

Каждый объект TLV должен состоять из двух или трех последовательных полей: обязательного поля тега, обязательного поля длины и условного поля значения. Кодировка поля тэгов приведена в таблице 3.

Поле тега состоит из одиночного байта, кодирующего номер тега от 1 до 254. Значения '00' и 'FF' являются недействительными для поля тега.

Т а б л и ц а 3 – Кодировка поля тэгов

b8	b7	b6	b5	b4	b3	b2	b1	Описание
0	0	1	1	-	-	-	-	Сообщение. Структурированное кодирование, т.е. поле значения кодировано в TLV
0	0	0	1	-	-	-	-	Протокольные данные, передаваемые в сообщениях с содержательными данными
0	0	1	0	-	-	-	-	Открытые содержательные данные, передаваемые в сообщениях с содержательными данными
1	0	1	0	-	-	-	-	Зашифрованные содержательные данные, передаваемые в сообщениях с содержательными данными
0	0	0	0	-	-	-	-	Данные, передаваемые в сообщениях при установлении соединения и аутентификации
-	-	-	-	x	x	x	x	Номер тэга

Поле длины состоит из одного или большего числа последовательных байтов. Кодирование этих байтов должно соответствовать основным правилам кодирования ASN.1 и определению в таблице 4.

В коротком формате поле длины состоит из единичного байта, в котором бит 8 установлен в состояние 0, а биты с 7 по 1 кодируют число байтов в поле значения. Таким образом одним байтом может быть закодировано любое число от нуля до 127.

В длинном формате поле длины состоит из двух или более байтов.

Поля длины TLV объектов приведены в таблице 4.

Таблица 4 – Поля длины TLV объектов и правила кодирования

Диапазон	Байт	1 байт	2 байт	3 байт
От 0 до 127	1 байт	От '00' до 7F'	-	-
От 0 до 255	2 байта	'81'	От '00' до 'FF'	-
От 0 до 65535	3 байта	'82'	От '0000' до 'FFFF'	

Если поле длины равно нулю, то поле значения отсутствует, т.е. объект является пустым. В противном случае, если объект простой, поле значения состоит из последовательных байтов; если объект структурированный, поле значения состоит из набора простых TLV объектов.

4.1.3 Типы сообщений

Типы сообщений приведены в таблице 5.

Т а б л и ц а 5 – Типы сообщений

Тэг	Название	Примечание
0x30	CONNECTREQUEST	Выдается тахографом сразу после установления соединения
0x31	SERVERHELLO	Выдается сервером при установлении сессии или в качестве запроса на повторную аутентификацию
0x33	DENYSESSION	Выдается сервером в случае разрыва соединения и/или закрытия сессии ЗОС по инициативе сервера
0x34	CACERTREQUEST	Выдается тахографом, если у него нет сертификата ДЦ
0x35	CACERTCHAIN	Выдается сервером в ответ на CACERTREQUEST
0x36	INITSESSION	Выдается тахографом для динамической аутентификации
0x37	CONFIRMSESSION	Выдается сервером в ответ на успешную динамическую аутентификацию
0x39	MESSAGE	Зашифрованные сообщения, защищенные имитовставкой. (Данные в сообщении могут быть не зашифрованы)
0x3A*	PROMPT	Периодически выдается тахографом для согласования текущей частоты передачи запросов
0x3B*	SERVERREQUEST	Выдается сервером в ответ на PROMPT
* Опционально		

4.1.4 Формат тела сообщений

4.1.4.1 CONNECTREQUEST

Тэг 0x30, выдается тахографом сразу после установления соединения. Состоит из набора объектов TLV, приведенных в таблице 6.

Т а б л и ц а 6 – Набор объектов TLV, выдаваемых тахографом сразу после установления соединения

Тэг	Наименование	Длина, байт	Количество	Примечание
0x02	Server Address	n	0/1	Адрес (DNS-имя) сервера
0x03	Part Number	16	1	Заводской номер БТИ
0x04	KeyId	16	1	Идентификатор открытого ключа БТИ
0x05	Random	16	1	Случайное число БТИ
0x06	RFU	4	1	0x00000000

4.1.4.2 SERVERHELLO

Тэг 0x31, выдается сервером сразу после получения запроса на установление соединения или в ходе установленной сессии с целью проведения повторной динамической аутентификации. Состоит из набора объектов TLV, приведенных в таблице 7.

Т а б л и ц а 7 – Набор объектов TLV, выдаваемых сервером сразу после получения запроса на установление соединения или в ходе установленной сессии

Тэг	Наименование	Длина, байт	Количество	Примечание
0x01	Certificate	до 3000	1	Сертификат сервера
0x05	Random	16	1	Случайное число сервера

4.1.4.3 DENYSESSION

Тэг 0x33, выдается сервером в случае разрыва соединения, сессии ЗОС. Состоит из набора объектов TLV приведенных в таблице 8.

Т а б л и ц а 8 – Набор объектов TLV, выдаваемых сервером в случае разрыва соединения

Тэг	Наименование	Длина, байт	Количество	Примечание
0x09	ErrorCode	2	1	Код причины разрыва соединения.
0x0A	Description	0-n	1	Описание причины разрыва соединения (короткое сообщение)

4.1.4.4 CACERTREQUEST

Тэг 0x34, выдается тахографом, если у него нет открытого ключа ДЦ для проверки сертификата сервера. Сообщение содержит объекты TLV с идентификаторами ключей ДЦ известных БТИ (см. таблицу 9).

Т а б л и ц а 9 – Набор объектов TLV, выдаваемых тахографом, если у него нет открытого ключа ДЦ для проверки сертификата сервера

Тэг	Наименование	Длина, байт	Количество	Примечание
0x04	KeyId	16	1 и более	Идентификатор ключа ДЦ

4.1.4.5 CACERTCHAIN

Тэг 0x35, выдается сервером в ответ на сообщение тахографа - CACERTREQUES. Сообщение содержит объекты TLV с сертификатами ДЦ, составляющими цепочку сертификатов, которые необходимо передать в БТИ в том порядке, в каком они присланы сервером (см. таблицу 10).

