ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59289— 2020

Глобальная навигационная спутниковая система на транспорте

ТЕХНИЧЕСКИЕ СРЕДСТВА КОНТРОЛЯ НА ТРАНСПОРТЕ

Единый расширяемый набор протоколов обмена данными технических средств контроля с информационными системами

Издание официальное

Москва
Стандартинформ
2021

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным унитарным предприятием «ЗащитаИнфоТранс» Министерства транспорта Российской Федерации (ФГУП «ЗащитаИнфоТранс»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 363 «Радионавигация»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 декабря 2020 г. № 1442-ст

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 (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2021

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 2
4 Общие положения 9
5 Протокол транспортного уровня 10
5.1 Субъекты взаимодействия 10
5.2 Механизмы обеспечения маршрутизации и надежности доставки данных 10
5.3 Построение систем и аппаратно-программных комплексов на основе протокола транспортного уровня 11
5.4 Типы данных 11
5.5 Структуры данных 11
5.6 Структуры данных пакетов транспортного уровня 12
5.7 Структура данных при использовании резервных каналов передачи данных на основе сервисов SMS и LPWAN 12
6 Спецификация протокола уровня поддержки услуг 12
6.1 Назначение протокола уровня поддержки услуг 12
6.2 Определение структур данных 13
7 Перечень сервисов, поддерживаемых в протоколе 13
8 Спецификация сервиса передачи и обработки мониторинговой информации EGTS_TELEDATA_SERVICE 13
8.1 Требования к БНСО для использования услуги EGTS_TELEDATA_SERVICE 13
8.2 Состав сервиса EGTS_TELEDATA_SERVICE 14
8.3 Использование EGTS_COMMANDS_SERVICE 14
9 Спецификация сервиса аутентификации EGTS_AUTH_SERVICE 14
9.1 Общие положения 14
9.2 Описание подзаписей сервиса EGTS_AUTH_SERVICE 15
10 Спецификация сервиса управления и конфигурирования EGTS_COMMANDS_SERVICE 15
10.1 Описание подзаписей 15
11 Спецификация сервиса EGTS_FIRMWARE_SERVICE 15
11.1 Описание подзаписей 15
12 Спецификация сервиса экстренного реагирования при аварии EGTS_ECALL_SERVICE 15
12.1 Назначение сервиса экстренного реагирования при аварии 15
12.2 Минимально необходимый набор функций БНСО для использования услуги EGTS_ECALL_SERVICE 15
12.3 Состав и описание подзаписей сервиса EGTS_ECALL_SERVICE 15
12.4 Использование сервиса EGTS_COMMANDS_SERVICE 15
12.5 Список и описание команд, параметров и подтверждений при использовании сервиса EGTS_ECALL_SERVICE 15
12.6 Формат сообщения AL-ACK 16
13 Спецификация протокола обмена телематическими данными с применением криптографической защиты данных 16
13.1 Общие сведения 16
13.2 Протокол уровня приложения 16
13.3 Криптографическая защита данных 28

14 Протокол обмена данными тахографа с автоматизированной информационной системой «Тахографический контроль» 29
Приложение А (справочное) Описание принципа построения навигационно-информационной системы на основе протокола транспортного уровня 30
Приложение Б (справочное) Описание процедуры авторизации БНСО на авторизующей ТП. 32
Приложение В (обязательное) Коды результатов обработки. 37
Приложение Г (справочное) Пример реализации алгоритма расчета контрольной суммы CRC16 на языке C/* 39
Приложение Д (справочное) Пример реализации алгоритма расчета контрольной суммы CRC8 на языке C/* 40
Приложение Е (рекомендуемое) Описание спецификации протокола обмена данными тахографа с АИС «ТК» 41
Библиография 58

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Глобальная навигационная спутниковая система на транспорте

ТЕХНИЧЕСКИЕ СРЕДСТВА КОНТРОЛЯ НА ТРАНСПОРТЕ

Единый расширяемый набор протоколов обмена данными технических средств контроля с информационными системами

Global navigation system in transport. Technical means of controlling in transport.
A single extensible set of protocols of data exchange of technical means of controlling with information systems

Дата введения — 2021—06—01

1 Область применения

Настоящий стандарт распространяется на технические средства контроля местоположения, скорости, технического состояния колесных транспортных средств (далее — транспортные средства) и их грузов, времени управления и отдыха водителей транспортных средств, режимов труда и отдыха водителей транспортных средств, функционирующие с использованием технологий ГЛОНАСС или ГЛОНАСС совместно с иными глобальными навигационными спутниковыми системами, устанавливаемые на транспортные средства и предназначенные для применения в составе интеллектуальных транспортных систем, навигационно-информационных систем, систем управления на транспорте, в том числе автоматизированных и роботизированных, Государственной автоматизированной информационной системы «ЭРА-ГЛОНАСС», системы взимания платы в счет возмещения вреда, причиняемого автомобильным дорогам общего пользования федерального значения транспортными средствами, имеющими разрешенную максимальную массу свыше 12 т, автоматизированной информационной системы «Тахографический контроль», систем мониторинга состояния грузов и в других системах транспортной телематики (далее — бортовое навигационно-связное оборудование).

Настоящий стандарт устанавливает требования к протоколам обмена данными БНСО с Государственной автоматизированной информационной системой «ЭРА-ГЛОНАСС», системой взимания платы в счет возмещения вреда, причиняемого автомобильным дорогам общего пользования федерального значения транспортными средствами, имеющими разрешенную максимальную массу свыше 12 тонн, автоматизированной информационной системой «Тахографический контроль», системами мониторинга состояния грузов, и другими информационными системами органов государственной власти и организаций транспортной телематики различного назначения.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 33464 Глобальная навигационная спутниковая система. Система экстренного реагирования при авариях. Устройство/система вызова экстренных оперативных служб. Общие технические требования

ГОСТ 33465—2015 Глобальная навигационная спутниковая система. Система экстренного реагирования при авариях. Протокол обмена данными устройства/системы вызова экстренных оперативных служб с инфраструктурой системы экстренного реагирования при авариях

Издание официальное

ГОСТ 33472—2015 Глобальная навигационная спутниковая система. Аппаратура спутниковой навигации для оснащения колесных транспортных средств категорий M и N. Общие технические требования

ГОСТ Р 34.10 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 34.11 Информационная технология. Криптографическая защита информации. Функция хэширования

ГОСТ Р 34.12 Информационная технология. Криптографическая защита информации. Блочные шифры

ГОСТ Р 34.13 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

ГОСТ Р 52928 Система спутниковая навигационная глобальная. Термины и определения

ГОСТ Р 53632Показатели качества услуг доступа в Интернет. Общие требования

ГОСТ Р 55524 Глобальная навигационная спутниковая система. Системы навигационно-информационные. Термины и определения

ГОСТ Р 56096 Система передачи космических данных и информации. Пакетная телеметрия

ГОСТ Р ИСО/МЭК 7498-1 Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель

ГОСТ Р ИСО/МЭК 19762-1 Информационные технологии (ИТ). Технологии автоматической идентификации и сбора данных (АИСД). Гармонизированный словарь. Часть 1. Общие термины в области АИСД

Примечание — 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 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по ГОСТ Р 52928—2010, ГОСТ Р ИСО/МЭК 7498-1—99, ГОСТ 33464—2015, ГОСТ Р 55524—2013, ГОСТ Р ИСО/МЭК 19762-1—2011, ГОСТ Р 53632—2009, ГОСТ Р 56096—2014, а также следующие термины с соответствующими определениями:

3.1.1 **авторизация:** Процесс определения достоверности полномочий предъявителя на доступ к ресурсу или использованию услуг.

3.1.2 **аппаратно-программные комплексы:** Набор технических и программных средств, работающих совместно для выполнения одной или нескольких сходных задач.

3.1.3 **аутентификация:** Действия по проверке заявленной подлинности объекта.

3.1.4 **байт:** Строка, состоящая из нескольких битов, обрабатываемая как единое целое и обычно представляющая знак или часть знака.

3.1.5 **блок СКЗИ тахографа:** Составная часть тахографа, являющаяся программно-аппаратным шифровальным (криптографическим) средством, которая содержит средства шифрования, средства электронной подписи, обеспечивающие создание электронной подписи владельца этого компонента тахографа, квалифицированный сертификат ключа проверки электронной подписи владельца этого компонента тахографа и криптографические ключи для криптографического преобразования информации, обеспечивающая с использованием сигналов ГЛОНАСС или ГЛОНАСС совместно с иными глобальными спутниковыми навигационными системами формирование тахографической информации, в том числе по результатам измерений, а также его взаимную аутентификацию с иными защищенными компонентами тахографа, запись с заданной периодичностью и хранение тахографической информа-

ции, передачу этой информации, подписанной усиленной квалифицированной электронной подписью, иным компонентам тахографа, в том числе в зашифрованном виде.

3.1.6 **бортовое навигационно-связное оборудование;** БНСО: аппаратно-программное техническое устройство, устанавливаемое на контролируемое транспортное средство для определения координатно-временных параметров, параметров движения транспортного средства с использованием технологий ГЛОНАСС или ГЛОНАСС совместно с иными глобальным навигационными спутниковыми системами, приема и регистрации (хранения) в некорректируемом виде данных от бортового оборудования (датчиков) и передачи информации во внешние системы по сетям беспроводной связи.

Примечание — В понятие БНСО входят следующие технические устройства и системы:
- аппаратура спутниковой навигации, устанавливаемая на транспортные средства в соответствии с [1];
- тахографы, устанавливаемые на транспортные средства в соответствии с [2];
- бортовые устройства взимания платы в счет возмещения вреда, причиняемого автомобильным дорогам общего пользования федерального значения транспортными средствами, имеющими разрешенную максимальную массу свыше 12 т, устанавливаемые на транспортные средства в соответствии с [3].

3.1.7 **бит:** Разряд, принимающий цифровое значение 0 или 1 в двоичной системе счисления.

3.1.8 **ГЛОНАСС:** Глобальная навигационная спутниковая система Российской Федерации.

3.1.9 **государственная автоматизированная информационная система «ЭРА-ГЛОНАСС»:** Федеральная государственная территориально распределенная автоматизированная информационная система экстренного реагирования при авариях, обеспечивающая оперативное получение формируемой в некорректируемом виде на основе использования сигналов ГЛОНАСС информации о дорожно-транспортных и об иных происшествиях на автомобильных дорогах в Российской Федерации, обработку этой информации, ее хранение и передачу в экстренные оперативные службы, а также доступ к этой информации государственных органов, органов местного самоуправления, должностных лиц, юридических лиц, физических лиц, решение иных задач в области получения, обработки, хранения и передачи информации, не связанной с дорожно-транспортными и иными происшествиями на автомобильных дорогах в Российской Федерации.

3.1.10 **дискретный выход:** Выход, на который контроллер может подать логический ноль либо логическую единицу.

3.1.11 **длина пакета:** Размер пакета в байтах, включая заголовок и поле данных пакета. Минимальное значение (включая заголовок) должно составлять 7 байт, максимальное — 65549 байт.

3.1.12 **интерфейс:** Совместно используемая граница между двумя функциональными единицами, определяемая различными функциональными характеристиками, параметрами физического соединения, параметрами взаимосвязи при обмене сигналами, а также другими характеристиками в зависимости от задаваемых требований.

3.1.13 **код:** Совокупность правил, с помощью которых устанавливается соответствие элементов одного набора элементам другого набора.

3.1.14 **контрольная сумма:** Некоторое значение, рассчитанное по набору данных путем применения определенного алгоритма и используемое для проверки целостности данных при их передаче или хранении.

3.1.15 **криптографическая защита информации:** Защита информации с помощью ее криптографического преобразования.

3.1.16 **одометр:** Счетчик — прибор для измерения количества оборотов колеса. При помощи него может быть измерен пройденный транспортным средством путь.

3.1.17 **ошибка:** Недопустимое состояние, которое испытывает система.

3.1.18 **СВП «Платон»:** Система взимания платы в счет возмещения вреда, причиняемого автомобильным дорогам общего пользования федерального значения транспортными средствами, имеющими разрешенную максимальную массу свыше 12 т.

3.1.19 **тахографическая информация:** Информация ограниченного доступа, в том числе подписанная квалифицированной электронной подписью, содержащая сведения о времени управления транспортным средством и отдыха водителя транспортного средства, о режиме труда и отдыха водителя транспортного средства, управление которым входит в его трудовые обязанности, текущем местоположении, направлении, скорости и маршруте движения транспортных средств, формируемая тахографами с использованием сигналов ГЛОНАСС или ГЛОНАСС совместно с иными глобальными спутниковыми навигационными системами, о тахографах, защищенных компонентах тахографов и транспортных средствах, оснащенных тахографом, о водителях транспортных средств, а также иные

технические сведения, формируемые при оснащении транспортных средств тахографами и их эксплуатации.

3.1.20 **транспортные средства:** Колесные транспортные средства категорий M и N, предназначенные для эксплуатации на автомобильных дорогах общего пользования.

3.1.21 **протокол передач данных:** Набор соглашений интерфейса логического уровня, которые определяют обмен данными между различными программами и задают единообразный способ передачи сообщений и обработки ошибок при взаимодействии программного обеспечения разнесенной в пространстве аппаратуры, соединенной тем или иным интерфейсом.

3.1.22 **протокол IP:** Основной протокол межсетевого взаимодействия, используемый в сети Интернет, работающий в паре с протоколом управления передачей (TCP), образуя стек протоколов TCP/IP.

3.1.23 **системы транспортной телематики:** Информационные системы, обеспечивающие автоматизированный сбор, обработку, передачу и представление потребителям данных о местоположении и состоянии транспортных средств, а также информации, получаемой на основе этих данных, в целях эффективного и безопасного использования транспортных средств различного назначения и принадлежности.

3.1.24 **символ:** Графическое представление понятия, имеющее смысл в конкретном контексте.

3.1.25 **тахограф:** Техническое средство контроля, обеспечивающее непрерывную, некорректируемую регистрацию и хранение информации о скорости и маршруте движения транспортного средства, о времени управления транспортным средством и отдыха водителя транспортного средства, о режиме труда и отдыха водителя транспортного средства, управление которым входит в его трудовые обязанности, формируемые с использованием сигналов ГЛОНАСС или ГЛОНАСС совместно с иными глобальными спутниковыми навигационными системами, а также обеспечивающими передачу этой информации в зашифрованном и некорректируемом виде с заданной периодичностью с использованием государственной автоматизированной информационной системы «ЭРА-ГЛОНАСС» в автоматизированную информационную систему «Тахографический контроль».

3.1.26 **телематическая платформа:** Комплекс аппаратно-программных средств, предназначенный для сбора, обработки, хранения и маршрутизации мониторинговой информации от БНСО в диспетчерские пункты и центры, а также обмена технологической информацией между диспетчерскими центрами (пунктами) и БНСО.

3.1.27 **телематическое сообщение:** Одно или несколько сообщений электросвязи, содержащих информацию, структурированную в соответствии с протоколом обмена, поддерживаемым взаимодействующими информационной системой и БНСО.

3.1.28 **технические средства контроля на транспорте:** Комплекс аппаратно-программых средств, предназначенных для контроля установленных критичных значений пространственно-временных характеристик колесных транспортных средств, параметров технического состояния транспортного средства и перевозимых им грузов в целях обеспечения безопасности применения транспортных средств.

Примечания

1 Технические средства контроля на транспорте по конструктивным особенностям, связанным со степенью их мобильности, подразделяются на следующие группы: стационарные, передвижные, бортовые, носимые.

2 Бортовое навигационно-связное оборудование относится к группе бортовых технических средств контроля.

3.1.29 **циклический избыточный код (Cyclic redundancy check, CRC):** Алгоритм нахождения контрольной суммы, предназначенный для проверки целостности данных.

3.1.30 **цифровая подпись:** Реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

3.1.31 **шифрование информации:** Криптографическая защита информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче.

3.1.32 **CP-1251 (CodePage CP1251):** Набор символов и кодировка, являющаяся стандартной 8-битной кодировкой для всех русских версий Microsoft Windows.

3.1.33 **DORIS (Doppler Orbitography and Radiopositioning Integrated by Satellite):** Французская гражданская система точного (сантиметрового) определения орбиты и позиционирования.

3.1.34 **eCall (EmergencyCall):** Общеевропейская система экстренного реагирования при авариях;

3.1.35 **Little-endian:** Порядок следования байт от младшего к старшему.