Т а б л и ц а 10 – Набор объектов TLV, выдаваемых сервером в ответ на сообщение тахографа - CACERTREQUES

Тэг	Наименование	Длина, байт	Количество	Примечание
0x01	Certificate	до 3000	1 и более	Сертификат ДЦ (Передаются в том порядке, в котором должны быть переданы в БТИ на проверку)

4.1.4.6 INITSESSION

Тэг 0x36, выдается тахографом для динамической аутентификации. Состоит из набора объектов TLV, приведенных в таблице 11.

Т а б л и ц а 11 – Набор объектов TLV, выдаваемых тахографом для динамической аутентификации

Тэг	Наименование	Длина, байт	Количество	Примечание
0x01	Certificate	до 3000	1	Сертификат открытого ключа БТИ
0x05	Random	16	1	Случайное число БТИ
0x07	S	64	1	Криптограмма БТИ

4.1.4.7 CONFIRMSESSION

Тэг 0x37, выдается сервером в ответ на сообщение тахографа INITSESSION для динамической аутентификации (см. таблицу 12).

Т а б л и ц а 12 – Набор объектов TLV, выдаваемых сервером в ответ на сообщение тахографа INITSESSION

Тэг	Наименование	Длина, байт	Количество	Примечание
0x08	H	10	1	Текущее время сервера (4 байта) || Проверочная криптограмма сервера (6 байт)

4.1.4.8 PROMPT

Тэг 0x3A, периодически выдается тахографом для согласования текущей частоты передачи данных. Состоит из набора объектов TLV, приведенных в таблице 13:

Т а б л и ц а 13 – Набор объектов TLV, выдаваемых тахографом для согласования текущей частоты передачи данных

Тэг	Наименование	Длина, байт	Количество	Примечание
0x03	Part Number	16	0/1	Заводской номер БТИ
0x0B	Freq	4	1	Текущая частота передачи сообщений

4.1.4.9 SERVERREQUEST

Тэг 0x3B, выдается сервером в ответ на сообщение PROMPT. Состоит из набора объектов TLV, приведенных в таблице 14.

Т а б л и ц а 14 – Набор объектов TLV, выдаваемых сервером в ответ на сообщение тахографа PROMPT

Тэг	Наименование	Длина, байт	Количество	Примечание
0x03	Part Number	16	0/1	Заводской номер БТИ
0x0B	Freq	4	1	Текущая частота передачи сообщений
0x0C	ServerRequest	4	1	Код процедуры/уведомления, запрашиваемого сервером. В случае передачи фиксированного значения (например 0) тахограф считает, что необходимости в оперативном общении с сервером нет

4.1.4.10 MESSAGE

Тэг 0x39, выдается сервером и тахографом. Используется для передачи содержательных данных в открытом или зашифрованном виде. Состоит из набора объектов TLV, приведенных в таблице 15.

Т а б л и ц а 15 – Набор объектов TLV, выдаваемых сервером и тахографом при обмене содержательными данными

Тэг	Наименование	Длина, байт	Количество	Примечание
0x20	Payload	до 4000	0 - если есть 0xA0 1 - если нет	Открытые содержательные данные. Если в сообщении нет содержательных данных, должен присутствовать это объект нулевой длины
0xA0	Payload_enc	до 4000	0 - если есть 0x20 1 - если нет	Зашифрованные содержательные данные. Если в сообщении нет содержательных данных, должен присутствовать это объект нулевой длины
0x10	SerialNo*	4	1	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	1	Номер последнего сообщения, полученного отправителем данного
0x12	RetransmitReq	1	0-1	Запрос повторной передачи данных предыдущего сообщения с кодом причины запроса
0x13	IDProcessingSys	4	0-1	Код/идентификатор системы сбора и обработки данных
0x14	VPProcessingSys	1	0-1	Версия протокола обмена с системой сбора и обработки данных
0x15	UTISerial	16(32)	0-1	Заводской (заводской и регистрационный) номер БТИ
0x1C	Diagnostic	1	0-1	Диагностические данные для сервера
0x1D	Priority	1	0-1	Уровень приоритета сообщения
0x1F	Source	1	1	Источник данных
0x1E	MAC	6	1	Имитовставка

4.1.4.10.1 Объект SerialNo

Тахограф ведет непрерывный учет сформированных сообщений. Каждому сформированному сообщению присваивается последовательный порядковый номер. При обрыве и восстановлении или установлении нового соединения нумерация продолжается.

Для сервера допускается ведение непрерывного учета сформированных ответных сообщений только в течение установленного соединения. Нумерация сохраняется при обрыве сессии с восстановлением и при повторной динамической аутентификации. При установлении нового соединения нумерация может начаться заново.

4.1.4.10.2 Объект Source

Сообщение содержит обязательный объект источника содержательных данных

сообщения.

В объекте источника содержательных данных сообщения сервер может передать запрос на передачу данных БТИ или тахографу.

Кодировка источника данных приведена в таблице 16.

Т а б л и ц а 16 – Кодировка источника данных в сообщении, передаваемом тахографом или сервером

b8-b5	b4	b3	b2	b1	Источник
0	0	0	0	x	0 – Данные блока/для блока тахографической информации 1 – Данные тахографа/для тахографа
0	0	0	1	0	Запрос сервера на передачу данных тахографу
0	0	1	0	0	Запрос сервера на передачу данных блоку тахографической информации
0	1	0	0	0	Устройства контроля состояния водителя

4.1.4.10.3 Объект Priority

Сообщение может содержать необязательный объект приоритета, имеющий значение от 0 до 255. Если в сообщении отсутствует объект приоритета, оно считается имеющим приоритет 0 (не приоритетно).

4.1.4.10.4 Объекты содержательных данных сообщения

Сообщение содержит обязательный объект с содержательными данными сообщения. Данные, подготовленные БТИ, тахографом или сервером передаются в открытом виде в объекте TLV с тэгом 0x20 или в зашифрованном виде в объекте TLV с тэгом 0xA0. Длина объекта не более 4000 байт

4.1.5 Формирование сообщения MESSAGE

При формировании сообщения выполняются следующие действия:

1) Формирование содержательных данных сообщения;

2) Формирование набора объектов TLV сообщения

3) Формирование тела сообщения: к полученному набору добавляется тэг(0x39) и длина;

4) Формирование сообщения: к телу сообщения добавляется заголовок и в таком виде сообщение передается на сервер/тахограф.