3.2. В настоящем стандарте применены следующие сокращения:

АС — автомобильная система/устройство вызова экстренных служб;

АИС «ТК» — автоматизированная информационная система «Тахографический контроль»;

БД — база данных;

БНСО — бортовое навигационно-связное оборудование;

ГАИС«ЭРА-ГЛОНАСС» — Государственная автоматизированная информационная система «ЭРА-ГЛОНАСС»;

ГЛОНАСС — российская спутниковая система навигации;

ГНСС — глобальная навигационная спутниковая система;

ДТП — дорожно-транспортные происшествия;

ДУЖ — датчик уровня жидкости;

ЕЭК ООН — Европейская экономическая комиссия Организации Объединенных Наций;

МНД — минимальный набор данных;

НИС — навигационно-информационные системы;

ОЗУ — оперативное запоминающее устройство;

ПО — программное обеспечение;

ППУ — протокол уровня поддержки услуг;

ПТУ — протокол транспортного уровня;

ТП — телематическая платформа;

ТС — транспортное средство;

СВП«ПЛАТОН» — система взимания платы в счет возмещения вреда, причиняемого автомобильным дорогам общего пользования федерального значения транспортными средствами, имеющими разрешенную максимальную массу свыше 12 т;

СКЗИ — средство криптографической защиты информации;

ФГУП — федеральное государственное унитарное предприятие;

AC — AuthorizationCode (код авторизации, используемый на принимающей стороне (БНСО) и обеспечивающий ограничение доступа на выполнение отдельных команд);

ACFE — AuthorizationCodeFieldExists (битовый флаг, определяющий наличие полей ACL и AC в подзаписи);

ACL — AuthorizationCodeLength (длина в байтах поля БНСО, содержащего код авторизации на стороне получателя);

ACT — Action 9 описание действия, используемое в случае типа команды (поле CT = = CT_COM подзаписи EGTS_SR_COMMAND _DATA);

ADIO — Analog Digital Inputs Octet (показания дополнительных дискретных входов);

ADR — Address (адрес модуля, для которого данная команда предназначена);

ADS — Accelerometer Data Structure (структуры данных показаний акселерометра);

ALT — Altitude [высота над уровнем моря, м (опциональный параметр, наличие которого определяется битовым флагом «ALTE»)];

ALTS — AltitudeSign (битовый флаг, определяет высоту относительно уровня моря и имеет смысл только при установленном флаге «ALTE»);

ANS — Analog Sensor (значение аналоговых датчиков);

ASFE — Analog Sensor Field Exists (битовые флаги, определяющие наличие показаний от соответствующих аналоговых датчиков);

ASN — Analog Sensor Number (номер аналогового входа);

ASV — Analog Sensor Value (значение показаний аналогового входа);

ATM — AbsoluteTime [время проведения измерений первой передаваемой структуры показаний акселерометра (число секунд с 00:00:00 01.01.2010 UTC)];

BB — битовый флаг, признак отправки данных из памяти («черный ящик»);

BBU — битовый флаг, определяющий, что в качестве источника питания БНСО используется внутренняя батарея;

BBV — значение напряжения резервной батареи, В, с дискретностью 0,1 В;

BS — Buffer Size (максимальный размер буфера приема БНСО в байтах);

BSE — BufferSizeExists (битовый флаг, определяющий наличие поля BS в подзаписи);

CT — CommandType (тип команды);

CCD — Command Code (код команды);

CCT — Command Confirmation Type (тип подтверждения);

CD — CommandData (тело команды параметры, данные возвращаемые на команду-запрос, использующие кодировку из поля CHS или значение по умолчанию);

CFE — CounterFieldExists (битовые флаги, определяют наличие соответствующих полей счетных входов);

CHS — Charset (кодировка символов, используемая в поле CD, содержащем тело команды);

CHSFE — CharsetFieldExists (битовый флаг, определяющий наличие поля CHS в подзаписи);

CID — Command Identifier (идентификатор команды, сообщения);

CMI — Component or Module Identifier (номер компонента в случае принадлежности сущности непосредственно БНСО или идентификатор периферийного модуля/порта, подключенного к БНСО, в зависимости от значения параметра MT);

CMP — Compressed (определяет, используется ли сжатие данных из поля SFRD);

CN — Counter (значение счетных входов);

CNV — Counter Value (значение показаний счетного входа);

CRC-8(16) — Cyclic Redundancy Code (циклический избыточный код);

CRN — Confirmed Record Number (номер подтверждаемой записи (значение поля RN из обрабатываемой записи));

CS — битовое поле, тип используемой системы;

CSMRN — Concatenated Short Message Reference Number (номер конкатенируемого SMS-сообщения),

D — Delimiter (разделитель строковых параметров (всегда имеет значение 0));

DID — Dispatcher ID (уникальный идентификатор диспетчера);

DIN — Digital Inputs (битовые флаги, определяют состояние основных дискретных входов);

DIOE — Digital Inputs Octet Exists (битовые флаги, определяющие наличие соответствующих полей дополнительных дискретных входов);

DIR — Direction (направление движения ТС, выраженное в градусах, относительно севера по часовой стрелке);

DIRH — Direction the Highest bit (старший бит параметра DIR);

DNS — DomainNameSystem (система доменных имен);

DORIS — Doppler Orbitography and Radiopositioning Integrated by Satellite [французская гражданская система точного (сантиметрового) определения орбиты и позиционирования];

DOUT — Digital Outputs (битовые флаги дискретных выходов);

DPR — Doors Presented (битовое поле, определяющее наличие счетчиков на дверях и структуру поля PCD);

DRL — DoorsReleased (битовое поле, определяющее двери, которые открывались и закрывались при подсчете пассажиров);

DSCR — Description (краткое описание модуля);

DSN — Digital Sensor Number (номер дискретного входа);

DSST — Digital Sensor State (состояние дискретного входа);

DT — Dispatcher Type (тип диспетчера);

eCall — EmergencyCall (общеевропейская система экстренного реагирования при авариях);

EGTS — Era Glonass Telematics Standard (телематический стандарт);

ENA — Encryption Algorithm (поле, определяющие код алгоритма, используемый для шифрования данных из поля SFRD);

EPQ — Expected Parts Quantity (ожидаемое число частей передаваемой сущности);

EVFE — Event ID Field Exists (битовое поле, определяющее наличие в данном пакете поля EVID);

EVID — Event Identifier (уникальный идентификатор события);

EXE — битовый флаг, определяет наличие поля EXP и следующего за ним разделителя D;

EXP — специальная последовательность, используемая в процессе шифрования;

FDL — Frame Data Length (поле FDL определяет размер в байтах поля данных SFRD);

FIX — битовое поле, тип определения координат;

FLG — Flags (поле, определяющее дополнительные параметры навигационной посылки);

FM — Format (формат данных, содержащихся в поле MSD данной подзаписи);

FN — File Name (поле, определяющее имя файла);

FTP — File Transfer Protocol (протокол передачи файлов);

FWV — Firmware Version (версия аппаратной части модуля);

GPRS — General Packet Radio Service (технология пакетной передачи данных посредством сотовой связи);

GPS — Global Positioning System (система глобального позиционирования);

GRP — Group (битовый флаг, определяющий принадлежность передаваемых данных определенной группе, идентификатор которой указан в поле OID);

GSM — Global System for Mobile (глобальный стандарт цифровой мобильной сотовой связи, с разделением каналов по времени и частоте);

HCS — Header Check Sum (контрольная сумма заголовка транспортного уровня);

HDID — Home Dispatcher Identifier (идентификатор «домашней» ТП);

HDIDE — Home Dispatcher Identifier Exists (битовый флаг, который определяет наличие поля HDID в подзаписи);

HDOP — Horizontal Dilution of Precision (снижение точности в горизонтальной плоскости);

HE — Header Encoding (кодировка заголовка);

HFE — HDOP Field Exists (определяет наличие поля HDOP);

HL — Header Length [длина заголовка транспортного уровня в байтах с учетом байта контрольной суммы (поля HCS)];

HTTP — HyperText Transfer Protocol (протокол передачи гипертекста);

IBU — битовый флаг, определяющий, что в качестве источника питания БНСО используется внешний резервный источник;

IBV — значение напряжения внутренней батареи, В, с дискретностью 0,1 В;

ID — Identity (уникальный идентификатор передаваемой сущности);

IED — Information-Element-Data (данные информационных элементов);

IEI — Information-Element-Identifier (идентификатор информационного элемента);

IMAP — Internet Message Access Protocol (протокол прикладного уровня для доступа к электронной почте);

IMEI — International Mobile Equipment Identity (идентификатор мобильного устройства (модема));

IMEIE — International Mobile Equipment Identity Exists (битовый флаг, который определяет наличие поля IMEI в подзаписи);

IMSI — International Mobile Subscriber Identity (идентификатор мобильного абонента);

IMSIE — International Mobile Subscriber Identity Exists (битовый флаг, который определяет наличие поля IMSI в подзаписи);

IP — Internet Protocol (межсетевой протокол);

IPQ — In Passengers Quantity (число пассажиров, вошедших через дверь);

IRNSS — Indian Regional Navigation Satellite System (индийская региональная спутниковая система навигации);

ISDN — Integrated Services Digital Network (цифровая сеть с интегрированными услугами);

ISL — Identity String Length (результирующая длина идентификационных данных);

ISLE — Identity String Length Exists (битовый флаг, определяет наличие поля ISL);

LAHS — битовый флаг определяет полушарие широты;

LAT — Latitude (широта по модулю);

LIE — Length of Information-Element (параметры, определяющие размер данных информационных элементов);

LIFE — Loop In Field Exists (битовые флаги, определяющие наличие информации о состоянии шлейфовых входов);

LIN — Loop In Number (номер шлейфового входа);

LIS — Loop In State (значение состояния шлейфового входа);

LLSD — Liquid Level Sensor Data (показания ДУЖ в формате, определяемом полем RDF);

LLSEF — Liquid Level Sensor Error Flag (битовый флаг, определяющий наличие ошибок при считывании значения датчика уровня жидкости);

LLSN — Liquid Level Sensor Number (порядковый номер датчика уровня жидкости);

LLSVU — Liquid Level Sensor Value Unit (битовый флаг, определяющий единицы измерения показаний ДУЖ);

LNGC — Language Code (код языка, предпочтительного к использованию на стороне БНСО);

LNGCE — Language Code Exists (битовый флаг, который определяет наличие поля LNGC в подзаписи);

LOHS — битовый флаг определяет полушарие долготы;

LONG — долгота по модулю, градусы;

LPWAN — Low-power-Wide-area-Network (энергоэффективная сеть дальнего радиуса действия);

MT — Module Type (тип модуля, для которого предназначена передаваемая сущность);

OA — Object Attribute (характеристика принадлежности передаваемой сущности);

OT — Object Type (тип сущности по содержанию);

OSI — open systems interconnection (базовая эталонная модель взаимодействия открытых систем);

PKE — битовый флаг, определяет наличие полей PKL и PBK;

PBK — Public Key (данные публичного ключа);

SMS — Short Message Service (служба коротких сообщений);

TCP — Transmission Control Protocol (протокол управления передачей);

Telnet — teletype network (сетевой протокол для реализации текстового интерфейса по сети);

TM — Time (время формирования записи на стороне отправителя);

TMFE — Time Field Exists (битовое поле, определяющее наличие в данном пакете поля TM);

UDP — User Datagram Protocol (протокол пользовательских датаграмм).

4 Общие положения

Сетевая модель взаимодействия открытых систем согласно ГОСТ Р ИСО/МЭК 7498-1-99 определяет следующие уровни обмена данными:

- физический;
- канальный;
- сетевой;

- транспортный;
- сеансовый;
- представления данных;
- прикладной.

В терминах сетевой модели OSI в системах передачи данных транспортной телематики для передачи данных между бортовыми устройствами и инфраструктурой:

- транспортный уровень — протокол TCP;
- сетевой уровень — протокол IP.

Соответствие сетевой модели OSI, стека протоколов TCP/IP и протоколов передачи данных систем транспортной телематики представлено в таблице 1.

Таблица 1

Модель OSI		Стек протоколов TCP/IP		Протоколы TCP/IP	Протоколы систем транспортной телематики
Номер уровня	Название уровня	Номер уровня	Название уровня		
7	Прикладной	4	Прикладной	FTP, HTTP, POP3, IMAP, telnet, SMTP, DNS, TFTP	Уровень поддержки услуг
6	Представления данных				
5	Сеансовый				Транспортный уровень
4	Транспортный	3	Транспортный	TCP, UDP	TCP
3	Сетевой	2	Межсетевой	IP	IP
2	Канальный	1	Управления доступом к среде передачи данных	—	—
1	Физический				—

Настоящий стандарт устанавливает требования к протоколу транспортного уровня обмена информацией между элементами систем транспортной телематики.

5 Протокол транспортного уровня

5.1 Субъекты взаимодействия

5.1.1 Обмен данными между бортовым навигационно-связным оборудованием и системами и аппаратно-программными комплексами осуществляется при помощи сетей беспроводной связи.

5.1.2 Субъектами взаимодействия в рамках унифицированного протокола для целей обслуживания объекта мониторинга и управления являются:

- бортовое навигационно-связное оборудование, установленное на объекте мониторинга (БНСО);
- аппаратно-программные комплексы, обслуживающие объект мониторинга, осуществляющие сетевое взаимодействие с аппаратными средствами, установленными на объекте мониторинга.

5.2 Механизмы обеспечения маршрутизации и надежности доставки данных

5.2.1 Обеспечение маршрутизации

В основу протокола транспортного уровня положен принцип гибкой маршрутизации пакетов данных между взаимоувязанными элементами распределенной сети телематических платформ, использующих данный протокол. В качестве адресов маршрутизации используются идентификаторы телематической платформы, которые должны быть уникальны в рамках одной взаимоувязанной сети.

5.2.2 Механизм проверки целостности данных

Проверка целостности передаваемой информации основана на применении контрольных сумм заголовка транспортного уровня и данных уровня поддержки услуг. Принимающая сторона подсчитывает контрольные суммы и сравнивает их с соответствующими значениями, записанными отправляющей стороной в определенные поля пакета. Если контрольные суммы не совпадают, то считается, что целостность нарушена, на что отправляется подтверждение в виде кода ошибки результата обработки.

В целях обеспечения минимизации использования системных ресурсов при обработке пакетов протокола в части транспортного уровня и данных уровня поддержки услуг используются различные поля и алгоритмы обеспечения контроля целостности. При этом используется механизм, основанный на подсчете контрольной суммы передаваемой последовательности байт (CRC).

Для части пакета транспортного уровня используется алгоритм вычисления циклического избыточного кода CRC-8.

Для части пакета уровня поддержки услуг используется алгоритм вычисления циклического избыточного кода CRC-16.

5.2.3 Обеспечение надежности доставки

Отправляющая сторона после передачи пакета ожидает на него подтверждение в виде пакета определенного типа, содержащего идентификатор ранее переданного пакета и код результата его обработки на принимающей стороне. Ожидание проводится в течение определенного промежутка времени, зависящего от типа используемого протокола транспортного уровня (значение данного параметра TL_RESPONSE_TO указано в ГОСТ 33472—2015, приложение А, таблица А.13).

После получения подтверждения отправляющая сторона проводит анализ кода результата. Коды результатов обработки регламентированы протоколом и представлены в таблице В.1 приложения В. Пакет считается не доставленным в том случае, если подтверждение не приходит по истечении времени TL_RESPONSE_TO. Недоставленные пакеты отправляются повторно (количество попыток отправки регламентировано протоколом; в таблице А.13 ГОСТ 33472—2015 указано значение данного параметра — TL_RESEND_ATTEMPTS). По достижении предельного числа попыток отправки канал передачи данных считается ненадежным и производится уничтожение установленной сессии (разрыв соединения в случае использования TCP/IP протокола в качестве транспортного протокола) и попытка создания новой сессии (соединения) через время, определяемое параметром TL_RECONNECT_TO.

5.3 Построение систем и аппаратно-программных комплексов на основе протокола транспортного уровня

5.3.1 Все сервисы в рамках одного аппаратно-программного комплекса соединяются с диспетчером (часть аппаратно-программного комплекса, выполняющая функции координации межсистемного взаимодействия и маршрутизации) и не имеют непосредственных связей между собой.

5.3.2 БНСО также осуществляет взаимодействие с сервисами аппаратно-программного комплекса через компонент «диспетчер». При этом он идентифицируется по специальным пакетам, содержащим уникальный номер БНСО UNIT_ID, назначаемый ему при регистрации в сети, а также другие учетные данные и информацию о состоянии модулей и блоков БНСО.

5.3.3 Протоколом транспортного уровня (далее — протокол) зарезервирован диапазон номеров типов сервисов до 63. Пользовательские сервисы имеют типы с номерами, начиная с 64.

5.3.4 Тахограф и блок СКЗИ тахографа осуществляют взаимодействие с сервисами АИС «ТК» через инфраструктуру ГАИС «ЭРА-ГЛОНАСС». При этом тахограф и блок СКЗИ тахографа идентифицируются по пакетам данных, содержащим уникальные идентификационные номера тахографа и блока СКЗИ тахографа, назначаемые им при регистрации в АИС «ТК».

5.4 Типы данных

5.4.1 Протоколом определены и используются несколько различных типов данных полей и параметров.

5.4.2 Типы данных полей и параметров должны соответствовать ГОСТ 33472—2015 (приложение А, таблица А.2).

5.5 Структуры данных

5.5.1 Состав пакета протокола транспортного уровня представлен на рисунке 1.

Заголовок протокола транспортного уровня	Данные уровня поддержки услуг	Контрольная сумма данных уровня поддержки услуг

Рисунок 1 — Схема состава пакета протокола транспортного уровня

5.5.2 Пакет данных протокола транспортного уровня состоит из заголовка, поля данных уровня поддержки услуг, а также поля контрольной суммы данных уровня поддержки услуг.

5.5.3 Состав пакета транспортного уровня должен соответствовать ГОСТ 33472—2015 (А.5, приложение А).

5.6 Структуры данных пакетов транспортного уровня

Протоколом предусмотрены следующие типы пакетов транспортного уровня:

EGTS_PT_RESPONSE (подтверждение на пакет транспортного уровня);

EGTS_PT_APPDATA (пакет, содержащий данные протокола уровня поддержки услуг);

EGTS_PT_SIGNED_APPDATA (пакет, содержащий данные протокола уровня поддержки услуг с цифровой подписью).

На каждый пакет типа EGTS_PT_APPDATA или EGTS_PT_SIGNED_APPDATA, поступающий от БНСО, блока СКЗИ тахографа на аппаратно-программный комплекс или от аппаратно-программного комплекса на БНСО, блока СКЗИ тахографа, отправляется пакет типа EGTS_PT_RESPONSE, содержащий в поле PID номер пакета из пакета EGTS_PT_APPDATA или EGTS_PT_SIGNED_APPDATA.

5.6.1 Описание и структура данных пакетов EGTS_PT_APPDATA, EGTS_PT_RESPONSE и EGTS_PT_SIGNED_APPDATA должны соответствовать ГОСТ 33472—2015 (А.6, приложение А).

5.7 Структура данных при использовании резервных каналов передачи данных на основе сервисов SMS и LPWAN

5.7.1 Общее описание формата передачи информации при использовании сервисов SMS и LPWAN должно соответствовать ГОСТ 33472—2015 (А.7, А.8, приложения А).

6 Спецификация протокола уровня поддержки услуг

6.1 Назначение протокола уровня поддержки услуг

Протокол уровня поддержки услуг предназначен для обеспечения обмена данными между БНСО, блоком СКЗИ тахографа и системами и аппаратно-программными комплексами в целях обеспечения функционирования информационных услуг. Каждой услуге соответствует отдельный сервис, который является ключевым элементом в рамках системы, построенной с применением протокола.

Протокол уровня поддержки услуг выполняет следующие основные функции:

- обмен информационными сообщениями, содержащими данные для обработки различными сервисами, а также запросы на выдачу информации сервисами;
- обеспечение уведомления о результатах доставки и обработки данных уровня поддержки услуг;
- идентификация принадлежности данных определенному типу сервиса;
- определение характеристики данных (число, тип, состав, размер, кодировка и др.).

6.1.1 Обмен информационными сообщениями

Основной структурой протокола уровня поддержки услуг, содержащей в себе все необходимые данные для обработки информации или запроса на предоставление той или иной услуги, является запись. Каждая запись может иметь в своем составе несколько подзаписей, содержащих необходимые данные и определяющих действия, которые должен произвести сервис, обрабатывающий данную подзапись.

6.1.2 Обеспечение уведомления о результате доставки и обработки данных уровня поддержки услуг

На уровне поддержки услуг уведомление отправляющей стороны о результате доставки и обработки данных обеспечивается механизмом подтверждений информационных записей при помощи специальных подзаписей, содержащих идентификатор полученной/обработанной записи.

6.1.3 Идентификация принадлежности данных

Для идентификации принадлежности записи тому или иному сервису используется идентификатор типа сервиса, который определяет функциональные особенности и характеристики обрабатываемых данных. Тип сервиса является его идентификатором при внутриплатформенной маршрутизации и является уникальным в рамках протокола.

6.1.4 Определение характеристики данных

Данные в протоколе уровня поддержки услуг записываются в виде подзаписи, имеющей свой уникальный идентификатор в рамках отдельного типа сервиса, а также строго определенную структуру организации данных в зависимости от подзаписи. Использованием такой организации данных в протоколе достигается однозначное определение типа данных, их физического смысла, размера и способа упаковки.

6.2 Определение структур данных

6.2.1 Общая структура

Общая структура протокола уровня поддержки услуг, которая входит в состав пакета протокола транспортного уровня (см. раздел 5), может содержать одну или несколько записей, идущих одна за другой и имеющих различный состав данных, предназначенных разным сервисам.

6.2.1.1 Структуры и состав отдельных записей должны соответствовать ГОСТ 33472—2015 (В.2, приложение В).

7 Перечень сервисов, поддерживаемых в протоколе

Протоколы уровня поддержки услуг обеспечивают обмен данными между БНСО, блоком СКЗИ тахографа и системами и аппаратно-программными комплексами в целях обеспечения функционирования информационных услуг. Каждой услуге соответствует отдельный сервис, который является ключевым элементом в рамках системы, построенной с применением протокола.

Перечень сервисов, поддерживаемых данной версией протокола, приведен в таблице 2.

Таблица 2 — Перечень сервисов, поддерживаемых настоящей версией протокола

Код	Наименование сервиса	Описание сервиса	Спецификация сервиса
1	EGTS_AUTH_SERVICE	Сервис предназначен для осуществления процедуры аутентификации БНСО, блока СКЗИ тахографа на авторизующей ТП	См. раздел 9
2	EGTS_TELEDATA_SERVICE	Сервис предназначен для обработки телематической информации (координатные данные, данные о срабатывании датчиков и т. д.), поступающей от БНСО, блока СКЗИ тахографа	См. раздел 8
3	EGTS_COMMANDS_SERVICE	Сервис предназначен для передачи управляющих и конфигурационных команд, информационных сообщений и статусов между БНСО, блоком СКЗИ тахографа и ТП	См. раздел 10
4	EGTS_FIRMWARE_SERVICE	Сервис предназначен для передачи на БНСО конфигурации и непосредственно самого программного обеспечения аппаратной части БНСО, блока СКЗИ тахографа, а также различного периферийного оборудования, подключенного к БНСО, блоку СКЗИ тахографа и поддерживающего возможность удаленного обновления программного обеспечения	См. раздел 11
10	EGTS_ECALL_SERVICE	Сервис, обеспечивающий выполнение функционала системы ЭРА-ГЛОНАСС	См. раздел 12

Код сервиса, указанный в таблице 2, указывается в заголовке записи протокола уровня поддержки услуг — поля SST и RST.

8 Спецификация сервиса передачи и обработки мониторинговой информации EGTS_TELEDATA_SERVICE

8.1 Требования к БНСО для использования услуги EGTS_TELEDATA_SERVICE

8.1.1 Для использования сервиса EGTS_TELEDATA_SERVICE на стороне БНСО должны быть также реализованы следующие функции:

- поддержка сервиса обработки команд EGTS_COMMANDS_SERVICE (см. раздел 10);
- обработка команд управления и установки параметров БНСО, отправляемых оператором через GPRS, и передача соответствующих подтверждений на них (подробнее см. 8.3).

8.2 Состав сервиса EGTS_TELEDATA_SERVICE

Сервис EGTS_TELEDATA_SERVICE предназначен для передачи от БНСО на ТП мониторинговой информации.

8.2.1 Список и описание подзаписей, используемых сервисом EGTS_TELEDATA_SERVICE, должен соответствовать ГОСТ 33472—2015 (Б.2, приложение Б).

8.3 Использование EGTS_COMMANDS_SERVICE

Списки и описание команд, подтверждений на команды, а также списки параметров БНСО, необходимых для реализации услуги EGTS_TELEDATA_SERVICE, должны соответствовать ГОСТ 33472—2015 (Б.3, приложение Б).

9 Спецификация сервиса аутентификации EGTS_AUTH_SERVICE

9.1 Общие положения

БНСО инициирует обмен данными с запросом к авторизующей ТП на идентификацию (путем передачи записи с идентификационными данными на авторизующую ТП).

БНСО может быть зарегистрирована как в БД одной «домашней» авторизующей ТП, так и на нескольких, произвольно удаленных ТП.

Авторизующая ТП — платформа, которая принимает запись с запросом на идентификацию от БНСО. Кроме того, эта платформа проверяет полученные данные (идентификаторы, тип клиента) в своей БД и, при необходимости, производит запрос к БНСО, используя имеющуюся таблицу маршрутизации.

Запись с запросом на идентификацию содержит следующие данные:

- идентификатор БНСО, который необходим для регистрации в базе данных (далее — БД) авторизующей ТП;
- набор данных, которые необходимы для однозначной идентификации БНСО на стороне авторизующей ТП.

Данный тип сервиса применяется для:

- осуществления процедур идентификации и аутентификации при установлении соединения между БНСО и авторизующей ТП;
- получения учетных данных БНСО на стороне авторизующей ТП;
- получения информации на авторизующей ТП об инфраструктуре на стороне БНСО, например составе и версиях ПО модулей, блоков, периферийного оборудования и т.д. Данная функция настоящего сервиса является опциональной, и БНСО сама принимает решение об объеме информации, отправляемой на авторизующую ТП;
- получения информации на авторизующей ТП о ТС;
- передачи авторизующей ТП на БНСО перечня поддерживаемых сервисов;
- передачи авторизующей ТП на БНСО данных о способе и параметрах шифрования;
- передачи БНСО на авторизующую ТП аутентификационных данных для реализации шифрования данных;
- реализации алгоритма «запросов» на использование сервисов на стороне БНСО. Настоящий протокол предполагает реализацию использования сервисов авторизующей ТП на стороне БНСО. Следует различать «простой» алгоритм использования сервисов и алгоритм «запросов». «Простой» алгоритм подразумевает, что для БНСО доступны все сервисы, и в этом случае авторизуемой ТП разрешено сразу отправлять данные для требуемого сервиса после прохождения процедуры авторизации. Алгоритм «запросов» на использование сервисов подразумевает, что перед тем, как использовать тот или иной тип сервиса (отправлять данные), БНСО должна получить от авторизующей ТП информацию о доступных для использования сервисов. «Запрос» на использование сервисов может быть выполнен как на этапе авторизации, так и после нее;
- передачи БНСО от авторизующей ТП результатов процедуры аутентификации.

Сервис должен быть использован БНСО только в случае применения в качестве транспорта протокола TCP/IP после создания каждого нового соединения с авторизующей ТП.

Описание полного пакета подзаписей сервиса EGTS_AUTH_SERVICE для реализации перечисленных выше функций приведено в 9.2.

Описание алгоритма авторизации БНСО на авторизующей ТП приведено в приложении Б.

9.2 Описание подзаписей сервиса EGTS_AUTH_SERVICE

9.2.1 Список подзаписей, используемых сервисом EGTS_AUTH_SERVICE, должен соответствовать ГОСТ 33472—2015 (В.3.2.2, приложение В).

10 Спецификация сервиса управления и конфигурирования EGTS_COMMANDS_SERVICE

Данный тип сервиса предназначен для обработки команд, сообщений и подтверждений, передаваемых между БНСО, ТП и клиентскими приложениями.

10.1 Описание подзаписей

10.1.1 Описание и список подзаписей сервиса EGTS_COMMAND_SERVICE должен соответствовать ГОСТ 33472—2015 (В.3.4, приложение В).

11 Спецификация сервиса EGTS_FIRMWARE_SERVICE

Данный тип сервиса предназначен для передачи на БНСО конфигурации и обновления ПО аппаратной части модулей и блоков самой БНСО, а также периферийного оборудования, подключенного к БНСО.

11.1 Описание подзаписей

Для осуществления взаимодействия в рамках данного сервиса используется несколько подзаписей, описание и код которых указаны в ГОСТ 33472—2015 (В.3.3, приложение В).

12 Спецификация сервиса экстренного реагирования при аварии EGTS_ECALL_SERVICE

12.1 Назначение сервиса экстренного реагирования при аварии

Сервис экстренного реагирования предназначен для обеспечения возможности реализации функционала по оказанию базовой услуги реагирования при аварии, предоставляемой системой. В протоколе уровня поддержки услуг этот сервис определен как EGTS_ECALL_SERVICE и имеет код 10.

12.2 Минимально необходимый набор функций БНСО для использования услуги EGTS_ECALL_SERVICE

Для использования автомобильной системой вызова экстренных оперативных служб сервиса EGTS_ECALL_SERVICE в БНСО должен быть реализован набор функций, указанных в ГОСТ 33465—2015 (подраздел 7.2).

12.3 Состав и описание подзаписей сервиса EGTS_ECALL_SERVICE

Для осуществления взаимодействия в рамках сервиса EGTS_ECALL_SERVICE используется несколько подзаписей, описание и код которых определены в ГОСТ 33465—2015 (подраздел 7.3).

12.4 Использование сервиса EGTS_COMMANDS_SERVICE

Описание, состав и форматы подзаписей сервиса EGTS_COMMANDS_SERVICE, используемого в целях оказания базовой услуги системы экстренного реагирования при авариях, приведены в разделе 10.

12.5 Список и описание команд, параметров и подтверждений при использовании сервиса EGTS_ECALL_SERVICE

Список и описание команд БНСО и подтверждений, необходимых для реализации базовой услуги, а также список параметров БНСО, определены в ГОСТ 33465—2015 (подраздел 7.5 и таблицы 46 и 47).

12.6 Формат сообщения AL-ACK

Настоящий протокол также устанавливает требования к формату сообщения AL-ACK, которое высылается посредством использования тонального модема [4].

Сообщение AL-ACK, направляемое системой экстренного реагирования при авариях в сторону БНСО и содержащее подтверждение корректности минимального набора данных, принятого с использованием тонального модема, должно высылаться также посредством использования тонального модема.

Сообщение AL-ACK должно иметь формат, определенный в ГОСТ 33465—2015 (подраздел 8.2).

13 Спецификация протокола обмена телематическими данными с применением криптографической защиты данных

13.1 Общие сведения

Передача телематических данных о позиционировании транспортных средств реализуется с помощью протокола, использующего криптографическую защиту данных посредством шифрования по алгоритмам. Использование шифрования обеспечивает гарантию некорректируемости, конфиденциальности и достоверности данных.

Протокол разделен на четыре функциональные части:

- управление БНСО — обеспечивает передачу команд управления состояниями БНСО, настройки БНСО, настройки шифрования на БНСО;
- мониторинг БНСО — обеспечивает передачу данных о внутренних событиях от БНСО;
- обновление БНСО — обеспечивает передачу команд на обновление программного обеспечения БНСО;
- телематические данные БНСО — обеспечивает передачу данных о местоположении от БНСО.

13.2 Протокол уровня приложения

Протокол взаимодействия является асинхронным, то есть пакеты передаются без ожидания ответа на предыдущий пакет. Пакеты, не получившие ответа, присылаются повторно при следующем сеансе связи.

Сообщения, содержащие координаты, параметры, события и данные самодиагностики, объединяются в пакеты. Каждый пакет объединяется единым заголовком и шифруется криптографическими методами. Рекомендованный размер пакетов: 10—20 Кб. Все полученные пакеты хранятся в хронологическом порядке. Подтверждения о получении пакета не шифруются.

Сообщения-команды к БНСО передаются независимо от пакетов с сообщениями и ответов на них. Команды шифруются. Ответы от БНСО о получении команды не шифруются.

13.2.1 Авторизация

При установлении TCP-соединения проводится процедура авторизации. В случае неуспешного прохождения процедуры авторизации сервер проводит обрыв соединения. Описание сообщения авторизации БНСО приведено в таблице 3.

Таблица 3 — Описание сообщения авторизации БНСО

Поле	Размер	Описание
Версия	2	Текущая версия протокола
Уникальный номер устройства	8	Уникальный идентификатор БНСО

Пример сообщения авторизации:

Байты	***0***	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	
Значения	***02***	***05***	***60***	***a5***	***b4***	***92***	***60***	***41***	***01***	***00***	
			Уникальный номер устройства								***SERIAL 0x0001416092b4a560 = 353358010688864***
	Версия протокола										***n.m***

Передается версия протокола и уникальный номер БНСО.

13.2.2 Типы сообщений

Перечень типов сообщений приведен в таблице 4.

Таблица 4 — Перечень типов сообщений

Код	Тип сообщения	Описание
0x01	POSITION	Передача координат от БНСО
0x02	PARAM	Передача параметров от БНСО
0x03	EVENT	Передача информации о событиях БНСО
0x04	TEST	Передача данных самодиагностики БНСО
0x0F	Подтверждение	Подтверждение получения пакета от сервера
0x1F	Команда	Передача команды на БНСО
0x2F	Ответ на команду	Ответ от БНСО
0x3F, 0x5F, 0x6F, 0x7F, 0x8F	Обновление встроенного ПО	Обновление встроенного ПО БНСО либо отдельных его модулей, контрольные точки
0x4F	Ответ на обновление встроенного ПО	Ответ от БНСО

13.2.3 Общий формат заголовка пакета

Заголовок пакета имеет структуру, приведенную в таблице 5.

Таблица 5 — Структура заголовка пакета

Поле	Размер	Описание
Номер пакета	2	Номер пакета начинается с 0000, заканчивается FFFF, передача происходит раз в 30 с, 22 сут
Количество байт	2	Количество байт в посылке без учета первых шести
Время формирования	4	Время формирования посылки в формате UNIXTime Часовой пояс — UTC
Ключ	32	Ключ шифрования
Имитовставка	4	Имитовставка
Вектор инициализации	8	Вектор инициализации шифрования
Имитовставка данных	4	Имитовставка шифруемых данных
Номер набора ключей	1	Номер набора ключей
Проверочное число	1	Произвольное число, которое шифруется вместе с данными, идущими после заголовка. Данное число возвращается в ответе

Пример заголовка:

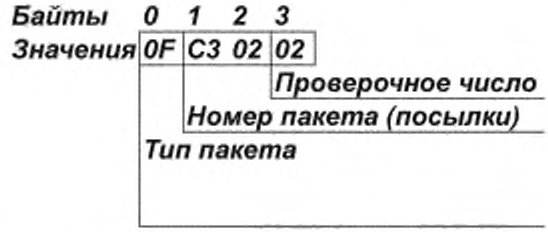


Общий формат ответа (подтверждения от сервера) приведен в таблице 6.

Таблица 6 — Общий формат ответа

Поле	Размер
Тип пакета	1
Номер пакета (посылки)	2
Проверочное число	1

Пример подтверждения:



13.2.4 Управление БНСО

13.2.4.1 Сообщения типа «Параметр»

Сообщения типа «Параметр» имеют структуру, приведенную в таблице 7.

Таблица 7 — Сообщения типа «Параметр»

Поле	Размер	Описание
Тип сообщения	1	Тип сообщения PARAM
Количество байт	1	Количество байт данных (без учета полей «Тип сообщения» и «Количество байт»)
Код параметра	1	Код параметра описан в таблице 8
Значение	2(1+)	

Описание кодов параметра управления БНСО приведено в таблице 8.

Таблица 8 — Описание кодов параметра управления БНСО

Наименование атрибута	Код	Значение
Периодичность записи координат	01	Целое положительное в секундах
Периодичность отправки координатных последовательностей	02	Целое положительное в секундах
Набор классов ТС, доступных для установки	03	Битовая маска
Набор регистрируемых событий	04	Битовая маска по порядку номеров событий
Статус сервисного разъема	05	Целое положительное (01 — включено или 00 — выключено)
Номер набора ключей	06	Целое положительное
Статус (режим) БНСО	07	Целое положительное (перечень возможных значений см. в таблице 9)
Световая индикация	08	00 — красная, 01 — зеленая, 02 — желтая
Периодичность записи событий (не используется)	09	Целое положительное в секундах
Периодичность отправки событий	10	Целое положительное в секундах

Пример сообщения «Параметр»:



Передается параметр «Периодичность записи координат» (01) со значением 0x0003 = 3 с.
Перечень кодов статуса (состояние/режим) БНСО приведен в таблице 9.

Таблица 9 — Перечень кодов статуса (состояние/режим) БНСО

Статус (состояние/режим) БНСО	Код
Не активно	01
Хранение	02
Транспортировка	03
Штатный	04
Ожидание	05
Вне территории Российской Федерации	06
Аварийный	07
Блокировка логическая	08
Сервисный	09
Блокировка аппаратная (нарушена целостность корпуса БНСО)	10

13.2.4.2 Сообщения типа «Команда»

БНСО способно принимать команды, в соответствии с которыми оно выполняет те или иные действия. Сообщения типа «Команда» имеют структуру, приведенную в таблице 10.