4.1.5.1 Формирование набора объектов TLV тела сообщения MESSAGE

4.1.5.1.1 Набор объектов TLV сообщения MESSAGE, подготовленного тахографом

Если данные для выгрузки присутствуют, тахограф формирует набор объектов TLV с открытыми – тэг 0x20 или зашифрованными – тэг 0xA0 содержательными данными, приведенными в таблице 17.

Т а б л и ц а 17 – Набор объектов TLV сообщения MESSAGE, сформированного тахографом

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload	до 4000	Содержательные данные, подготовленные БТИ
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения полученного отправителем данного или 0x00000000 для первого сообщения
0x13	IDProcessingSys	4	Код/идентификатор системы сбора и обработки данных
0x14	VPProcessingSys	1	Версия протокола обмена с системой сбора и обработки данных
0x15	UTISerial	16(32)	Заводской (заводской и регистрационный) номер БТИ
0x1C	Diagnostic	1	Диагностические данные для сервера
0x1F	Source	1	Источник данных: 0 – БТИ, 1 – тахограф. По умолчанию – 0
0x1E	MAC	6	Имитовставка

4.1.5.1.2 Набор объектов TLV сообщения MESSAGE, подготовленного сервером

Сервер формирует набор объектов TLV с подтверждением с открытыми – тэг 0x20 или зашифрованными – тэг 0xA0 данными, приведенными в таблице 18.

Т а б л и ц а 18 – Набор объектов TLV сообщения MESSAGE, сформированного сервером

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload/ Payload_enc	до 4000	Содержательные данные с подтверждением
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения полученного от тахографа
0x13	IDProcessingSys	4	Код/идентификатор системы сбора и обработки данных
0x14	VPProcessingSys	1	Версия протокола обмена с системой сбора и обработки данных
0x15	UTISerial	16(32)	Заводской (заводской и регистрационный) номер БТИ
0x1F	Source	1	Источник данных
0x1E	MAC	6	Имитовставка

4.1.5.2 Формирование тахографом сообщения MESSAGE осуществляется в следующем порядке:

1) Формируется набор объектов TLV без объекта содержательных данных и без объекта имитовставки.

Каждому сформированному набору присваивается порядковый номер. При обрыве и восстановлении или установлении нового соединения нумерация продолжается.

2) Формируется объект содержательных данных сообщений:

- если тахограф формирует сообщение с данными БТИ, объект содержательных данных Payload / Payload_enc формируется нулевой длины;

- если тахограф формирует сообщение с собственными данными, объект содержательных данных Payload/Payload_enc формируется с данными, подготовленными тахографом.

3) Сформированный набор объектов TLV передается БТИ в команде «Получение посылки для сервера».

4) Получив сформированный набор объектов TLV, БТИ выполняет следующие действия:

- если тип данных «данные подготовленные БТИ» и объект с тэгом содержательных данных пуст, формируются содержательные данные;

- если установлен признак шифрования, переданные или сформированные содержательные данные шифруются;

- значение объекта содержательных данных модифицируется в соответствии с выполненными операциями;

- вычисляется имитовставка на весь набор объектов тела сообщения и формируется объект имитовставки;

- переформированный набор объектов выдается в ответ на команду.

5) Формируется тело сообщения: к полученному набору объектов TLV добавляется тэг(0x39) и длина;

6) Формируется сообщение: к телу сообщения добавляется заголовок, после чего сообщение передается на сервер.

4.1.5.3 Разбор сообщения MESSAGE осуществляется в следующем порядке:

1) Из тела сообщения извлекается набор объектов TLV и проверяется его корректность.

В принятом с сервера сообщении должен содержаться объект SerialNo, содержащий последовательный номер сообщения, отправленного сервером и объект

Confirmed, содержащий последовательный номер полученного от тахографа сообщения.

2) Набор объектов TLV передается БТИ в команде «Передача подтверждения сервера».

3) Получив набор объектов TLV тела сообщения, БТИ выполняет следующие действия:

- отделяет объект имитовставки;

- выполняет проверку имитовставки;

- извлекает объект содержательных данных;

- извлекает шифротекст и выполняет расшифровывание, если установлен признак шифрования.

- выполняется регистрация подтверждения, если в объекте содержательных данных передается подтверждение получения данных БТИ, данные в ответ на команду не выдаются.

- открытые данные выдаются в ответ на команду вместе с тегом и длиной, если в объекте содержательных данных передаются данные для тахографа.

4) Если при разборе тела сообщения обнаружена ошибка, тахограф должен выполнить процедуру обработки ошибки или повторить передачу данных в следующем по порядку сообщении.

4.2 Процедуры протокола

4.2.1 Инициализация обмена с сервером осуществляется при выполнении следующих условий:

1) обмен с сервером не инициализирован (обмен с сервером завершен, включение питания);

2) у тахографа есть необходимость в передаче информации в систему сбора и обработки данных.

Процедура включает следующие действия:

1) тахограф устанавливает TCP-соединение с сервером в соответствии с техническим регламентом (приложение Б);

2) тахограф выполняет процедуру открытия сессии ЗОС.

4.2.2 Завершение обмена с сервером выполняется в следующих случаях:

1) в случае разрыва соединения в соответствии с техническим регламентом (приложение Б):

- отсутствие обмена в пределах таймаута (≥ 595 с отсутствуют данные для передачи, нет ответа сервера);

- отсутствие TCP-соединение более 10 мин при попытке восстановления соединения после возникновения ошибки по TCP.

2) ошибка при открытии сессии ЗОС (ошибка аутентификации), ошибка ЗОС.

Процедура включает следующие действия:

- тахограф разрывает TCP-соединение;

-тахограф удаляет контекст обмена, хранящийся в оперативной памяти (сеансовые ключи, контекст ОТД (ServerCTX) и др.).

3) тахограф подает в БТИ команду «Завершение обмена с сервером».