Таблица 10 — Структура сообщений типа «Команда»

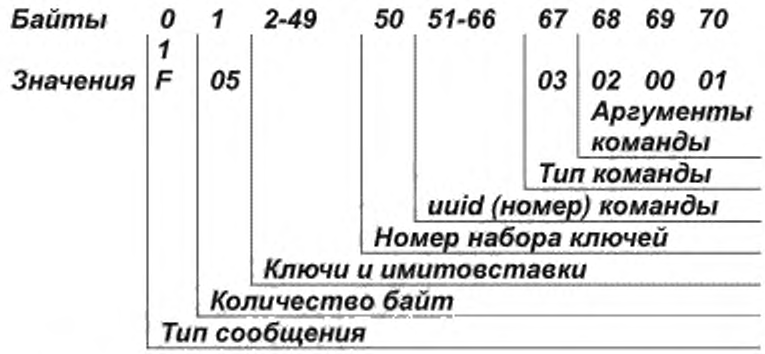
Поле	Размер, байт	Описание
Тип сообщения	1	Тип сообщения — Команда
Количество байт	1	Количество байт данных (без учета полей «Тип пакета» и «Количество байт»)
Ключи и имитовставки	48	Аналогично общему заголовку
Номер набора ключей	1	Номер набора ключей
Номер команды	16	Uuid команды
Тип команды	1	Код команды
Аргументы команды	0+	Аргументы команды

Перечень типов команд приведен в таблице 11.

Таблица 11 — Типы (коды) команд

Код	Команда	Аргументы команды
01	Проведение самодиагностики	0 байт
02	Считать параметр	1 байт — код параметра. При значении байта 0xFF последовательно возвращаются все параметры
03	Задание параметра	2 или более байт. Первый — номер параметра, далее его задаваемое значение
04	Обновить встроенное программное обеспечение	1 байт — сразу обновлять или после перезагрузки
05	Подача звукового сигнала	1 байт — количество секунд
06	Записать контрольные точки	0 байт

Пример сообщения-команды:



Обычное значение параметра 03 с id = 02 (Периодичность отправки координатных последовательностей) — 0x0001 = 1 с.

Формат ответа БНСО на команды приведен в таблице 12.

Таблица 12 — Ответы на команды от БНСО

Поле	Размер	Описание
Тип сообщения	1	Тип сообщения — ответ на команду
Длина	1	Длина данных в пакете
Uuid	16	Uuid команды
Результат	1	Код результата выполнения команды

Коды результатов выполнения команд приведены в таблице 13.

Таблица 13 — Коды результатов выполнения команд

Результат	Значение
0x00	Успешно
0x01	Выполняется
0x02	Готова к продолжению (для обновления встроенного ПО в новой сессии)
0x03	Аналогичная команда уже выполнена
0xFD	Выполнение отменено
0xFE	Недопустимые аргументы
0xFF	Иные ошибки

Пример сообщения с ответом на команду:



Ответ на команду от БНСО — выполнение отменено.

13.2.5 Мониторинг БНСО

13.2.5.1 Сообщения типа «Событие» (EVENT)

Сообщения типа EVENT имеют структуру, приведенную в таблице 14.

Таблица 14 — Структура сообщения типа EVENT

Поле	Размер	Описание
Тип сообщения	1	Тип сообщения EVENT
Количество байт	1	Количество байт данных (без учета полей «Тип пакета» и «Количество байт»)
Код параметра	1	Код параметра, описан в таблице 15
Значение	0+	Опционально — значение параметра

Описание кодов событий БНСО приведено в таблице 15.

Таблица 15 — Описание кодов событий БНСО

Наименование параметра	Код	Значение
Изменен режим работы БНСО	01	2 байта — старый и новый статусы
Начало движения ТС	02	
Конец движения ТС	03	
Нарушение целостности корпуса БНСО	04	
Запуск самодиагностики	05	
Результат самодиагностики	06	1 байт; 1 — успешно, 0 — ошибки
Запуск обновления встроенного ПО	07	
Результат обновления встроенного ПО	08	1 байт; 1 — успешно, 0 — сбой
Длительная потеря сигнала ГНСС	09	
Определение помех сигналу ГНСС	10	
Длительная потеря сигнала GSM	11	
Определение помех сигналу GSM	12	
Изменение используемой базовой станции	13	8 байт; 4 байта целое — LAC, 4 байта — CELL ID
Неспособность определить положение БНСО	14	
Прохождение известной точки контроля	15	8 байт — широта, долгота точки
Выезд за пределы Российской Федерации	16	
Въезд на территорию Российской Федерации	17	
Установка нового класса ТС	18	1 байт — номер класса
Бортовое питание выкл.	19	
Бортовое питание вкл.	20	
Уменьшение заряда батареи до критического уровня	21	1 байт; 0 — основная батарея, 1 — резервная
Восстановление батареи выше критического уровня	22	1 байт; 0 — основная батарея, 1 — резервная
Увеличение количества циклов перезаряда аккумулятора	23	2 байта — количество циклов перезарядки
Информация об ошибках ПО БНСО	24	1 байт — код ошибки
Информация о неисправностях	25	1 байт — код ошибки
Достижение значения заряда батареи	26	2 байта: первый — целое, значение в процентах, второй байт — заряжается или разряжается батарея (1 — заряжается, 0 — разряжается)
Отключение при разрядке батареи	27	

Пример сообщения EVENT:



Пакет передает событие «Результат самодиагностики» со значением «1» — успешно.

13.2.5.2 Сообщения типа «Самодиагностика» (TEST)

Формат сообщения «Самодиагностика» приведен в таблице 16.

Таблица 16 — Формат сообщения «Самодиагностика»

Поле	Размер	Описание
Тип сообщения	1	Тип сообщения TEST
Количество байт	1	Количество байт данных (без учета полей «Тип пакета» и «Количество байт»); всегда 1
Битовая маска	1	Битовая маска XXXXX000 Код параметра описан в таблице 17; 0 — ошибка, 1 — успешно

Описание кодов самодиагностики приведено в таблице 17.

Таблица 17 — Описание кодов самодиагностики

Наименование параметра	Код
Целостность образа программного обеспечения	01
Работоспособность коммуникационного модуля	02
Работоспособность модуля позиционирования бортового устройства	03
Работоспособность модуля СКЗИ	04
Работоспособность модуля электропитания	05

Пример сообщения самодиагностики:



F8 (11111000) — все исправно.

При получении команды на проведение самодиагностики БНСО сначала отправляет результаты самодиагностики, а затем — ответ на команду.

13.2.6 Обновление БНСО

В процессе обновления встроенного ПО БНСО принимают участие как специальные типы сообщений для передачи обновленной версии встроенного программного обеспечения, так и сообщения типа «Команда».

Схема процесса «Обновление БНСО» приведена на рисунке 2.

Формат сообщения для обновления ПО приведен в таблице 18.

Таблица 18 — Формат сообщения для обновления ПО

Поле	Размер	Описание
Тип сообщения	1	Тип сообщения: 0x3F — сообщение с основным встроенным ПО 0x4F — сообщение с ответом по основному встроенному ПО 0x5F — резерв для встроенного ПО отдельных модулей (ГНСС, GSM, модуль шифрования) 0x6F — сообщение с ответом по версии встроенного ПО модуля 0x7F — контрольные точки 0x8F — сообщение с ответом по контрольным точкам
Количество байт	2	Количество байт данных (без учета полей «Тип сообщения» и «Количество байт»)
Ключи и имитовставки	48	Аналогично общему заголовку
Номер ключевого набора	1	Номер набора ключей
Номер текущего пакета	2	Номер текущего сообщения из общего количества частей ПО
Всего пакетов	2	Количество сообщений, которое будет передано на БНСО. До конца передачи БНСО не рвет сессию
Часть файла обновления встроенного ПО	N	Байты файла обновления встроенного ПО

При передаче контрольных точек вместо файла содержащего обновленное встроенное ПО передается файл с точками. Формат данного файла протоколом не ограничивается.

Пример сообщения с обновлением встроенного программного обеспечения:

Байты	***0***	***1 2***	***3-50***	***51 52 53***	***54 55***	***56 – (56+N)***
Значения	***3F***	***05 03***		***A1 00***	***F1 00***	***Часть файла «прошивки»***
					Всего сообщений	
				Номер текущего сообщения		
			Ключи и имитовставки			
		Количество байт				
	Тип сообщения					

Формат ответа (подтверждения) на команду запуска процедуры обновления встроенного ПО от БНСО приведен в таблице 19.

Таблица 19 — Формат ответа (подтверждения) на команду запуска процедуры обновления встроенного ПО от БНСО

Поле	Размер	Описание
Тип сообщения	1	
Количество байт	1	Количество байт данных
Номер посылки	2	

Пример ответа на обновление:

Байты	***0***	***1***	***2***	***3***
Значения	***4F***	***C3***	***02***	***02***

Номер посылки

Количество байт

Тип сообщения

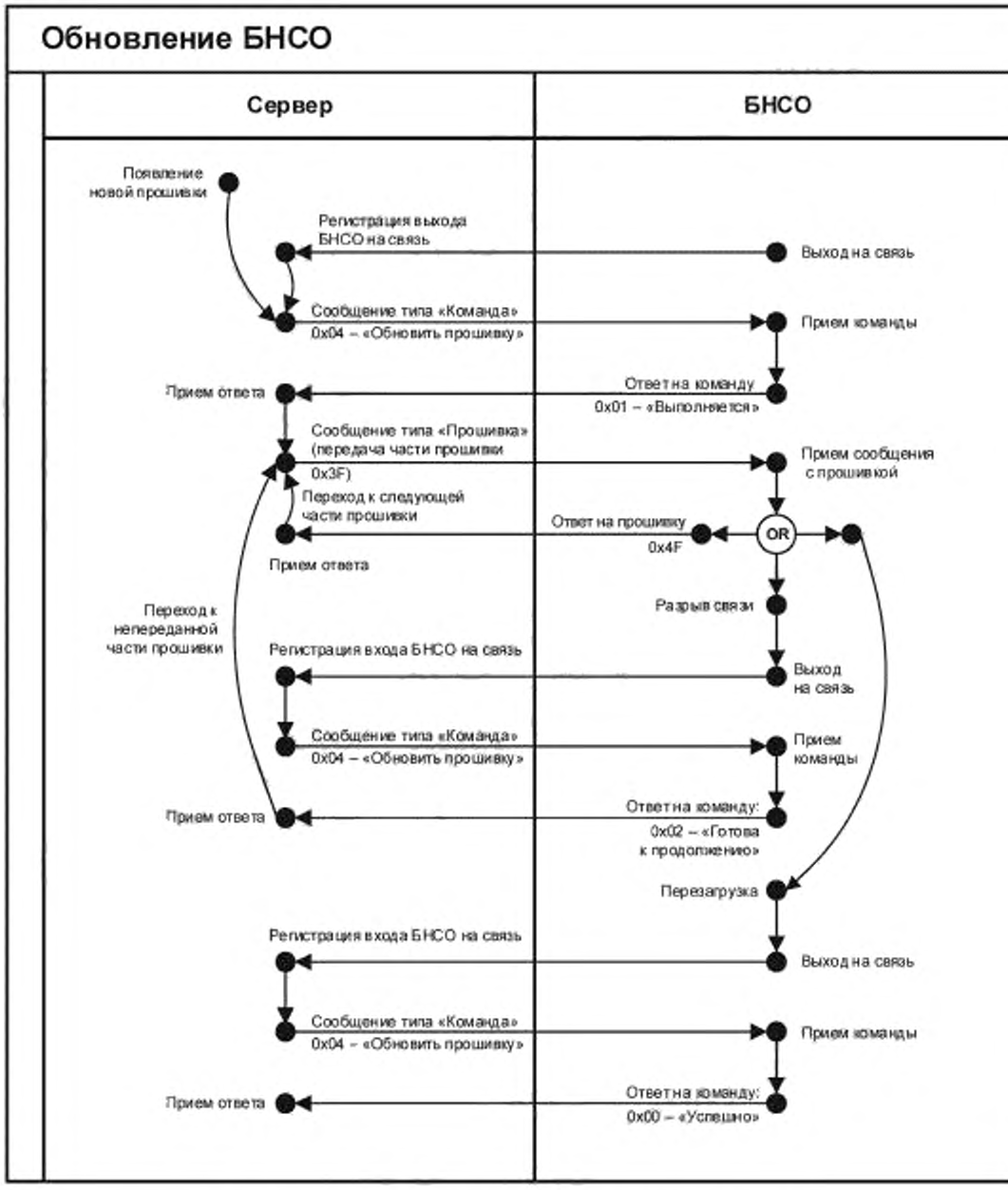


Рисунок 2 — Схема процесса «Обновление встроенного ПО БНСО»

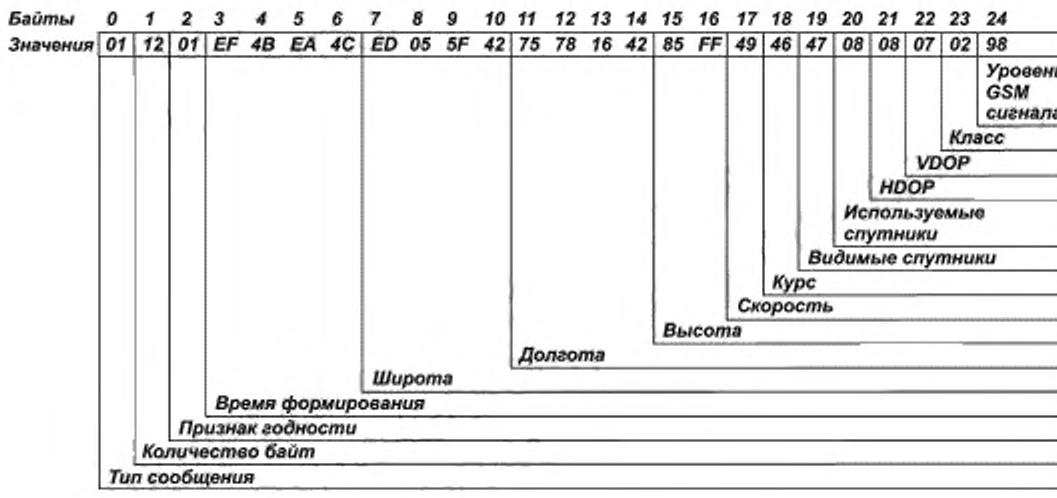
13.2.7 Передача данных о местоположении ТС

Сообщения с координатами сохраняются с определенной частотой и отправляются через заданные интервалы времени, объединенные в пакеты. Формат сообщения «Координаты БНСО» приведен в таблице 20.

Таблица 20 — Формат сообщения «Координаты БНСО»

Поле	Размер	Описание
Тип сообщения	1	Тип сообщения POSITION
Количество байт	1	Количество байт данных (без учета полей «Тип пакета» и «Количество байт»)
Признак годности	1	Признак годности данных позиционирования (VALID, notVALID)
Время формирования	4	В формате UNIXTime Часовой пояс — UTC
Широта	4	Широта в формате IEEE 754 (положительное число, если N северная; отрицательное число, если S южная), в десятичных градусах, в системе координат ПЗ-90.11
Долгота	4	Долгота в формате IEEE 754 (положительное число, если E восточная; отрицательное число, если W западная), в десятичных градусах, в системе координат ПЗ-90.11
Высота	2	Высота над уровнем моря в метрах, старший бит — знак, обратный код
Скорость	1	Скорость над поверхностью, км/ч
Курс	1	Направление азимута курса в градусах, деленное на 2
Спутники видимые	1	Количество используемых спутников
Спутники используемые	1	Количество видимых спутников
HDOP	1	Целое число. Снижение точности по горизонтали, умноженное на 10
VDOP	1	Целое число. Снижение точности по вертикали, умноженное на 10
Класс БНСО	1	Целое число. Текущий класс БНСО
Уровень сигнала	1	Целое число. Уровень сигнала

Пример пакета с координатными данными:



13.3 Криптографическая защита данных

Для решения задачи обеспечения целостности, конфиденциальности и аутентичности информации, передаваемой БНСО, а также обеспечения требуемого уровня быстродействия используются следующие криптоалгоритмы:

а) конфиденциальность информации обеспечивается шифрованием передаваемых данных с использованием алгоритма;

б) целостность и аутентичность информации обеспечивается путем выработки имитовставки (кода аутентичности сообщения) с использованием алгоритма.

13.3.1 Процесс обмена данными между сервером и БНСО

Процесс обмена данными включает следующие действия:

- Передача данных от БНСО на сервер:
  подготовка данных для передачи от БНСО серверу;
  расшифровка данных на стороне сервера;
- Передача данных от сервера на БНСО:
  подготовка данных для передачи от сервера на БНСО;
  расшифровка данных на стороне БНСО.

Схемы процесса приведены на рисунках 3 и 4.

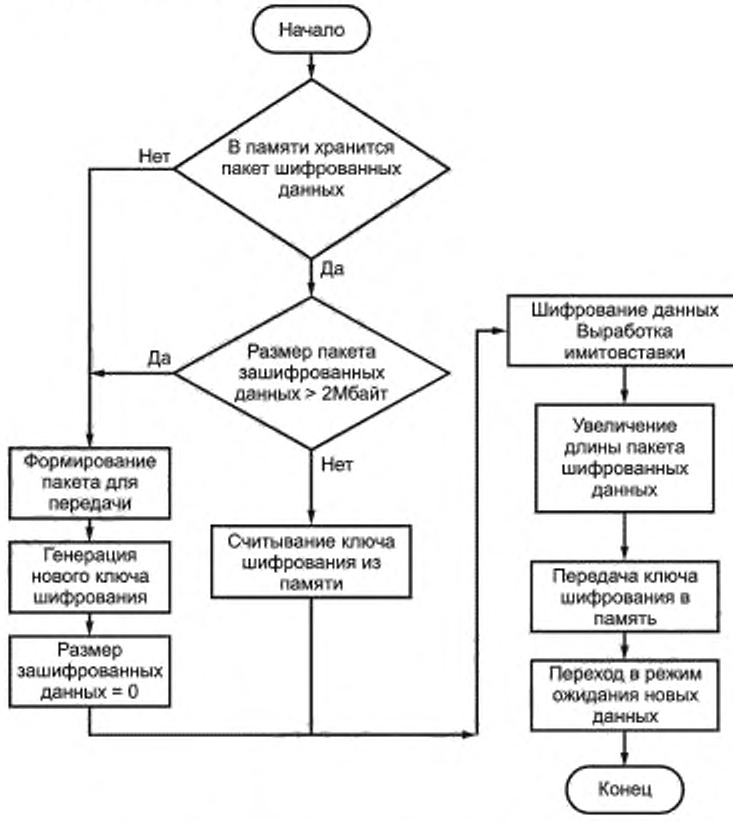


Рисунок 3 — Схема передачи данных от БНСО на сервер



Рисунок 4 — Схема передачи данных от сервера на БНСО

14 Протокол обмена данными тахографа с автоматизированной информационной системой «Тахографический контроль»

Информация, передаваемая от тахографа в АИС «ТК» и от АИС «ТК» в тахограф передается пакетами, формируемыми в тахографе и принимаемыми в тахографе блоком СКЗИ тахографа.