4.2.3 Обмен сообщениями

После инициализации обмена с сервером обмен сообщениями выполняется в соответствии с техническим регламентом по приложению Б и протоколом сессии ЗОС (см. 4.4).

4.2.4 Обработка ошибок

В процессе обмена возможны следующие исключительные ситуации:

- разрыв TCP-соединение более 10 мин, то в этой ситуации выполняется процедура завершения обмена (см. 4.2.2);

- ошибка взаимодействия по TCP (разрыв TCP-соединение менее 595 с и другие), то в этой ситуации после восстановления соединения обмен продолжается в рамках ранее открытой сессии ЗОС (см. 4.4.2.2);

- ошибка аутентификации, то в этой ситуации выполняется процедура завершения обмена (см. 4.2.2);

- ошибка ЗОС (ошибка MAC, некорректный набор объектов TLV, превышен лимит использования сеансовых ключей), то в этой ситуации выполняется процедура повторной аутентификации (см. 4.4.4);

- ошибка взаимодействия с БТИ, то в этой ситуации выполняется процедура завершения обмена (раздел 4.2.2)

4.3 Открытие сессии защищенного обмена сообщениями

Процедура открытия сессии выполняется в рамках процедуры инициализации обмена с сервером или процедуры повторной аутентификации и включает следующие действия:

1) тахограф формирует и отправляет сообщение с запросом на открытие сессии ЗОС и получает от сервера ответное сообщение с подтверждением, в котором передается сертификат открытого ключа сервера;

2) если у тахографа нет ключей для проверки сертификата, тахограф формирует и отправляет сообщение с запросом сертификатов и получает ответное сообщение;

3) тахограф инициирует процедуру аутентификации с сервером. Тахограф формирует и отправляет сообщение с криптограммой и получает ответное сообщение с проверочной криптограммой сервера;

4) в случае успешной проверки криптограммы сервера сессия считается установленной и тахограф переходит к передаче подготовленных данных.

4.3.1 Схема открытия сессии приведена на рисунке 1.

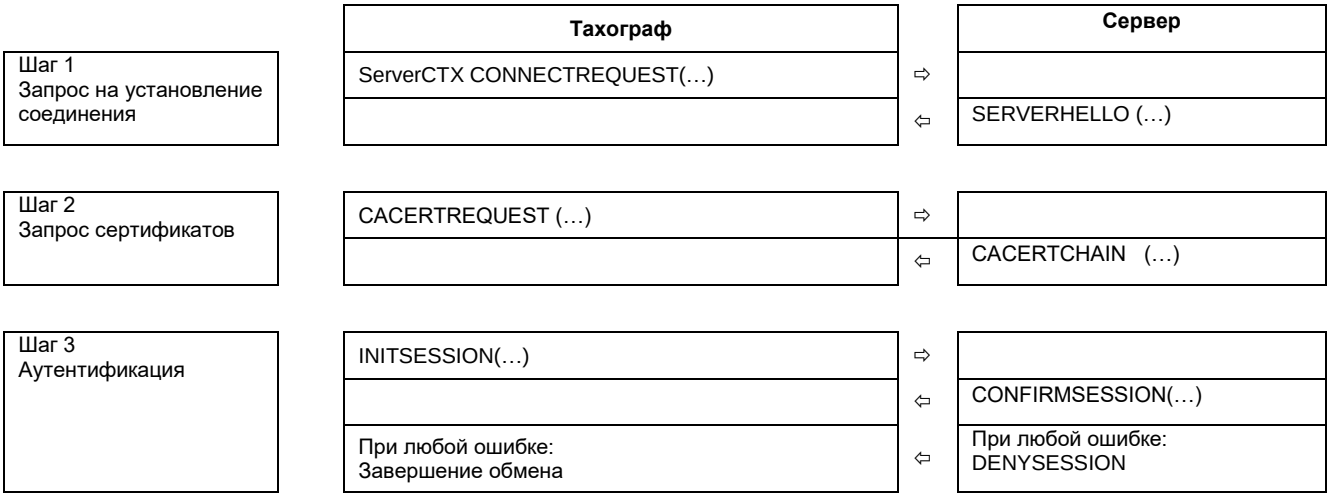

Рисунок 1 – Открытие сессии передачи тахографом подготовленных данных

4.3.2 Сценарий открытия сессии:

1) тахограф запрашивает у БТИ значение текущего состояния БТИ и статус выгрузки документов в команде «Запрос статуса БТИ».

Операции по выгрузке допустимы только в случае, если БТИ функционален.

2) тахограф формирует сообщение CONNECTREQUEST:

- считывает данные для передачи серверу (адрес (DNS-имя) сервера или другие идентификационные данные);

- запрашивает у БТИ данные активации БТИ в команде «Запрос данных активации БТИ». В ответ получает идентификационные данные БТИ, включая заводской номер БТИ;

- запрашивает у БТИ идентификаторы ключей. В ответ получает идентификатор ключа БТИ и идентификаторы ключей ДЦ известных БТИ;

- вырабатывает случайное число;

- формирует тело сообщения.

Тело сообщения CONNECTREQUEST приведено в таблице 19.

Т а б л и ц а 19 – Набор объектов TLV сообщения CONNECTREQUEST

Тэг	Наименование	Длина, байт	Количество	Примечание
0x02	Server Address	n	0/1	Адрес (DNS-имя) сервера
0x03	Part Number	16	1	Заводской номер БТИ
0x04	KeyId	16	1	Идентификатор открытого ключа БТИ
0x05	Random	16	1	Случайное число
0x06	RFU	4	1	0x00000000

3) тахограф формирует заголовок сообщения (см. 4.1.1) и передает сообщение CONNECTREQUEST серверу.

П р и м е ч а н и е – Если открытие сессии выполняется в рамках процедуры инициализации обмена, поле ServerCTX в заголовке заполняется байтами со значением 0x00. Если открытие сессии выполняется в рамках процедуры повторной аутентификации, поле заполняется значением поля ServerCTX, взятого из последнего полученного успешного ответа от сервера.

4) тахограф получает ответное сообщение SERVERHELLO.

Тело ответного сообщения SERVERHELLO приведено в таблице 20.