Доступ к тахографической информации, передаваемой в пакетах между блоком СКЗИ тахографа и АИС «ТК», ограничивается с использованием шифрования информации в соответствии с ГОСТ Р 34.12 и ГОСТ Р 34.13.

Зашифрованные пакеты данных удостоверяются кодом аутентификации сообщения (MAC), который проверяется принимающим устройством.

Защита тахографической информации, передаваемой в пакетах между блоком СКЗИ тахографа и АИС «ТК», от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также для обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования тахографической информации осуществляется с использованием криптографической защиты информации в соответствии с ГОСТ Р 34.12 и ГОСТ Р 34.13, а также с использованием создания и проверки электронной подписи в соответствии с ГОСТ Р 34.10 и ГОСТ Р 34.11.

Схема электронной подписи использует следующие два типа алгоритмов:

- необратимый асимметричный алгоритм, содержащий подписывающую функцию Sign[SK](), использующую закрытый ключ SK, и проверяющую функцию Verify[PK](), использующую открытый ключ PK;
- алгоритм вычисления хэш-функции, который преобразовывает последовательность данных произвольной длины в 256-битный хэш-код (хэш-значение).

Протокол обмена информацией блока СКЗИ тахографа с АИС «ТК» является протоколом прикладного уровня.

При этом пакеты прикладного уровня инкапсулируются в пакеты протокола EGTS уровня поддержки услуг с использованием сервиса передачи и обработки мониторинговой информации EGTS_TELEDATA_SERVICE.

На транспортном уровне обмен соответствующими данными проводится в составе пакетов EGTS_PT_APPDATA протокола транспортного уровня.

Описание спецификации протокола обмена данными тахографа с АИС «ТК» представлено в приложении Е.

Приложение А
(справочное)

Описание принципа построения навигационно-информационной системы на основе протокола транспортного уровня

Минимальным и достаточным элементом системы, использующей протокол транспортного уровня, является телематическая платформа. В качестве основной составной части телематической платформы, выполняющей функции координации внутриплатформенного взаимодействия и маршрутизации используется такое понятие как диспетчер.

Протоколом различается логический уровень межплатформенной маршрутизации, данные в котором (информационные пакеты) предаются на уровне отдельных телематических платформ, а также уровень внутриплатформенной маршрутизации, информация в котором предается между отдельными сервисами одной платформы. Под «сервисом» понимается отдельная составная часть телематической платформы, обеспечивающая функциональное выполнение алгоритма той или иной услуги с использованием описываемого протокола транспортного уровня. Во всех указанных типах маршрутизации взаимодействие происходит через диспетчера.

Генераторами и потребителями данных в системе, построенной на основе протокола транспортного уровня, являются сервисы, которые на стороне-отправителе создают пакеты, а на стороне-получателе проводят обработку пакетов, полученных от других сервисов. Каждый сервис реализует различную бизнес-логику в зависимости от функционала той или иной услуги. Тип сервиса является его главной функциональной характеристикой и используется диспетчером для внутриплатформенной маршрутизации данных. Как правило, во взаимодействии участвуют комплементарная пара сервисов, один из которых расположен на стороне абонентского терминала (применительно к настоящему стандарту — БНСО), например генерирует пакеты с координатными данными и показаниями датчиков, а другой на стороне телематической платформы такие данные обрабатывает.

Все сервисы в рамках одной телематической платформы соединяются с диспетчером и не имеют непосредственных связей между собой.

Телематическая платформа может иметь связи с другими платформами и проводить обмен данными на основе данных маршрутизации. Для осуществления маршрутизации диспетчер обращается к локальному хранилищу, содержащему данные о соседних телематических платформах и доступных на них сервисах, а также информацию о сервисах, функционирующих в рамках своей платформы. При организации связи между диспетчерами различных телематических платформ происходит обмен информацией о типах сервисов, доступных на каждой из сторон, а также их статусе. Поиск маршрута сводится к поиску направления (соединения) по типу запрашиваемого сервиса. Если запрашиваемый сервис находится на той же телематической платформе, что и диспетчер, то взаимодействие происходит с использованием только внутриплатформенной маршрутизации. То есть, если имеются соответствующие разрешения, поиск сервиса ведется по данным маршрутизации на соседних телематических платформах, и на нахождении такого маршрута и доступности маршрута происходит трансляция запроса на найденную платформу, при этом в качестве адреса используется идентификатор диспетчера удаленной платформы.

БНСО также осуществляет взаимодействие с сервисами телематической платформы через диспетчера. При этом БНСО идентифицируется по специальным пакетам, содержащим уникальный номер БНСО, назначаемый ей при регистрации в системе, а также другие учетные данные и информацию о внутренней инфраструктуре и состоянии модулей и блоков БНСО.

Структурная схема взаимодействия элементов системы, основанной на описываемом протоколе транспортного уровня, представлена на рисунке А.1. Каждый сервис имеет определенный тип, который на рисунке А.1 определяется параметром SID.

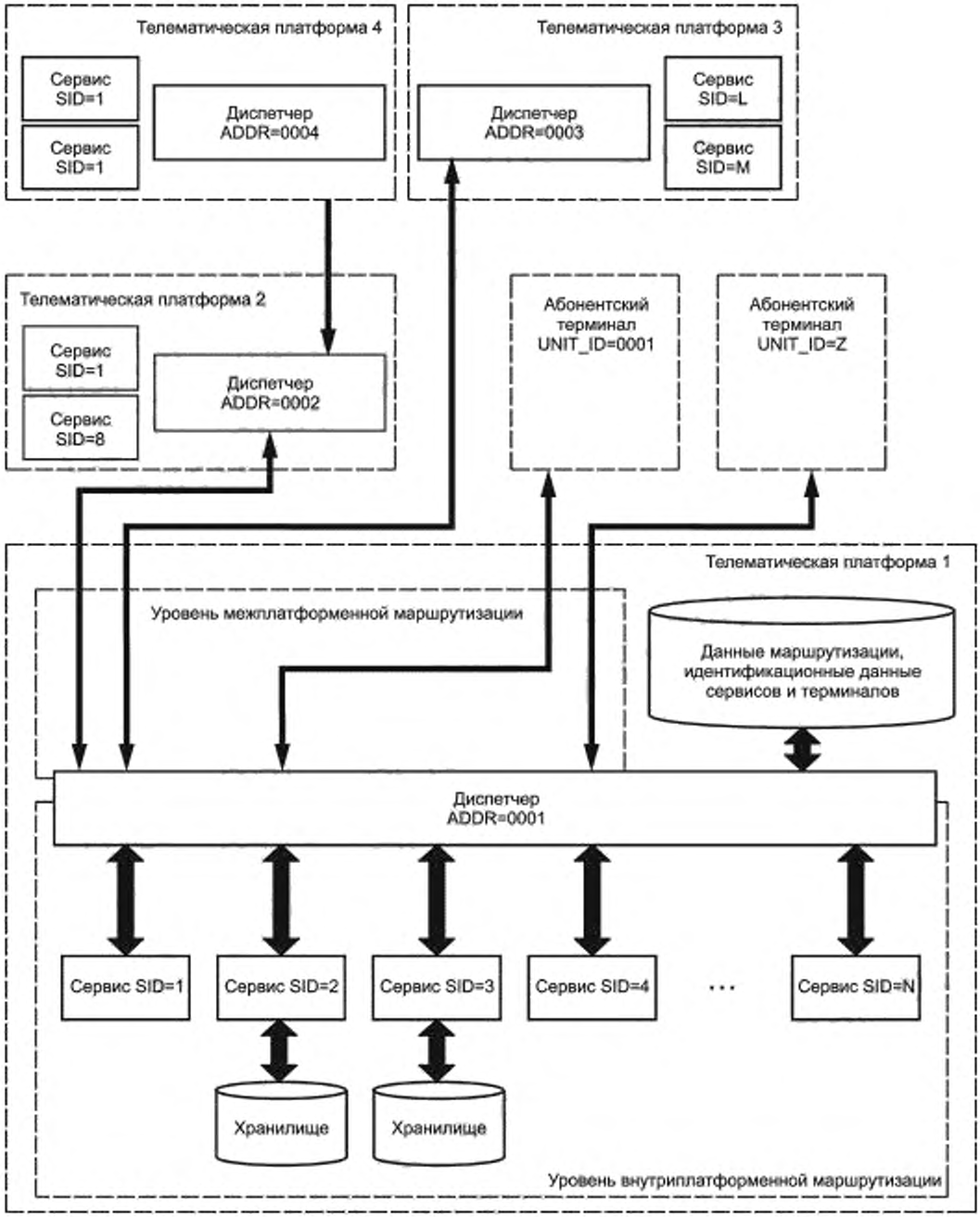


Рисунок А.1 — Структурная схема взаимодействия элементов системы, основанной на протоколе транспортного уровня

Приложение Б
(справочное)

Описание процедуры авторизации БНСО на авторизующей ТП

Для работы БНСО в инфраструктуре оператора ей должен быть назначен уникальный идентификатор UNIT_ID, которому должны соответствовать определенные значения IMEI, IMSI и другие учетные данные БНСО, необходимые для осуществления взаимодействия в системе оператора.

Конфигурирование БНСО может быть проведено одним из способов:

1) после регистрации БНСО в сети GSM или UMTS инфраструктура сотового оператора отслеживает появление нового устройства и инициирует отправку ему зашифрованного SMS-сообщения с учетными данными. Шифрование проводится ключом и алгоритмом, известными данной БНСО и сохраненными к моменту конфигурирования в хранилище оператора. Для определения ключей и алгоритмов шифрования на стороне БНСО используются соответствующие поля из заголовка протокола транспортного уровня, а также данные о ключах, зашитых в памяти БНСО. Учетные данные передаются в виде конфигурационного файла с использованием подзаписи EGTS_SR_SERVICE_FULL_DATA или EGTS_SR_SERVICE_PART_DATA сервиса EGTS_FIRMWARE_SERVICE (описание сервиса см. раздел 11).

Файл конфигурации должен содержать:

- параметр EGTS_GPRS_APN (параметры точки доступа для установления GPRS сессии), параметр EGTS_SERVER_ADDRESS, определяющий адрес и порт сервера, с которым необходимо установить TCP/IP соединение;
- уникальный идентификатор БНСО UNIT_ID. В конфигурационном файле также могут присутствовать другие параметры, необходимые для работы БНСО. Далее БНСО проводит расшифровку SMS-сообщения, проверяет корректность структур данных, вычисляет и сравнивает с полученными в сообщении значениями контрольные суммы. Если расшифровка и проверка прошли успешно, БНСО устанавливает GPRS сессию и соединяется с указанным сервером по TCP/IP. После прохождения процедуры аутентификации БНСО отправляет подтверждение об успешной конфигурации в виде подзаписи EGTS_SR_RECORD_RESPONSE с кодом EGTS_PC_OK на полученную запись EGTS_SR_SERVICE_FULL_DATA или EGTS_SR_SERVICE_PART_DATA сервиса EGTS_FIRMWARE_SERVICE (описание сервиса см. раздел 11).

На рисунке Б.1 представлен описанный алгоритм конфигурирования БНСО;

2) после регистрации БНСО в сети GSM или GPRS устанавливается GPRS сессия и TCP/IP соединение с сервером, информация об адресе которого уже записана в памяти БНСО. При прохождении процедуры аутентификации инфраструктура оператора анализирует параметр TID из подзаписи EGTS_SR_TERM_IDENTITY. Если TID имеет значение 0, проводится процедура конфигурирования при помощи сервиса EGTS_FIRMWARE_SERVICE (описание сервиса см. раздел 11), как описано в способе 1, отправляется файл конфигурации с использованием подзаписи EGTS_SR_SERVICE_FULL_DATA или EGTS_SR_SERVICE_PART_DATA. Далее, после прихода подтверждения получения конфигурационного файла от БНСО, ему отправляется результат авторизации с кодом EGTS_PC_ID_NFOUND, указывающий, что TID = 0 в системе не найден. После этого сервер, не разрывая соединение с БНСО, ожидает повторной авторизации БНСО, но уже с корректным параметром TID.

На рисунке Б.2 приведен описанный алгоритм конфигурирования БНСО.

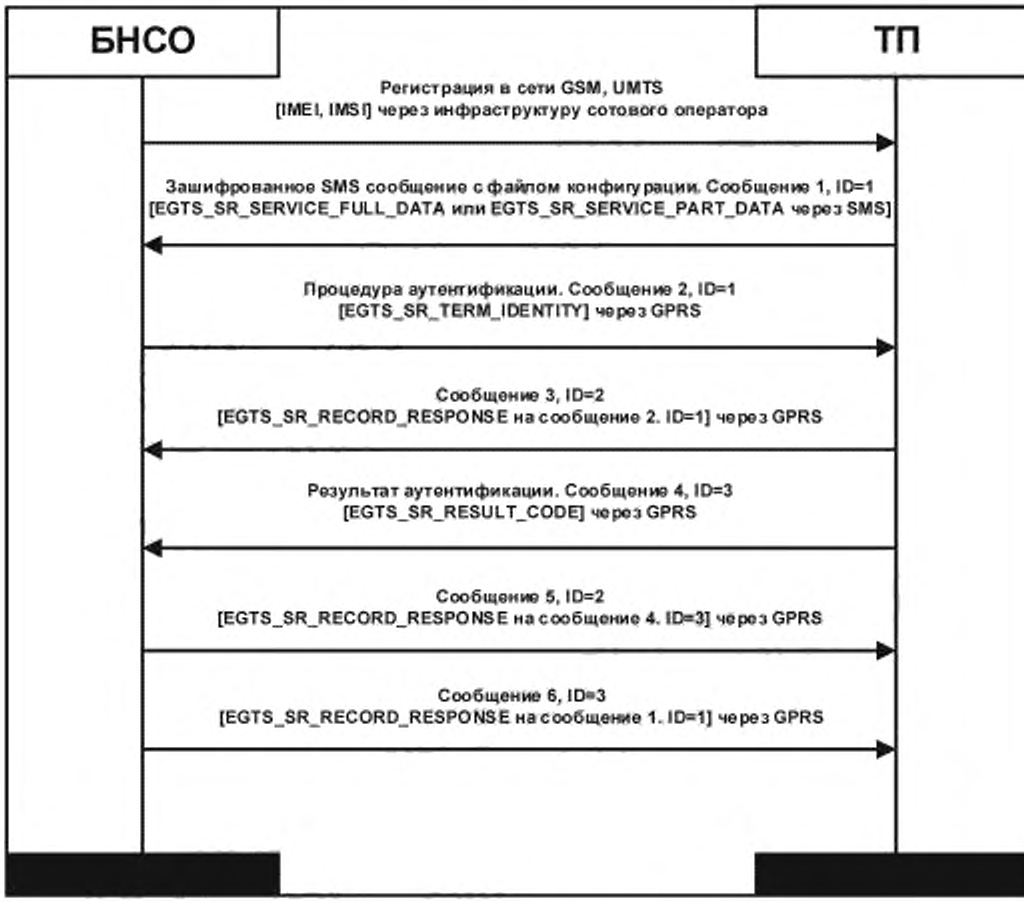


Рисунок Б.1 — Алгоритм конфигурации БНСО с использованием SMS

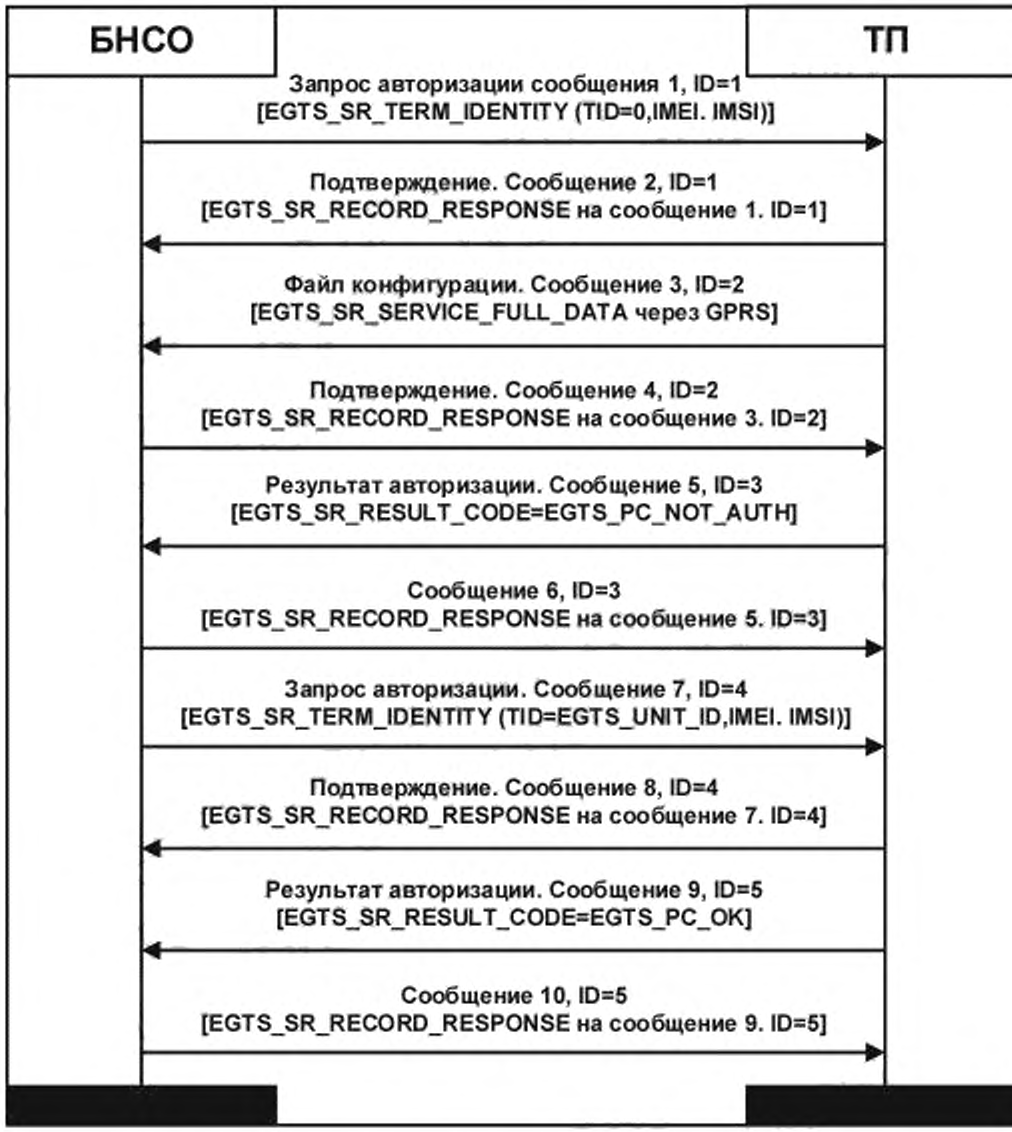


Рисунок Б.2 — Алгоритм конфигурации БНСО с использованием GPRS

Если авторизация прошла успешно, ТП в зависимости от алгоритма запроса использования сервисов может перед подзаписью EGTS_SR_RESULT_CODE добавлять подзаписи типа EGTS_SR_SERVICE_INFO, определяющие состав сервисов, разрешенных для БНСО и поддерживаемых ТП. Это означает, что БНСО сразу после авторизации может использовать только перечисленные сервисы, даже если он предполагает «простой» алгоритм поддержи прав использования сервисов.