Таблица 20 – Набор объектов TLV сообщения SERVERHELLO

Тэг	Наименование	Длина, байт	Количество	Примечание
0x01	Certificate	до 3000	1	Сертификат сервера
0x05	Random	16	1	Случайное число сервера

Если полученное сообщение не SERVERHELLO, выполняется процедура завершения обмена (см. 4.2.2)

5) тахограф проверяет заголовок и структуру ответного сообщения. Если обнаружена ошибка, выполняется процедура завершения обмена (см. 4.2.2).

6) если открытие сессии выполняется в рамках процедуры инициализации обмена с сервером, тахограф подает в БТИ команду «Инициализация обмена с сервером».

7) тахограф извлекает из сообщения сертификат и передает его БТИ в команде «Предварительная проверка сертификата сервера».

БТИ:

- извлекает из сертификата поле CommonName;

- извлекает идентификатор ключа ДЦ для проверки сертификата и выполняет поиск ключа с идентификатором из сертификата в списке доверенных ключей ДЦ БТИ;

- выдает в ответ:

- итог поиска идентификатора ключа ДЦ, извлеченного из сертификата (ключ найден или ключ не найден);

- поле CommonName.

8) тахограф сравнивает CommonName с адресом (DNS-именем) сервера, использованным для установления соединения.

Если поле CommonName не совпадает с тем именем/адресом сервера, которое использовалось для установления соединения, выполняется процедура завершения обмена (см. 4.2.2).

9) если результат поиска – ключ известен БТИ, то переход к подпункту 13).

10) если результат поиска – ключ не известен БТИ, тахограф формирует сообщение CACERTREQUEST (см. 4.1.3.4), в которое включает идентификаторы ключей ДЦ, полученные от БТИ.

Тело сообщения CACERTREQUEST приведено в таблице 21.

Т а б л и ц а 21 – Набор объектов TLV сообщения CACERTREQUEST

Тэг	Наименование	Длина, байт	Примечание
0x04	Key ID	16	Идентификатор открытого ключа ДЦ для проверки сертификата БТИ
…	…..		…..
0x04	Key ID	16	Идентификатор открытого ключа ДЦ для проверки сертификата ДЦ

11) тахограф передает сообщение CACERTREQUEST серверу и получает ответное сообщение CACERTCHAIN с цепочкой сертификатов.

Тело ответного сообщения CACERTCHAIN приведено в таблице 22.

Т а б л и ц а 22 – Набор объектов TLV сообщения CACERTCHAIN

Тэг	Наименование	Длина, байт	Примечание
0x01	Certificate	до 3000	Сертификат ключа ДЦ для проверки следующего сертификата ДЦ
….		…..	
0x01	Certificate	до 3000	Сертификат ключа ДЦ для проверки сертификата сервера

Если не получено сообщение CACERTCHAIN, выполняется процедура завершения обмена (см. 4.2.2).

12) если получено сообщение CACERTCHAIN с цепочкой сертификатов, тахограф передает в БТИ сертификаты в том порядке, в каком они присланы сервером в команде «Проверка сертификата сервера».

Если проверка не успешна, выполняется процедура завершения обмена (см. 4.2.2).

13) тахограф передает в БТИ сертификат сервера, переданный в сообщении SERVERHELLO, в команде «Проверка сертификата сервера»;

Если проверка не успешна, выполняется процедура завершения обмена (см. 4.2.2).

14) если проверка успешна, запрашивает у БТИ сертификат БТИ в команде «Запрос сертификата ключа аутентификации БТИ»;

15) тахограф вызывает команду формирования криптограммы динамической аутентификации «Получение криптограммы БТИ», передавая туда случайное число, полученное от сервера в сообщении SERVERHELLO.

В ответ на команду БТИ выдает криптограмму и свое случайное число.

16) тахограф формирует сообщение INITSESSION (см. 4.1.3.6), в которое включает данные, полученные от БТИ.

Тело сообщения INITSESSION приведено в таблице 23.

Т а б л и ц а 23 – Набор объектов TLV сообщения INITSESSION

Тэг	Наименование	Длина, байт	Примечание
0x01	Certificate	до 3000	Сертификат открытого ключа БТИ
0x05	Random	16	Случайное число БТИ
0x07	S	80	Криптограмма

17) тахограф передает сообщение INITSESSION серверу и получает ответное сообщение CONFIRMSESSION

Тело ответного сообщения CONFIRMSESSION приведено в таблице 24.

Т а б л и ц а 24 – Набор объектов TLV сообщения CONFIRMSESSION

Тэг	Наименование	Длина, байт	Примечание
0x08	H	10	Текущее время сервера (4 байта) || Проверочная криптограмма сервера (6 байт)

Если не получено сообщение CONFIRMSESSION, выполняется процедура завершения обмена (см. 4.2.2).

18) если получено сообщение CONFIRMSESSION, тахограф вызывает команду «Проверка криптограммы сервера».

Если проверка не успешна, выполняется процедура завершения обмена (см. 4.2.2).

19) если проверка успешна, тахограф начинает выгрузку данных (см. 4.4.3.2).

4.4 Протокол сессии ЗОС

4.4.1 После открытия сессии тахограф отправляет на сервер подготовленные данные, в том числе:

- данные, которые были отправлены в ходе предыдущей сессии, но подтверждение не было получено до разрыва соединения;

- данные, которые были сформированы в период отсутствия связи.

4.4.2 Протокол сессии состоит из упорядоченного обмена сообщениями между тахографом и сервером в соответствии с техническим регламентом (приложение Б).

В ходе установленной сессии тахограф может отправлять на сервер следующие сообщения:

- защищенное имитовставкой сообщение MESSAGE, содержащие зашифрованные/открытые данные;

- сообщение CONNECTREQUEST, инициирующее повторную аутентификацию.

Сервер может отправлять тахографу в ответ на полученное сообщение:

- защищенное имитовставкой сообщение MESSAGE, содержащие зашифрованные/открытые данные (подтверждение);

- сообщение DENYSESSION о закрытии текущей сессии ЗОС.

4.4.2.1 Обмен указанными сообщениями осуществляется в следующем порядке:

1) Тахограф формирует и отправляет сообщение MESSAGE.

2) Сервер, получив сообщение, отправленное тахографом, отправляет ответное сообщение MESSAGE с подтверждением в соответствии с техническим регламентом (приложение Б).

Если при проверке сервером принятого сообщения тахографа не сошлась имитовставка или набор объектов TLV некорректен, сервер посылает сообщение DENYSESSION о закрытии сессии ЗОС (запрос на повторную аутентификацию).

3) Тахограф, после получения ответного сообщения от сервера (с подтверждением) формирует следующие сообщения с данными, на которые не получено подтверждение.

4) Если при проверке БТИ принятого сообщения сервера не сошлась имитовставка или набор объектов TLV некорректен, тахограф выполняет процедуру

обработки ошибки и посылает сообщение CONNECTREQUEST, инициирующее открытие новой сессии ЗОС (повторную аутентификацию).

5) Получив сообщение DENYSESSION, тахограф выполняет процедуру обработки ошибки и посылает сообщение CONNECTREQUEST, инициирующее открытие сессии ЗОС.

Схема обмена сообщениями приведена на рисунке 2.

	Тахограф		Сервер
1	Выдача данных MESSAGE(n, Data_n)	⇨	
		⇦	Передача квитанции MESSAGE(m, ack_ Data_n _m)
2	Выдача данных MESSAGE(n+1, Data_n+1)	⇨	
		⇦	Передача квитанции MESSAGE(m+1, ack_ Data_n+1 _m+1)
3	Выдача данных MESSAGE(n+2, Data_n+2)	⇨	
		⇦	Передача квитанции MESSAGE(m+2, ack_ Data_n+2 _m+2)
…	…	⇨	
		⇦	…
q	Выдача данных MESSAGE(n+q, Data_n+q)	⇨	
		⇦	Передача квитанции MESSAGE(m+q, ack_ Data_n+q _m+q)
	При ошибке ЗОС: Повторная аутентификация	⇦	При любой ошибке: DENYSESSION(…)

Рисунок 2 – Схема обмена сообщениями тахографа и сервера

4.4.2.2 Схема обмена после устранения ошибки взаимодействия по TCP приведена на рисунке 3.

	Тахограф		Сервер
Шаг 1 Продолжение обмена	ServerCTX≠ 0 MESSAGE(…)	⇨	
		⇦	а) Если сессия восстановлена (восстановлен контекст обработки поступающих данных, ошибки ЗОС отсутствуют) MESSAGE(…)
Шаг 2а) Продолжение обмена	MESSAGE(…)	⇨	
		⇦	MESSAGE(…)
Шаг 2б) Запрос повторной аутентификации		⇦	б) Если восстановление невозможно, DENYSESSION(…)

Рисунок 3 – Схема обмена сообщениями тахографа и сервера после обработки ошибки

4.4.3 Процедура выгрузки данных из тахографа

4.4.3.1 Выгрузка данных осуществляется в следующем порядке:

- тахограф формирует сообщение с объектом Payload/Payload_enc, содержащими данные БТИ или тахографа, с объектом SerialNo, содержащим порядковый номер

сообщения, с объектом Confirm, содержащим номер последнего принятого сообщения сервера и с объектом Source, содержащим источник данных;

- получив сообщение, отправляемое тахографом, сервер немедленно отправляет ответное сообщение с объектом SerialNo, содержащим порядковый номер сообщения, с объектом Confirm, содержащим номер принятого сообщения тахографа, с объектом Source и с объектом Payload/Payload_enc, содержащим подтверждение или запрос повторной передачи;

- при получении от сервера запроса повторной передачи данных тахограф формирует сообщение с данными, на которые не были получены подтверждения;

- при получении сообщения от сервера с подтверждением тахограф формирует следующие сообщение с данными БТИ или данными тахографа, если есть данные для передачи.

4.4.3.2 Сценарий выгрузки данных, подготовленных БТИ:

1) Тахограф считывает из БТИ значение текущего состояния БТИ (команда «Запрос статуса БТИ»);

2) Тахограф проверяет состояние БТИ. Если данные для выгрузки отсутствуют, завершение процедуры, повторное выполнение пункта через 2 минуты;

3) Если данные для выгрузки присутствуют, тахограф инкрементирует номер сообщения и формирует набор объектов TLV с объектом содержательных данных нулевой длины и без объекта имитовставки (таблица 25);

Т а б л и ц а 25 – Набор объектов TLV, формируемого тахографом, с объектом содержательных данных нулевой длины и без объекта имитовставки

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload/ Payload_enc	00	Содержательные данные
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения полученного отправителем данного или 0x00000000 для первого сообщения
…	…	…	…
0x1C	Diagnostic	1	Диагностические данные для сервера
0x1F	Source	1	Источник данных

4) Тахограф передает в БТИ сформированный набор объектов TLV в команде «Получение посылки для сервера» и получает в ответ набор объектов TLV с

содержательными данными (открытыми – тэг 0x20 или зашифрованными – тэг 0xA0) и объектом имитовставки, приведенным в таблице 26;

Т а б л и ц а 26 – Набор объектов TLV, сформированного БТИ

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload/ Payload_enc	до 4000	Данные БТИ
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения полученного отправителем данного или 0x00000000 для первого сообщения
..	..	..	..
0x1C	Diagnostic	1	Диагностические данные для сервера
0x1F	Source	1	Источник данных
0x1E	MAC	6	Имитовставка

5) Тахограф формирует сообщение MESSAGE (тэг 0x39 с данными, полученными от БТИ и заголовок);

6) Тахограф передает сообщение серверу и получает ответное сообщение;

7) Тахограф проверяет заголовок и структуру ответного сообщения, если обнаружена ошибка тахограф должен выполнить процедуру обработки ошибки (см. 4.2.4);

8) Тахограф передает в БТИ полученный набор объектов TLV в команде «Передача подтверждения сервера». Если команда выполнена успешно, то тахограф переходит к выгрузке следующего пакета данных, подготовленных БТИ.

9) Если от БТИ получен ответ с кодом ошибки, тахограф должен выполнить процедуру обработки ошибки (см. 4.2.4).