Если используется алгоритм «запросов» использования сервисов, то БНСО не может использовать сервисы, разрешение на использование которых не получено от стороны ТП. Причем разрешение на некоторые запрашиваемые сервисы может прийти позже. Например, когда сервисы находятся на удаленных ТП и от этих ТП в асинхронном режиме приходят ответы на запросы. В таком случае ТП, используя имеющиеся данные маршрутизации, отправляет асинхронный запрос на использование сервисов удаленной ТП, если идентификатор HDID указан в подзаписи EGTS_SR_TERM_IDENTITY при авторизации БНСО.

На рисунке Б.3 представлен изложенный алгоритм обмена сообщениями на этапе авторизации БНСО на стороне ТП.

После успешного подключения БНСО к ТП по протоколу TCP/IP БНСО должна быть авторизована. Для передачи первичных аутентификационных данных БНСО должна отправить сообщение, содержащее подзапись EGTS_SR_TERM_IDENTITY (сообщение 1) в течение времени EGTS_SL_NOT_AUTH_TO.

Получив сообщение с подзаписью EGTS_SR_TERM_IDENTITY, ТП отправляет на него сообщение 2 с подтверждением о приеме EGTS_SR_RECORD_RESPONSE на запись с идентификатором ID = 1. Необходимо использовать идентификатор пакета PID = 1 при каждой новой сессии авторизации на ТП. Далее, в зависимости от настроек (используется ли шифрование, применяется ли дополнительный алгоритм авторизации), ТП отправляет пакет (сообщение 3) с подзаписью EGTS_SR_AUTH_PARAM, содержащей параметры, необходимые для осуществления шифрования и/или алгоритма расширенной авторизации. Если шифрование и алгоритм расширенной авторизации не используется, то вместо подзаписи EGTS_SR_AUTH_PARAM ТП может отправить подзапись EGTS_SR_RESULT_CODE с результатом проведения процедуры авторизации БНСО.

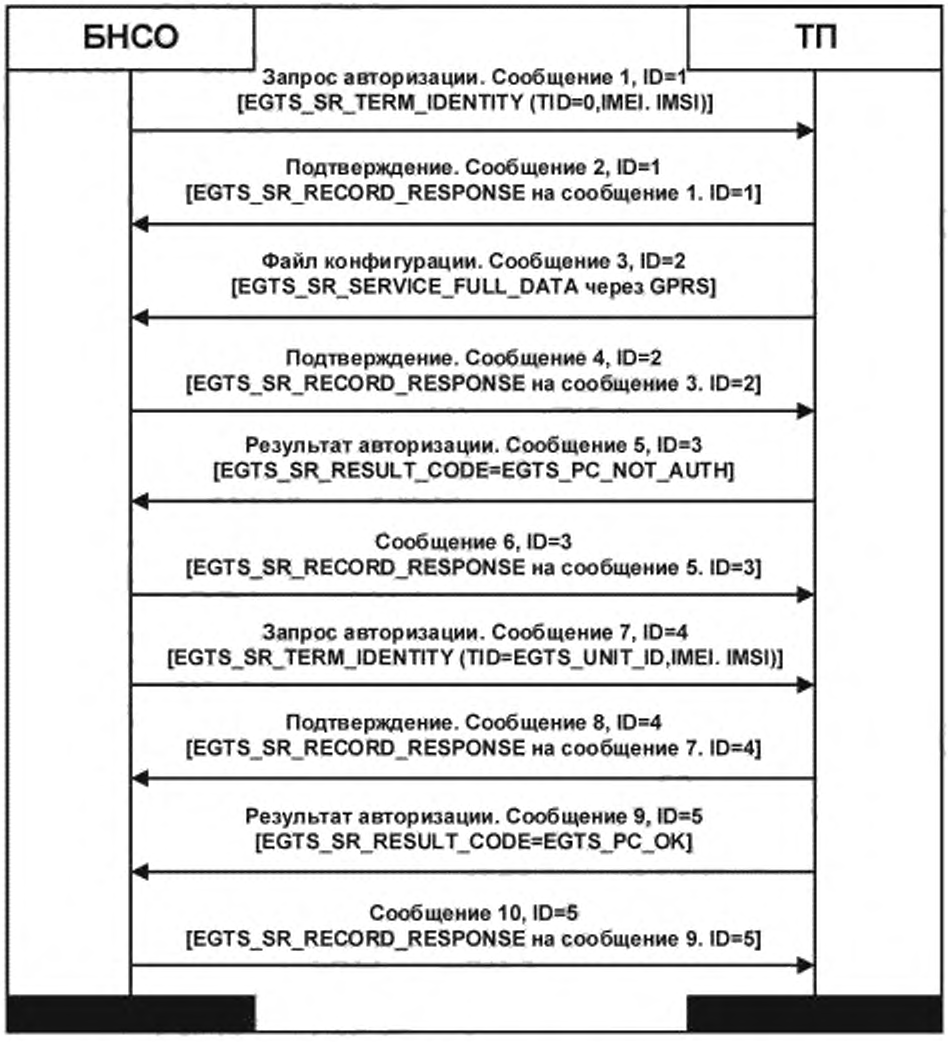


Рисунок Б.3 — Алгоритм обмена сообщениями на этапе авторизации БНСО на ТП

Далее БНСО отправляет сообщение 4 с подтверждением EGTS_SR_RECORD_RESPONSE на сообщение 3 с ID = 2. При использовании расширенного алгоритма авторизации и/или шифрования БНСО передает сообщение 5,

закодированное по правилам шифрования, указанным в сообщении 3 от ТП и содержащим подзапись EGTS_SR_AUTH_INFO с данными для расширенной авторизации.

После получения EGTS_SR_AUTH_INFO ТП отправляет сообщение 6 с подтверждением на сообщение 5 с ID = 3 и выполняет процедуру авторизации. ТП формирует сообщение 7 с результатом проведения авторизации в виде подзаписи EGTS_SR_RESULT_CODE, а также в случае успешной авторизации может добавить информацию о разрешенных для использования данной БНСО услуг в виде подзаписей EGTS_SR_SERVICE_INFO.

БНСО формирует сообщение 8 с подтверждением на сообщение 7 с ID = 4. БНСО может сформировать сообщение 9 и добавить подзаписи EGTS_SR_SERVICE_INFO, содержащие информацию о требуемых услугах (если применяется процедура использования сервисов «по запросу») и/или поддерживаемых сервисах на стороне БНСО.

Далее ТП создает сообщение 10 с подтверждением на сообщение 9 с ID = 5.

На этом этап авторизации заканчивается, и БНСО переходит на этап обмена информационными сообщениями с ТП согласно установленному в БНСО режиму работы.

В том случае, если процедура авторизации проходит неудачно (неверные аутентификационные данные БНСО, запрет доступа данной БНСО к ТП и т. д.), то после отправки сообщения, содержащего подзапись EGTS_SR_ RESULT_CODE с указанием в ней соответствующего кода, ТП должна разорвать установленное терминалом TCP/IP соединение.

Приложение В
(обязательное)

Коды результатов обработки

Коды результатов обработки приведены в таблице В.1.

Таблица В.1 — Коды результатов обработки

Значение	Обозначение	Описание
0	EGTS_PC_OK	Успешно обработано
1	EGTS_PC_IN_PROGRESS	В процессе обработки
128	EGTS_PC_UNS_PROTOCOL	Неподдерживаемый протокол
129	EGTS_PC_DECRYPT_ERROR	Ошибка декодирования
130	EGTS_PC_PROC_DENIED	Обработка запрещена
131	EGTS_PC_INC_HEADERFORM	Неверный формат заголовка
132	EGTS_PC_INC_DATAFORM	Неверный формат данных
133	EGTS_PC_UNS_TYPE	Неподдерживаемый тип
134	EGTS_PC_NOTEN_PARAMS	Неверное число параметров
135	EGTS_PC_DBL_PROC	Попытка повторной обработки
136	EGTS_PC_PROC_SRC_DENIED	Обработка данных от источника запрещена
137	EGTS_PC_HEADERCRC_EROR	Ошибка контрольной суммы заголовка
138	EGTS_PC_DATACRC_ERROR	Ошибка контрольной суммы данных
139	EGTS_PC_INVDATALEN	Некорректная длина данных
140	EGTS_PC_ROUTE_NFOUND	Маршрут не найден
141	EGTS_PC_ROUTE_CLOSED	Маршрут закрыт
142	EGTS_PC_ROUTE_DENIED	Маршрутизация запрещена
143	EGTS_PC_INVADDR	Неверный адрес
144	EGTS_PC_TTLEXPIRED	Превышено количество ретрансляции данных
145	EGTS_PC_NO_ACK	Нет подтверждения
146	EGTS_PC_OBJ_NFOUND	Объект не найден
147	EGTS_PC_EVNT_NFOUND	Событие не найдено
148	EGTS_PC_SRVC_NFOUND	Сервис не найден
149	EGTS_PC_SRVC_DENIED	Сервис запрещен
150	EGTS_PC_SRVC_UNKN	Неизвестный тип сервиса
151	EGTS_PC_AUTH_DENIED	Авторизация запрещена
152	EGTS_PC_ALREADY_EXISTS	Объект уже существует
153	EGTS_PC_ID_NFOUND	Идентификатор не найден
154	EGTS_PC_INC_DATETIME	Неправильная дата и время
155	EGTS_PC_IO_ERROR	Ошибка ввода/вывода

Окончание таблицы В.1

Значение	Обозначение	Описание
156	EGTS_PC_NO_RES_AVAI L	Недостаточно ресурсов
157	EGTS_PC_MODULE_FAULT	Внутренний сбой модуля
158	EGTS_PC_MODULE_PWR_FLT	Сбой в работе цепи питания модуля
159	EGTS_PC_MODULE_PROC_FLT	Сбой в работе микроконтроллера модуля
160	EGTS_PC_MODULE_SW_FLT	Сбой в работе программы модуля
161	EGTS_PC_MODULE_FW_FLT	Сбой в работе внутреннего ПО модуля
162	EGTS_PC_MODULE_IO_FLT	Сбой в работе блока ввода/вывода модуля
163	EGTS_PC_MODULE_MEM_FLT	Сбой в работе внутренней памяти модуля
164	EGTS_PC_TEST_FAILED	Тест не пройден
Примечание — Пакеты сообщений об ошибках (EGTS_PC_DECRYPT_ERROR, EGTS_PC_UNS_PROTOCOL, EGTS_PC_INC_DATAFORM, EGTS_PC_DATACRC_ERROR, EGTS_PC_INC_HEADERFORM, EGTS_PC_HEADERCRC_ERROR) предназначены для целей тестирования оборудования и в рабочей версии программного обеспечения и АС могут быть исключены.		

Приложение Г
(справочное)

Пример реализации алгоритма расчета контрольной суммы CRC16 на языке С/*

```
/*
Name: CRC-16 CCITT
Poly : 0x1021 x^16 + x^12 + x^5 + 1
Init: 0Xffff
Revert: false
XorOut: 0x0000
Check: 0x29B1 ("123456789")
*/
const unsigned short Crc16Table[256]= {
0x0000, 0x1021, 0x2042, 0x3063, 0x4084, 0x50A5, 0x60C6, 0x70E7,
0x8108, 0x9129, 0Xa14A, 0Xb16B, 0Xc18C, 0Xd1AD, 0Xe1CE, 0Xf1EF,
0x1231, 0x0210, 0x3273, 0x2252, 0x52B5, 0x4294, 0x72F7, 0x62D6,
0x9339, 0x8318, 0Xb37B, 0Xa35A, 0Xd3BD, 0Xc39C, 0Xf3FF, 0Xe3DE,
0x2462, 0x3443, 0x0420, 0x1401, 0x64E6, 0x74C7, 0x44A4, 0x5485,
0Xa56A, 0Xb54B, 0x8528, 0x9509, 0Xe5EE, 0Xf5CF, 0Xc5AC, 0Xd58D,
0x3653, 0x2672, 0x1611, 0x0630, 0x76D7, 0x66F6, 0x5695, 0x46B4,
0Xb75B, 0Xa77A, 0x9719, 0x8738, 0Xf7DF, 0Xe7FE, 0Xd79D, 0Xc7BC,
0x48C4, 0x58E5, 0x6886, 0x78A7, 0x0840, 0x1861, 0x2802, 0x3823,
0Xc9CC, 0Xd9ED, 0Xe98E, 0Xf9AF, 0x8948, 0x9969, 0Xa90A, 0Xb92B,
0x5AF5, 0x4AD4, 0x7AB7, 0x6A96, 0x1A71, 0x0A50, 0x3A33, 0x2A12,
0Xdbfd, 0Xcbdc, 0Xfbbf, 0Xeb9E, 0x9B79, 0x8B58, 0Xbb3B, 0Xab1A,
0x6CA6, 0x7C87, 0x4CE4, 0x5CC5, 0x2C22, 0x3C03, 0x0C60, 0x1C41,
0Xedae, 0Xfd8F, 0Xcdec, 0Xddcd, 0Xad2A, 0Xbd0B, 0x8D68, 0x9D49,
0x7E97, 0x6EB6, 0x5ED5, 0x4EF4, 0x3E13, 0x2E32, 0x1E51, 0x0E70,
0Xff9F, 0Xefbe, 0Xdfdd, 0Xcffc, 0Xbf1B, 0Xaf3A, 0x9F59, 0x8F78,
0x9188, 0x81A9, OXb1CA, 0Xa1EB, 0Xd10C, 0Xc12D, 0Xf14E, 0Xe16F,
0x1080, 0x00A1, 0x30C2, 0x20E3, 0x5004, 0x4025, 0x7046, 0x6067,
0x83B9, 0x9398, 0Xa3FB, 0Xb3DA, 0Xc33D, 0Xd31C, 0Xe37F, 0Xf35E,
0x02B1, 0x1290, 0x22F3, 0x32D2, 0x4235, 0x5214, 0x6277, 0x7256,
0Xb5EA, 0Xa5CB, 0x95A8, 0x8589, 0Xf56E, 0Xe54F, 0Xd52C, 0Xc50D,
0x34E2, 0x24C3, 0x14A0, 0x0481, 0x7466, 0x6447, 0x5424, 0x4405,
0Xa7DB, 0Xb7FA, 0x8799, 0x97B8, 0Xe75F, 0Xf77E, 0Xc71D, 0Xd73C,
0x26D3, 0x36F2, 0x0691, 0x16B0, 0x6657, 0x7676, 0x4615, 0x5634,
0Xd94C, 0Xc96D, 0Xf90E, 0Xe92F, 0x99C8, 0x89E9, 0Xb98A, 0Xa9AB,
0x5844, 0x4865, 0x7806, 0x6827, 0x18C0, 0x08E1, 0x3882, 0x28A3,
0Xcb7D, 0Xdb5C, 0Xeb3F, 0Xfb1E, 0x8BF9, 0x9BD8, 0Xabbb, 0Xbb9A,
0x4A75, 0x5A54, 0x6A37, 0x7A16, 0x0AF1, 0x1AD0, 0x2AB3, 0x3A92,
0Xfd2E, 0Xed0F, 0Xdd6C, 0Xcd4D, 0Xbdaa, 0Xad8B, 0x9DE8, 0x8DC9,
0x7C26, 0x6C07, 0x5C64, 0x4C45, 0x3CA2, 0x2C83, 0x1CE0, 0x0CC1,
0XeflF, 0Xff3E, 0Xcf5D, 0Xdf7C, 0Xaf9B, 0Xbfba, 0x8FD9, 0x9FF8,
0x6E17, 0x7E36, 0x4E55, 0x5E74, 0x2E93, 0x3EB2, 0x0ED1, 0x1EF0
};
unsigned short Crc16(unsigned char * pcBlock, unsigned short len)
{
unsigned short crc = 0Xffff;
while (len- -)
crc = (crc<<8) ^ Crc16Table[(crc>> 8) ^ *pcBlock++];
returncrc;
}
```

Приложение Д
(справочное)