4.4.3.3 Сценарий выгрузки данных, подготовленных тахографом:

1) Если присутствуют данные, подготовленные тахографом, тахограф инкрементирует номер сообщения и формирует набор объектов TLV с объектом содержательных данных, подготовленных тахографом и без объекта имитовставки в соответствии с таблицей 27.

Т а б л и ц а 27 – Набор объектов TLV, формируемых тахографом, с объектом содержательных данных и без объекта имитовставки

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload/ Payload_enc	до 4000	Содержательные данные
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения полученного отправителем данного или 0x00000000 для первого сообщения
…	…	…	…
0x1C	Diagnostic	1	Диагностические данные для сервера
0x1F	Source	1	Источник данных

2) Тахограф передает в БТИ сформированный набор объектов TLV в команде «Получение посылки для сервера» и получает в ответ набор объектов TLV с содержательными данными (открытыми – тэг 0x20 или зашифрованными – тэг 0xA0) и объектом имитовставки, приведенным в таблице 28.

Т а б л и ц а 28 – Набор объектов TLV, подготовленного БТИ по команде «Получение посылки для сервера»

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload/ Payload_enc	до 4000	Данные, подготовленные тахографом
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения полученного отправителем данного или 0x00000000 для первого сообщения
…	…	…	…
0x1C	Diagnostic	1	Диагностические данные для сервера
0x1F	Source	1	Источник данных
0x1E	MAC	6	Имитовставка

3) Тахограф формирует соо бщение MESSAGE (тэг 0x39 с данными и заголовок);

4) Тахограф передает сообщение серверу и получает ответное сообщение;

5) Тахограф проверяет заголовок и структуру ответного сообщения, если обнаружена ошибка, то тахограф должен выполнить процедуру обработки ошибки (см. 4.2.4);

6) Тахограф передает в БТИ полученный набор объектов TLV в команде «Передача подтверждения сервера» (тип данных – данные сервера для тахографа). Если команда выполнена успешно, то тахограф переходит к формированию тела следующего сообщения;

7) Если от БТИ получен ответ с кодом ошибки, тахограф должен выполнить процедуру обработки ошибки (см. 4.2.4).

4.4.4 Повторная аутентификация

Сервер может потребовать от тахографа проведения повторной аутентификации.

Для повторной аутентификации сервер посылает сообщение DENYSESSION.

Тахограф также может потребовать от сервера проведения повторной аутентификации, послав сообщение CONNECTREQUEST. В заголовке сообщения поле ServerCTX заполняется значением поля ServerCTX, взятого из последнего полученного успешного ответа от сервера.

4.4.4.1 Схема запроса повторной аутентификации сервером приведена на рисунке 4.

	Тахограф		**Сервер**
Шаг1	MESSAGE (…)	⇨	
		⇦	DENYSESSION(…)
Шаг 2 Открытие сессии	ServerCTX ≠ 0 CONNECTREQUEST (…)	⇨	
		⇦	SERVERHELLO(…)
	CACERTREQUEST (…)	⇨	
		⇦	CACERTCHAIN (…)
	INITSESSION (…)	⇨	
		⇦	CONFIRMSESSION(…)
	При любой ошибке: Завершение обмена	⇦	При любой ошибке: DENYSESSION(…)
Шаг 3	Продолжение обмена на новых ключах MESSAGE(…)	⇨	
		⇦	Продолжение обмена на новых ключах MESSAGE(…)

Рисунок 4 – Обмен сообщениями при запросе сервером повторной аутентификации

4.4.4.2 Схема запроса повторной аутентификации тахографом приведена на рисунке 5.

	Тахограф		**Сервер**
Шаг1 Открытие сессии	ServerCTX ≠ 0 CONNECTREQUEST(…)	⇨	
		⇦	SERVERHELLO(…)
	CACERTREQUEST (…)	⇨	
		⇦	CACERTCHAIN(…)
	INITSESSION (…)	⇨	
		⇦	CONFIRMSESSION(…)
	При любой ошибке: Завершение обмена	⇦	При любой ошибке: DENYSESSION(…)
Шаг 2	Продолжение обмена на новых ключах MESSAGE(…)	⇨	
		⇦	Продолжение обмена на новых ключах MESSAGE(…)

Рисунок 5 – Обмен сообщениями при запросе тахографом повторной аутентификации

Приложение А
(справочное)

Справочник вычисления CRC16 и используемых тегов при обмене данными тахографа и сервера

А.1 Вычисление CRC16

Алгоритм идентичен CRC-A по ГОСТ Р ИСО/МЭК 14443-3-2014, за исключением стартового значения CRC (CRC_IV). CRC_IV = 0xA56C (байтовая последовательность: 0x6CA5).

Пример

Стартовое значение: CRC_IV = 0x6CA5

Входные данные: Input = 0x0A123456

Результат: CRC16 = 0x4832

А.2 Используемые тахографом и сервером Тэги при обмене данными приведены в таблице А.1.

Т а б л и ц а А.1 – Теги, используемые тахографом и сервером при обмене данными

Тэг	Наименование	Длина, байт	Примечание
Сообщения			
0x30	CONNECTREQUEST	-	Выдается тахографом сразу после установления соединения
0x31	SERVERHELLO	-	Выдается сервером при установлении сессии в ответ на CONNECTREQUEST или в качестве запроса на повторную аутентификацию
0x33	DENYSESSION	-	Выдается сервером в случае отказа установления/восстановления сессии
0x34	CACERTREQUEST	-	Выдается тахографом если у него нет ключа ДЦ
0x35	CACERTCHAIN	-	Выдается сервером в ответ на CACERTREQUEST
0x36	INITSESSION	-	Выдается тахографом для динамической аутентификации
0x37	CONFIRMSESSION	-	Выдается сервером в ответ на успешную динамическую аутентификацию
0x39	MESSAGE	-	Зашифрованные сообщения, защищенные имитовставкой
0x3A	PROMPT	-	Периодически выдается тахографом для согласования текущей частоты передачи запросов

Продолжение таблицы А.1

Тэг	Наименование	Длина, байт	Примечание
0x3B	SERVERREQUEST	-	Выдается сервером в ответ на PROMPT
0x31, 0x38. 0x3C-0x3E	RFU	-	Зарезервировано
Простые тэги для передачи данных в сообщениях при установлении соединения и аутентификации			
0x01	Certificate	до 3000	Сертификат
0x02	Server Address	до 199	Адрес (DNS-имя) сервера и другие идентификационные данные
0x03	Part Number	16	Заводской номер БТИ
0x04	KeyId	16	Идентификатор(ы) ключа проверки сертификата
0x05	Random	16	Случайное число
0x07	S	64	Криптограмма аутентификации БТИ
0x08	H	10	Текущее время сервера (4 байта) || Проверочная криптограмма сервера (6 байт)
0x09	ErrorCode	2	Код причины разрыва соединения
0x0A	Description	0-n	Описание причины разрыва соединения (короткое сообщение)
0x0B	Freq	4	Текущая частота передачи сообщений, с
0x0C	ServerRequest	4	Код процедуры/уведомления, запрашиваемого сервером. В случае передачи фиксированного значения, например 0, тахограф считает, что необходимости в оперативном общении с сервером нет
0x06, 0x0D-0x0F	RFU	-	Зарезервировано
Простые тэги для передачи протокольных данных в сообщениях с содержательными данными (MESSAGE)			
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения, полученного отправителем данного

Окончание таблицы А.1

0x12	RetransmitReq	0	Запрос повторной передачи данных предыдущего сообщения
0x13	IDProcessingSys	4	Код/идентификатор системы сбора и обработки данных
0x14	VPProcessingSys	1	Версия протокола обмена с системой сбора и обработки данных
0x15	UTISerial	16(32)	Заводской (заводской и регистрационный) номер БТИ
0x16-0x1B	RFU	-	Зарезервировано
0x1C	Diagnostic	1	Диагностические данные для сервера
0x1D	Priority	1	Уровень приоритета сообщения
0x1F	Source	1	Источник данных
Простой тэг для передачи имитовставки			
0x1E	MAC	6	Имитовставка вычисляется на все тэги в сообщении
Составные тэги для передачи содержательных данных			
0x20	Payload	n	Открытые данные, передаваемые в сообщении
0xA0	Payload_enc	n	Зашифрованные данные, передаваемые в сообщении

Приложение Б
(обязательное)

Технический регламент взаимодействия тахографов с ОТД по TCP/IP

Б.1 Установка TCP соединения.

В случае если у тахографа есть необходимость в передаче информации в ОТД или тестирования канала связи:

а) тахограф начинает процедуру TCP подключения. При неудачной попытке соединения выполняется процедура обработки ошибок (см. Б.4);

б) тестирование канала связи допускается при включении устройства и не чаще, чем один раз в час.

Б.2 Общие положения TCP соединения:

а) общий таймаут на TCP соединение (TCP_INACTIVITY_TO), по которому не передаются пользовательские данные в любом направлении – 595 с.;

б) при отсутствии передачи данных в течение 595 с, ОТД разрывает TCP соединение (см. Б3) и закрывает сессию ЗОС.

в) любая передача пользовательских данных обнуляет таймер TCP_INACTIVITY_TO;

г) минимальный таймаут на ожидание любого ответа от сервера на этапе установки ЗОС (SEC_CONN_INIT_READ_TO) – 5 с;

д) после открытия сессии ЗОС, тахограф посылает запросы в ОТД и получает ответы по каналу ЗОС. Время ожидания ответа от процессинга (SEC_CONN_DATA_RSP_READ_TO) – не менее 33 с.

Б.3 Управление разрывом TCP соединения:

а) если установленным TCP и ЗОС соединением тахограф не пользуется в течение TCP_INACTIVITY_TO, то тахограф должен сам инициировать разрыв TCP соединения со своей стороны, и не устанавливать нового соединения, если нет необходимости в этот момент передачи данных/запросов в ОТД (или тестирования канала связи);

Примечание – После разрыва соединения, тахограф должен выполнить процедуру завершения обмена с сервером.

б) если соединение было принудительно разорвано со стороны ОТД, и у тахографа нет необходимости в этот момент передаче данных/запросов в ОТД, то тахограф не должен инициировать восстановление TCP соединения;

в) если у тахографа есть необходимость в передаче информации, то ситуация с ошибкой передачи данных по TCP соединению в пределах TCP_INACTIVITY_TO трактуется как ошибка взаимодействия и дальше тахограф должен следовать процедуре обработки ошибок, изложенной в Б.4.

Б.4 Процедура обработки ошибок:

а) после возникновения ошибки по TCP, тахограф делает паузу в 3 с и пытается повторно (до трех раз) установить TCP соединение, с паузой в 3 с между попытками.

б) в случае невозможности подключения после трех попыток, тахограф разрывает соединение, делает паузу (RECONNECT_WAIT_TO) в 30 + random (1...60) с и если у тахографа есть необходимость в передаче информации в ОТД, то снова выполняет попытку подключения (см.Б.1). Если подключение по TCP/IP успешно, то тахограф продолжает обмен в соответствии с Б.2.

Примечание – После разрыва соединения тахограф должен выполнить процедуру завершения обмена с сервером.

Библиография

[1] Европейское соглашение, касающееся работы экипажей транспортных средств, производящих международные автомобильные перевозки (ЕСТР), и Протокол о подписании. Заключено в г. Женева 01.07.1970 г. (в ред. поправки № 6 от 20.09.2010).

УДК 629.3.01 ОКС 43.040.10

Ключевые слова: автомобильные транспортные средства, тахографы цифровые, протоколы обмена, информационная система, контроль

Генеральный директор ФГУП «НАМИ» Ф.Л. Назаров

Заместитель генерального директора
по техническому регулированию
ФГУП «НАМИ» С.А. Аникеев

Директор Центра «Стандартизация и
идентификация» ФГУП «НАМИ» П.Г. Шачнев

Президент Ассоциации
«Тахографический центр» А.Б. Архангельский

Нормоконтроль:
Начальник Управления «Стандартизация»
Центра «Стандартизация и
идентификация» ФГУП «НАМИ» Е.Е. Бобылева