Пример реализации алгоритма расчета контрольной суммы CRC8 на языке С/*

```
/*
Name : CRC-8
Poly : 0x31 x^8 + x^5 + x^4 + 1
Init: 0xFF
Revert: false
XorOut: 0x00
Check: 0xF7 ("123456789")
*/
const unsigned char CRC8Table[256] = {
0x00, 0x31, 0x62, 0x53, 0xC4, 0xF5, 0xA6, 0x97,
0xB9, 0x88, 0xDB, 0xEA, 0x7D, 0x4C, 0x1F, 0x2E,
0x43, 0x72, 0x21, 0x10, 0x87, 0xB6, 0xE5, 0xD4,
0xFA, 0xCB, 0x98, 0xA9, 0x3E, 0x0F, 0x5C, 0x6D,
0x86, 0xB7, 0xE4, 0xD5, 0x42, 0x73, 0x20, 0x11,
0x3F, 0x0E, 0x5D, 0x6C, 0xFB, 0xCA, 0x99, 0xA8,
0xC5, 0xF4, 0xA7, 0x96, 0x01, 0x30, 0x63, 0x52,
0x7C, 0x4D, 0x1E, 0x2F, 0xB8, 0x89, 0xDA, 0xEB,
0x3D, 0x0C, 0x5F, 0x6E, 0xF9, 0xC8, 0x9B, 0xAA,
0x84, 0xB5, 0xE6, 0xD7, 0x40, 0x71, 0x22, 0x13,
0x7E, 0x4F, 0x1C, 0x2D, 0xBA, 0x8B, 0xD8, 0xE9,
0xC7, 0xF6, 0xA5, 0x94, 0x03, 0x32, 0x61, 0x50,
0xBB, 0x8A, 0xD9, 0xE8, 0x7F, 0x4E, 0x1 D, 0x2C,
0x02, 0x33, 0x60, 0x51, 0xC6, 0xF7, 0xA4, 0x95,
0xF8, 0xC9, 0x9A, 0xAB, 0x3C, 0x0D, 0x5E, 0x6F,
0x41, 0x70, 0x23, 0x12, 0x85, 0xB4, 0xE7, 0xD6,
0x7A, 0x4B, 0x18, 0x29, 0xBE, 0x8F, 0xDC, 0xED,
0xC3, 0xF2, 0xA1, 0x90, 0x07, 0x36, 0x65, 0x54,
0x39, 0x08, 0x5B, 0x6A, 0xFD, 0xCC, 0x9F, 0xAE,
0x80, 0xB1, 0xE2, 0xD3, 0x44, 0x75, 0x26, 0x17,
0xFC, 0xCD, 0x9E, 0xAF, 0x38, 0x09, 0x5A, 0x6B,
0x45, 0x74, 0x27, 0x16, 0x81, 0xB0, 0xE3, 0xD2,
0xBF, 0x8E, 0xDD, 0xEC, 0x7B, 0x4A, 0x19, 0x28,
0x06, 0x37, 0x64, 0x55, 0xC2, 0xF3, 0xA0, 0x91,
0x47, 0x76, 0x25, 0x14, 0x83, 0xB2, 0xE1, 0xD0,
0xFE, 0xCF, 0x9C, 0xAD, 0x3A, 0x0B, 0x58, 0x69,
0x04, 0x35, 0x66, 0x57, 0xC0, 0xF1, 0xA2, 0x93,
0xBD, 0x8C, 0xDF, 0xEE, 0x79, 0x48, 0x1B, 0x2A,
0xC1, 0xF0, 0xA3, 0x92, 0x05, 0x34, 0x67, 0x56,
0x78, 0x49, 0x1A, 0x2B, 0xBC, 0x8D, 0xDE, 0xEF,
0x82, 0xB3, 0xE0, 0xD1, 0x46, 0x77, 0x24, 0x15,
0x3B, 0x0A, 0x59, 0x68, 0xFF, 0xCE, 0x9D, 0xAC};
unsigned char CRC8(unsigned char *lpBlock, unsigned char len)
{
unsigned char crc = 0xFF;
while (len--)
crc = CRC8Table[crc ^ *lpBlock++];
returncrc;
}
```

Приложение Е
(рекомендуемое)

Описание спецификации протокола обмена данными тахографа с АИС «ТК»

Е.1 Описание взаимодействия с ТП

Е.1.1 Схема обмена сообщениями

	Тахограф		Сервер
1	Выдача данных маршрута MESSAGE(n,track_Data_n)	⇨	
		⇦	Передача квитанции MESSAGE(m, ack_ track_Data_n _m)
2	Выдача данных маршрута MESSAGE(n+1, track_Data_n+1)	⇨	
		⇦	Передача квитанции MESSAGE(m+1, ack_ track_Data_n+1 _m+1)
3	Выдача данных маршрута MESSAGE(n+2, track_Data_n+2)	⇨	
		⇦	Запрос данных по инициативе сервера MESSAGE(m+2, запрос _Data_m+2)
4	Выдача запрашиваемых данных MESSAGE(n+3, Data_n+3)	⇨	
		⇦	Передача подтверждения MESSAGE(m+3, confirm _Data_ n+3 _m+3)
5	Выдача запрашиваемых данных MESSAGE(n+4, Data_n+4)	⇨	
		⇦	Передача подтверждения MESSAGE(m+4, confirm _Data_ n+4 _m+4)
6	Все запрашиваемые данные выданы MESSAGE(n+5)	⇨	
		⇦	а) Передача квитанции на ранее полученные данные маршрута MESSAGE(m+5, ack_ track_Data_n+2 _m+5) б) Или передача подтверждения MESSAGE(m+5, n+5 _m+5)
7	Выдача данных маршрута, на которые не получена квитанция MESSAGE(n+6, track_Data_n+6)	⇨	
		⇦	Передача квитанции MESSAGE(m+6, ack_ track_Data_n+6 _m+6)

Е.1.1.1 Схема повторной выдачи данных тахографом в новом сообщении, если ответное сообщение не принято

	Тахограф		Сервер
1	Выдача данных маршрута MESSAGE(n, track_Data_n)	⇨	
	Сообщение сервера не принято (любая ошибка, возникшая при обработке сообщения)	⇦	Передача квитанции MESSAGE(m, ack_ track_Data_n _m)

Окончание таблицы

	Тахограф		Сервер
2	Повторная выдача данных в новом сообщении MESSAGE(n+1,track_Data_n)	⇨	
		⇦	MESSAGE(m+1,ack_ track_Data_n _m)
3	Сообщение сервера не принято. Разрыв соединения		

Е.1.1.2 Схема запроса сервера на повторную выдачу, если ответное сообщение не принято

	Тахограф		Сервер
1	Выдача данных маршрута MESSAGE(n, track_Data_n)	⇨	
		⇦	Передача квитанции MESSAGE(m, ack_ track_Data_n _m)
2	Выдача данных маршрута MESSAGE(n+1, track_Data_n+1)	⇨	Сообщение не принято
		⇦	Передача запроса на повторную выдачу MESSAGE(m+1, запрос на повторную выдачу)
3	Повторная выдача данных в новом сообщении MESSAGE(n+2, t rack_Data_n+1)	⇨	
		⇦	a) Передача квитанции MESSAGE(m+2, ack_ track_Data_n+1 _m+2)
			b) Сообщение не принято. Разрыв соединения

Е.2 Формат сообщений

Все сообщения представляют собой заголовок фиксированной длины и тело в формате BER TLV-структуры, тэгом которых является код типа пакета.

Е.2.1 Формат заголовка

Заголовок сообщения имеет фиксированную длину равную 25 байт.

Позиция (hex)	Длина	Значение/Описание
0x00	4	Фиксированная константа равная значению '41544C53' — Magic
0x04	1	Версия транспортного протокола
0x05	16	Регистрационный номер СКЗИ тахографа (RefNumber)
0x15	2	Длина тела сообщения с порядком байт BE
0x17	2	CRC16 тела сообщения, CCIT

Е.3 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
0x32	RESTORESESSION	Выдается тахографом, если у него есть сессионные ключи
0x33	DENYSESSION	Выдается сервером в случае отказа восстановления сессии

Окончание таблицы

Тэг	Название	Примечание
0x34	CACERTREQUEST	Выдается тахографом, если у него нет сертификата УЦ
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
0x38	REAUTH	Выдается тахографом в случае, если он считает, что необходима повторная динамическая аутентификация
0x39	MESSAGE	Зашифрованные сообщения, защищенные имитовставкой

Е.4 Формат тела сообщений

Е.4.1 CONNECTREQUEST

Тэг 0x30. Это сообщение выдается тахографом сразу после установления соединения. Состоит из последовательности таких TLV-структур:

Тэг	Наименование	Длина, байт	Количество	Примечание
0x02	Server Address		0/1	Адрес (DNS-имя) сервера
0x03	Part Number	16	1	Заводской номер СКЗИ тахографа
0x04	KeyId	16	1	Идентификатор открытого ключа СКЗИ тахографа ($IDPk_{KC}$)
0x05	Random	8	1	Случайное число СКЗИ тахографа (RND_{KC})
0x06	T	4	1	Криптограмма

Е.4.1.1 SERVERHELLO

Тэг 0x31. Это сообщение выдается сервером сразу после получения запроса на установление соединения или в ходе установленной сессии с целью проведения повторной динамической аутентификации.

Состоит из последовательности таких TLV-структур:

Тэг	Наименование	Длина, байт	Количество	Примечание
0x01	Сертификат		1	Сертификат сервера (C_S)
0x05	Random	16	1	Случайное число сервера (RND_S)

Е.4.1.2 RESTORESESSION

Тэг 0x32. Это сообщение выдается тахографом, если у него есть сессионные ключи.

Состоит из последовательности таких TLV-структур:

Тэг	Наименование	Длина, байт	Количество	Примечание
0x02	ServerAddress		0/1	Адрес (DNS-имя) сервера
0x03	Part Number	16	1	Заводской номер СКЗИ тахографа
0x04	KeyId	16	1	Идентификатор открытого ключа СКЗИ тахографа ($IDPk_{KC}$)
0x06	T	4	1	Криптограмма

Е.4.1.3 DENYSESSION

Тэг 0x33. Это сообщение выдается сервером в случае разрыва соединения. Пакет не содержит данных, состоит из кода команды и поля нулевой длины.

E.4.1.4 CACERTREQUEST

Тэг 0x34. Это сообщение выдается тахографом, если у него нет открытого ключа УЦ для проверки сертификата сервера.

Сообщение содержит тэги с идентификаторами ключей УЦ известных СКЗИ тахографа.

Тэг	Наименование	Длина, байт	Количество	Примечание
0x04	KeyId	16	1—2	Идентификатор ключа УЦ (Идентификаторы известных НКМ ключей УЦ)

E.4.1.5 CACERTCHAIN

Тэг 0x35. Это сообщение выдается сервером в ответ на сообщение тахографа CACERTREQUEST. Сообщение содержит тэги с сертификатами УЦ, составляющими цепочку сертификатов, которые необходимо передать в СКЗИ тахографа в том порядке, в каком они присланы сервером.

Тэг	Наименование	Длина, байт	Количество	Примечание
0x01	Сертификат УЦ	16	1 и более	Передаются в том порядке, в котором должны быть переданы в СКЗИ тахографа на проверку

E.4.1.6 INITSESSION

Тэг 0x36. Это сообщение выдается тахографом для динамической аутентификации.

Состоит из последовательности таких TLV-структур:

Тэг	Наименование	Длина, байт	Количество	Примечание
0x05	Random	16	1	Случайное число СКЗИ тахографа (RND_{KC})
0x06	S	80	1	Криптограмма

E.4.1.7 CONFIRMSESSION

Тэг 0x37.Это сообщение выдается сервером в ответ на сообщение тахографа INITSESSION для динамической аутентификации.

Тэг	Наименование	Длина, байт	Количество	Примечание
0x06	H	6	1	Проверочная криптограмма сервера

E.4.1.8 MESSAGE

Тэг 0x39. Это сообщение выдается сервером и тахографом. Содержимым данного пакета являются открытые или зашифрованные данные.

Состоит из последовательности таких TLV-структур:

Тэг	Наименование	Длина, байт	Количество	Примечание
0x20	Payload	до 978	0 — если есть 0xA0 1 — если нет	Открытые содержательные данные. Если в пакете нет содержательных данных, должно присутствовать это поле нулевой длины
0xA0	Payload_enc	до 978	0 — если есть 0x20 1 — если нет	Зашифрованные содержательные данные. Если в пакете нет содержательных данных, должно присутствовать это поле нулевой длины
0x10	SerialNo	4	0—1	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	1	Номер последнего сообщения, полученного отправителем данного

Окончание таблицы

Тэг	Наименование	Длина, байт	Количество	Примечание
0x12	RetransmitReq	0	0—1	Запрос повторной передачи предыдущего пакета
0x1A	Concatenation	1	0—1	0 — начало блока, 1 — продолжение, 2 — конец
0x1B	FragmentNo	1—4	0—1	Порядковый номер фрагмента конкатенированного сообщения
0x1C	Priority	1	0—1	Уровень приоритета сообщения
0x1F	ServerInitated	0	0—1	Добавляется сервером, если сообщение отправлено по его инициативе, а не в качестве подтверждения сообщения от тахографа
0x1E	MAC	6	1	Имитовставка

Е.4.2 Формирование сообщения MESSAGE

Сообщение типа MESSAGE формируется в такой последовательности:

1) Формируется пакет данных сообщения.

2) Формируется тело сообщения, к полученному пакету данных дописывается тэг ('39') и длина.

3) Формируется сообщение, к телу сообщения добавляется заголовок и в таком виде сообщение передается на сервер/тахограф.

Е.4.3 Формирование пакета данных сообщения MESSAGE

Е.4.3.1 Формирование пакета данных сообщения MESSAGE тахографом

1) Если данные для выгрузки присутствуют, тахограф формирует пакет с содержательными данными (открытыми — тэг 0x20 или зашифрованными — тэг 0xA0).

Пакет с содержательными данными:

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload	до 1016	Содержательные данные, подготовленные СКЗИ тахографа
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения, полученного отправителем данного или '00 00 00 00' для первого сообщения
0x1C	Priority	1	Уровень приоритета сообщения
0x1E	MAC	6	Имитовставка

2) Если выдаются данные по запросу сервера, тахограф формирует пакет с данными тахографа (открытыми — тэг 0x20 или зашифрованными — тэг 0xA0).

Пакет с содержательными данными (не последний фрагмент):

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload	до 1032/ до 1024	Фрагмент содержательных данных, подготовленных тахографом по запросу сервера
0x0A	Data	до 922/ до 914	Данные
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации). Сохраняется при обрыве сессии и при повторной динамической аутентификации

Окончание таблицы

Тэг	Наименование	Длина, байт	Примечание
0x11	Confirmed	4	Номер последнего сообщения, полученного отправителем данного
0x1A	Concatenation	1	0 — начало блока, 1 — продолжение
0x1B	FragmentNo	1—4	Порядковый номер фрагмента конкатенированного сообщения
0x1C	Priority	1	Уровень приоритета сообщения
0x1F	ServerInitated	0	Сообщение отправлено по инициативе сервера
0x1E	MAC	6	Имитовставка

Пакет с содержательными данными (последний фрагмент):

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload	до 1032/ до 1024	Последний фрагмент содержательных данных, подготовленных тахографом по запросу сервера
0x0A	Data	до 922/до 914	Данные
0x0B	Signed Attrs	46	Атрибуты подписи
0x0C	Signature	64	Подпись
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения, полученного отправителем данного
0x1A	Concatenation	1	2 — конец
0x1B	FragmentNo	1—4	Порядковый номер фрагмента конкатенированного сообщения
0x1C	Priority	1	Уровень приоритета сообщения
0x1F	ServerInitated	0	Сообщение отправлено по инициативе сервера
0x1E	MAC	6	Имитовставка

Пакет с содержательными данными (единственный):

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload	до 1032/до 1024	Содержательные данные, подготовленные тахографом по запросу сервера
0x0A	Data	до 922/до 914	Данные
0x0B	Signed Attrs	46	Атрибуты подписи
0x0C	Signature	64	Подпись
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения, полученного отправителем данного
0x1C	Priority	1	Уровень приоритета сообщения
0x1F	ServerInitated	0	Сообщение отправлено по инициативе сервера
0x1E	MAC	6	Имитовставка

Е.4.3.2 Формирование пакета данных сообщения MESSAGE сервером

С квитанцией (тэги 0x12 и 0x1F — отсутствуют, тэг 0x20 или 0xA0 — присутствует):

Тэг	Наименование	Длина байт	Примечание
0x20/0xA0	Payload	до 1016	Квитанция
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения, полученного от тахографа
0x1C	Priority	1	Уровень приоритета сообщения
0x1E	MAC	6	Имитовставка

С запросом повторной выдачи (тэги 0x12 — присутствуют, тэг 0x20 или 0xA0 — отсутствует):

Тэг	Наименование	Длина, байт	Примечание
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения, полученного от тахографа
0x12	RetransmitReq	0	Запрос повторной выдачи
0x1C	Priority	1	Уровень приоритета сообщения
0x1E	MAC	6	Имитовставка

С запросом данных по инициативе сервера (тэг 0x1F — присутствуют, тэг 0x20 или 0xA0 — присутствует):

Тэг	Наименование	Длина, байт	Примечание
0x20/0xA0	Payload	до 1016	Запрос
0x10	SerialNo	4	Порядковый номер сообщения (в порядке его генерации)
0x11	Confirmed	4	Номер последнего сообщения, полученного от тахографа
0x1C	Priority	1	Уровень приоритета сообщения
0x1F	ServerInitated	0	Сообщение отправлено по инициативе сервера, а не в качестве подтверждения сообщения от тахографа
0x1E	MAC	6	Имитовставка

Е.4.4 Формат содержательных данных (MESSAGE)

Е.4.4.1 Длина данных

Длина всего сообщения с учетом имитовставки не может превышать 1100 байт. Количество содержательных данных в пакете может составлять до 1032 байт в зависимости от присутствующих в сообщении полей служебных TLV-структур (Confirmed, MAC).

Е.4.4.2 Формат содержательных данных, подготовленных СКЗИ тахографа

Структура 0x20/0xA0:

Тэг	Наименование	Длина байт	Количество	Примечание
0x20/0xA0	Payload	до 1032/ до 1024	1	Содержательные данные (открытые или зашифрованные). Если в пакете нет содержательных данных, должно присутствовать это поле нулевой длины
	Запись 1	≤252	1	

Окончание таблицы

Тэг	Наименование	Длина, байт	Количество	Примечание
	Запись 2	≤252	0—1	
	Запись 3	≤252	0—1	
	.....			
	Запись n	≤252	0—1	До восьми записей в зависимости от протокола

Формат записи (события 'B5', 'B6', 'B7'):

Элемент	Определение	Длина, байт
N	Номер записи в архиве (CPC)	4
Part number	Заводской номер СКЗИ тахографа	16
DATE	Текущее (реальное) время ГГ.ММ.ДД.чч.мм.сс	6
TRE	'B5'/ 'B6'/ 'B7' — Код события	1
L	Длина данных	1
Данные	Регистрируемые данные	≤160
ЭЦП	Подпись	64

Е.4.4.3 Формат содержательных данных, подготовленных тахографом по запросу ТП
Структура 0x20/0xA0:

Тэг	Наименование	Длина, байт	Количество	Примечание
0x20/0xA0	Payload	до 1032/ до 1024	1	Содержательные данные (открытые или зашифрованные)
0x0A	Data	до 922/ до 914	0—1	Данные
0x0B	SignedAttrs	46	0—1	Атрибуты подписи
0x0C	Signature	64	0—1	Подпись

Структура поля Signedattrs:

Тэг	Наименование	Длина, байт	Количество	Примечание
0x01	метка времени	6	1	BCD
0x02	широта	4	1	fixed point
0x03	долгота	4	1	fixed point
0x04	part number	16	1	Заводской номер

Е.4.4.4 Формат содержательных данных, подготовленных ТП

Тэг	Наименование	Длина, байт	Количество	Примечание
0x20/0xA0	Payload	до 1032/ до 1024	1	Содержательные данные. Если в пакете нет содержательных данных, должно присутствовать это поле нулевой длины
	Квитанция 1	≤252	1	
	Квитанция 2	≤252	0—1	
	Квитанция 3	≤252	0—1	

Окончание таблицы

Тэг	Наименование	Длина, байт	Количество	Примечание
	.....			
	Квитанция n	≤252	0—1	До 8 записей в зависимости от протокола

Формат квитанции:

Элемент	Определение	Длина, байт	Примечание
N	Номер записи в архиве (CPC)	4	Получены от тахографа
Partnumber	Заводской номер СКЗИ тахографа	16	–//–
DATE	Текущее (реальное) время ГГ.ММ.ДД чч.мм.сс	6	–//–
TRE	'B5'/ 'B6' / 'B7' — Код события	1	–//–
L	Длина данных полученного события	1	–//–
Флаги	Флаги ТП	1	RFU

Е.4.4.5 Форматы отчетов

Е.4.4.5.1 Отчет о вводе карты

Событие регистрируется каждый раз при вводе карты.

Идентификатор выгрузки данного события используется в остальных событиях для привязки к конкретному сеансу управления автомобилем и карте тахографа.

Регистрируемое событие B1:

Размер	Идентификатор	Формат	Обязательность	Описание
1	flags	Байт	Обязательно	Флаги (описание см. ниже)
4	tachoInsertionTime	Метка времени в LE	Обязательно	Дата, время ввода карты по данным тахографа
4	cardAuthTime	Метка времени в LE	Обязательно	Дата, время аутентификации карты по часам СКЗИ тахографа
12	CardAuthCoordsAndTime	Структура, координаты с меткой времени, см. описание	Опционально	Последние известные координаты и время на момент регистрации события
18	FullCardNumber	Байтовый массив	Обязательно	Полный номер карты, с которой проводится аутентификация
16	NCMRand	Байтовый массив	Обязательно	Случайное число, использованное в аутентификации с картой
64	CardSignature	Байтовый массив	Обязательно	Подпись, выработанная картой в процессе аутентификации

Итого: 119 байт данных

Кодировка байта флагов:

8	7	6	5	4	3	2	1	Идентификатор	Описание
	1							TimeError	Флаг устанавливается, если на момент открытия отчета был установлен флаг «InternalTimeError» и далее не было подстройки времени
			1					TimeCorrection	Флаг устанавливается в случае, если на момент аутентификации было некорректное время, а на момент сохранения события была проведена подстройка времени по данным ГНСС и время было изменено
						1		InvalidFlag	Событие не содержит содержательных данных. Используется только для объединения сеанса
							1	Slot	Флаг соответствует номеру слота. (0 — водитель, 1 — соводитель)

Е.4.4.5.2 Отчет о режимах труда и отдыха водителя

Событие регистрируется при изъятии карты водителя при наличии данных о труде/отдыхе.

Е.4.4.5.2.1 Формат сохраняемых событий

Размер	Поле	Формат	Обязательность	Описание	Время заполнения
1	flags	Байт	Обязательно	Флаги (см. ниже)	Сохранение отчета
1	Number	Байт	Обязательно	Номер события в рамках одного сеанса	Обновляется при регистрации события
18	FullCardNumber	Байтовый массив	Обязательно	Заполняется при создании отчета. Полный номер последней введенной карты в слот тахографа (карта может быть не введена на протяжении отчета)	Создание отчета
4	CardInsertionID	Байт	Опционально	Ссылка на идентификатор записи ввода карты (индекс выгрузки вставленной карты)	
4	tachoInsertionTime	Метка времени	Обязательно	Время последнего ввода карты	Создание отчета
4	ReportBeginTime	Метка времени	Обязательно	Время начала отчета (метка времени, соответствующая началу первой минуты, включенной в отчет. Значение секунд обнулено)	Создание отчета

Окончание таблицы

Размер	Поле	Формат	Обязательность	Описание	Время заполнения
12	BeginCoordsWithTime	Структура, координаты с меткой времени	Опционально	Первые валидные полученные координаты от GNSS с меткой времени. Первые валидные полученные координаты от GNSS с меткой времени. Если за все время отчета не получено навигационных данных, поле заполняется значением '00'	Получение первых валидных координат
4	ReportEndTime	Метка времени	Обязательно	Время окончания отчета (Метка времени, соответствующая окончанию последней минуты, включенной в отчет)	Сохранение отчета
12	EndCoordsWithTime	Структура, координаты с меткой времени	Опционально	Последние валидные полученные координаты от GNSS с меткой времени. Если координат не было — поле обнулено	Получение очередных валидных координат
1	PeriodCount	Байт	Обязательно	Количество периодов активности водителя в данном отчете (1...20)	Сохранение отчета
5 *PeriodCount	PeriodActivityInfo	Структура	Обязательно	Список описателей смен режимов труда и отдыха	Каждую минуту

Кодировка байта флагов:

8	7	6	5	4	3	2	1	Идентификатор	Описание
1								TimeWarning	Устанавливается, если в отчете присутствует промежуток с установленным флагом «TimeWarning»
	1							TimeError	Флаг устанавливается, если на момент открытия отчета был установлен флаг «InternalTimeError» и далее не было подстройки времени
		1						PowerFailure	Флаг устанавливается в случае, если за период отчета был хотя бы один сброс питания
			1					TimeCorrection	Флаг устанавливается в случае, если на момент аутентификации был установлен флаг «InternalTimeError», а на момент сохранения события была проведена подстройка времени
				1				ErrorClose	Флаг установлен, если закрытие отчета было вызвано рассинхронизацией данных
					1			CardInserted	Флаг установлен, если отчет описывает промежуток времени, в течение которого карта была введена в слот
						X		RFU	Зарезервировано (Не анализировать)

Окончание таблицы

8	7	6	5	4	3	2	1	Идентификатор	Описание
							1	Slot	Флаг соответствует номеру слота (0 — водитель, 1 — соводитель)

E.4.4.5.2.2 Структура PeriodActivityInfo

Размер	Поле	Формат	Описание
2	Duration	Целое в LE	Длительность периода в календарных минутах
2	PeriodActivity	Целое в LE	Суммарный период зафиксированного движения ТС в минутах за данный период активности в календарных минутах
1	ActivityStatus	Байт	Описание поля см. ниже

Кодировка поля «ActivityStatus»:

8	7	6	5	4	3	2	1	Описание	Время установки
0	0	x	-	-	0	-	-	В течение периода был сброс питания	Начальный пуск
0	0	-	x	-	0	-	-	Расхождение времени между тахографом и СКЗИ тахографа в течение 5 с более чем на 5 с в двух последовательных календарных минутах	При обработке календарной минуты
0	0	-	-	x	0	-	-	Особое состояние (неприменимо/ паром/ переезд) на момент начала первой календарной минуты периода	При обработке календарной минуты
0	0	-	-	-	0	-	-	RFU	
X	X	-	-	-	0	x	x	Тип периода '00': отдых, '01': работа, '10': отсутствие питания более четырех минут, '11': ручной ввод (период не учитывается)	При обработке календарной минуты

E.4.4.5.3 Данные о смене деятельности

События являются частью отчета о труде/отдыхе и накапливаются независимо для каждого из слотов.

Событие начинает накапливаться при начале нового отчета либо при переполнении и сохранении предыдущего события того же типа в отчете.

Регистрация элемента происходит при обработке выдвигаемой из внутреннего буфера минуты.

Новая запись регистрируется, если в следующей минуте от предыдущей отличается хотя бы одно из полей:

1 activity

2 Особое состояние

3 Статус управления

События группируются по 8 в событие с идентификатором B2.

Событие:

Размер	Поле	Тип	Описание
1	Флаги	Байт	
1	report_ref	Байт	Ссылка на отчет
4	CardInsertionID	Номер события	
4	reportBeginTime	Метка времени	Время начала отчета
1	events_count	Байт	Количество записей

Окончание таблицы

Размер			Поле					Тип	Описание
13*11			Записи					Структура, см. описание	events[13]
8	7	6	5	4	3	2	1	Описание	
1								TimeWarning	
	1							TimeError	Флаг устанавливается, если на момент открытия отчета был установлен флаг «InternalTimeError» и далее не было подстройки времени
		1						PowerFailure	
			1					TimeCorrection	Флаг устанавливается в случае, если на момент аутентификации был установлен флаг «InternalTimeError», а на момент сохранения события была проведена подстройка времени
				1				ErrorClose	
					1			CardInserted	Наличие карты в слоте
						X		RFU	Зарезервировано (Не анализировать)
							1	Slot	Водитель/соводитель

Каждая запись:

Размер	Поле	Тип	Описание
1	ActivityStatusInfo	Байт	Вид деятельности (5 бит ActivityChangeInfo)
2	TimeChange	Метка времени	Относительное время смены вида деятельности в минутах
8	ShortCoords	Структура, координаты без метки времени, см. описание	Первые валидные координаты, полученные в календарную минуту, начало которой указано в поле TimeChange

Размер записи: 13(8 в 155).

Кодировка вида деятельности:

8	7	6	5	4	3	2	1	Описание
0	-	-	-	-	-	-	-	RFU
0	x	-	-	-	-	-	-	Расхождение времени между тахографом и СКЗИ тахографа в течении 5 с более чем на 5 с
0	-	x	-	-	-	-	-	Статус управления (на момент окончания минуты)
0	-	-	x	x	-	-	-	Особые ситуации (неприменимо или паром/переезд) (на момент окончания минуты)
0	-	-	-	-	x	x	x	Вид деятельности '000': (перерыв/отдых), '001': (готовность), '010': (работа), '011': (управление), '100': RFU, '101': (ручной ввод), '110': (ручной ввод), '111': (отсутствие питания)

Е.4.4.5.4 Данные ручного ввода

Событие регистрируется с идентификатором В7.

Событие:

Размер	Поле	Тип	Описание
1	RFU	Байт	Зарезервировано (не анализировать)
18	FullCardNumber	Байтовый массив	Обязательно
1	record_n	Байт	Количество записей с данными ручного ввода о периоде деятельности водителя (до 15)
15*9	Записи	Структура, см. описание	act[15]

Каждая запись:

Размер	Поле	Тип	Описание
4	PeriodActivityTimeStart	Метка времени в LE	Начало деятельности. Кодировка в соответствии с типом TimeReal
1	Driver_state	Байт	Вид деятельности водителя
4	PeriodActivityTimeEnd	Метка времени в LE	Окончание деятельности

Е.4.4.5.5 Данные от тахографа

Событие регистрируется с идентификатором В8.

Событие:

Размер	Поле	Тип	Описание
1	count	Байт	Количество событий
6*7	records	Структура, см. описание	act[6]

Каждая запись:

Размер	Поле	Тип	Описание
18	FullCardNumber	Байтовый массив	Полный номер карты, с которой проводится аутентификация
2	tacho_change	Битовая маска LE	Вид деятельности водителя
4	timeChange	Метка времени в LE	Время изменения вида деятельности

Е.4.4.5.6 Отчет о телеметрии

Событие содержит набор записей.

Каждая запись в наборе содержит статистическую информацию о состоянии ТС за период между подачей и снятием питания. Событие формируется по мере накопления максимального количества записей. Каждая запись формируется 1 раз в 4 мин. Всего накапливается 25(11) записей. Результирующее событие формируется 1 раз в 100 мин (1 ч 40 мин).

Регистрируемое событие В6(В9):

Размер	Описание	
1	Количество записей	events_count
23*6	Записи	events[6]

Каждая запись:

Размер	Описание	
2	Текущее состояние	Маска ошибок
4	Время начала регистрации	Включение питания либо 1 ч после включения

Окончание таблицы

Размер	Описание	
2	Общее количество секунд	Количество секунд, зафиксированных в этом событии
2	Количество секунд движения	
2	Количество секунд движения без ГНСС	
2	Количество секунд движения, зарегистрированных только по акселерометру	

Итого: 14.

Е.4.4.5.7 Маршрут движения транспортного средства

Внутри события перемешаны записи разных типов. Размер каждой записи получается из идентификатора.

Регистрируемое событие B5:

Размер	Описание	
1	Количество записей	eventTrack_count
X	Записи по 16 байт каждая	eventTracks

Маршрутная точка:

Размер	Тип	Описание	
1	Байт	Скорость	км/ч
2	Целое в LE	Высота	м
8	Структура	Координаты	
4	Метка времени в LE	Дата	TimeReal
1	Знаковое целое. Цена единицы — 2 градуса	Азимут	младший бит 2 градуса

Размер записи: 16.

Е.4.4.5.8 Превышение скорости:

Событие регистрируется при обнаружении превышения скорости внутренними средствами.

Регистрируемое событие B4:

Новая посылка: 102 байта

Размер	Тип данных	Описание
4	Номер записи в BE	Ссылка на идентификатор записи ввода карты водителя
4	Номер записи в BE	Ссылка на идентификатор записи ввода карты второго водителя
16	Байтовый массив	Заводской номер СКЗИ тахографа
15	Байтовый массив	Госномер ТС
4	Метка времени в LE	Срок окончания поверки СКЗИ тахографа
4	Метка времени в LE	Время начала превышения
1	Байт	Скорость на момент начала превышения
8	Структура	Координаты на момент начала превышения
4	Метка времени в LE	Время окончания превышения
1	Байт	Скорость на момент окончания превышения
8	Структура	Координаты на момент окончания превышения
1	Байт	Средняя скорость
1	Байт	Максимальная скорость

Е.5 Используемые тэги

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
0x32	RESUMESESSION		Выдается тахографом, если у него есть сессионные ключи
0x33	DENYSESSION		Выдается сервером в случае отказа установления/восстановления сессии
0x34	CACERTREQUEST		Выдается тахографом, если у него нет сертификата УЦ
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
0x38	REAUTH		Выдается тахографом в случае, если он считает, что необходима повторная динамическая аутентификация
0x39	MESSAGE		Зашифрованные сообщения, защищенные имитовставкой
0x3A-0x3F	RFU		Зарезервировано
Простые тэги для передачи данных в сообщениях при установлении соединения и аутентификации			
0x01	Сертификат	byte[]	Сертификат
0x02	Server Address	ascii	
0x03	Part Number	byte[]	Заводской номер СКЗИ
0x04	KeyId	byte[]	Идентификатор(ы) ключа проверки сертификата
0x05	Rnd /SSC	byte[16]	Случайное число / Случайное число — счетчик
0x06	Криптограмма	byte[]	Криптограмма аутентификации/запроса
0x08-0x0F	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	4e	Номер последнего сообщения, полученного отправителем
0x12	RetransmitReq	0	Запрос повторной передачи предыдущего пакета
0x13-0x19	RFU		
0x1A	Concatenation	1	0 — начало блока, 1 — продолжение, 2 — конец
0x1B	FragmentNo	1-4 int be	Порядковый номер фрагмента конкатенированного сообщения
0x1C-0x1D	RFU		
0x1C	Priority	1	Уровень приоритета сообщения

Окончание таблицы

Тэг	Наименование	Длина, байт	Примечание
0x1F	ServerInitated	0	Добавляется сервером, если сообщение отправлено по его инициативе, а не в качестве подтверждения сообщения от тахографа
Простой тэг для передачи имитовставки			
0x1E	MAC	6 byte[]	Имитовставка вычисляется на все тэги в сообщении
Составные тэги для передачи содержательных данных			
0x20	MessageData	byte[]	Открытые данные, передаваемые в сообщении
0xA0	MessageData	byte[]	Зашифрованные данные, передаваемые в сообщении
Простые тэги для передачи данных по запросу тахографа в тэгах 0x20/ 0xA0 в сообщениях с содержательными данными (MESSAGE)			
0x0A	Data	до 922/ до 914 список блоков	Данные
0x0B	Signed Attrs	46 byte[]	Атрибуты подписи
0x0C	Signature	64 byte[]	Подпись

Библиография

[1] Технический регламент Таможенного союза ТР ТС 018/2011 «О безопасности колесных транспортных средств»

[2] Федеральный закон от 10 декабря 1995 г. № 196-ФЗ «О безопасности дорожного движения»

[3] Федеральный закон от 8 ноября 2007 г. № 257-ФЗ «Об автомобильных дорогах и дорожной деятельности в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации»

[4] ИСО/МЭК 8859-8:1999 Информационные технологии. 8-битовые однобайтовые наборы кодированных графических знаков. Часть 8. Латинский/древнееврейский алфавит

УДК 621.398 ОКС 35.240.60

Ключевые слова: телекоммуникации, радионавигация, протокол обмена данными, глобальная навигационная спутниковая система, тахограф, системы транспортной телематики

Редактор *Н.А. Аргунова*
Технический редактор *И.Е. Черепкова*
Корректор *С.И. Фирсова*
Компьютерная верстка *М.В. Лебедевой*

Сдано в набор 11.01.2021. Подписано в печать 22.01.2021. Формат 60x84¼. Гарнитура Ариал.
Усл. печ. л. 6,98. Уч.-изд. л. 6.28.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru