ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53531— 2009

ТЕЛЕВИДЕНИЕ ВЕЩАТЕЛЬНОЕ ЦИФРОВОЕ. ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СЕТЯХ КАБЕЛЬНОГО И НАЗЕМНОГО ТЕЛЕВИЗИОННОГО ВЕЩАНИЯ

Основные параметры. Технические требования

Издание официальное

Москва
Стандартинформ
2020

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным унитарным предприятием «Самарский отраслевой научно-исследовательский институт радио» (ФГУП СОНИИР)

2 ВНЕСЕН Техническим комитетом по стандартизации № 480 «Связь»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 793-ст

4 В настоящем стандарте учтены основные нормативные положения следующих международных стандартов:

- DVB Doc. A011 rev.1, June 1996 «Цифровое телевизионное вещание. Единый алгоритм скремблирования. Соглашение о нераспространении» (DVB Doc. A011 rev.1, June 1996 «Digital Video Broadcasting (DVB) — DVB Common Scrambling Algorithm — Distribution Agreement», NEQ);
- DVB Doc. A0061, rev.1, Oct. 95 «Цифровое телевизионное вещание. Антипиратское законодательство для цифрового телевизионного вещания» (DVB Doc. A0061, rev.1, Oct. 95 «Digital Video Broadcasting (DVB) — Recommendations — Of the European Project — Digital Video Broadcasting — Antipiracy legislation for digital video broadcasting», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Май 2020 г.

*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, 2010, 2020

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 Основные параметры оборудования защиты информации, передаваемой по сетям кабельного и наземного телевизионного вещания, от несанкционированного доступа 6
4.1 Определение системы 6
4.2 Структурные схемы передающих и приемных частей систем ограничения доступа 9
4.3 Основные параметры 15
5 Технические требования 16
5.1 Общие технические требования 16
5.2 Требования к интерфейсам 16
5.3 Требования электромагнитной совместимости 16
5.4 Требования безопасности 18
5.5 Требования к электропитанию 18
5.6 Требования по стойкости к климатическим и механическим воздействиям 18
Приложение А (справочное) Структура и основные параметры транспортного потока, основные параметры таблиц программно-зависимой информации (PSI) и таблиц информации о службах (SI), дескриптор ограниченного доступа 19
Приложение Б (обязательное) Параметры интерфейсов между компонентами оборудования системы ограничения доступа Simulcrypt 33
Приложение В (обязательное) Требования к параметрам транспортного потока на входе и выходе оборудования системы ограничения доступа 37
Приложение Г (рекомендуемое) Правила скремблирования транспортного потока. Правила формирования слова управления 39
Приложение Д (обязательное) Требования к параметрам интерфейсов доступа к сети передачи данных с использованием контроля несущей и обнаружением коллизий (Ethernet, Fast Ethernet, Gigabit Ethernet) 40
Приложение Е (обязательное) Требования к параметрам интерфейсов передачи данных RS-232, RS-422, асинхронного последовательного интерфейса (ASI) и синхронного параллельного интерфейса (SPI) 43
Библиография 45

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТЕЛЕВИДЕНИЕ ВЕЩАТЕЛЬНОЕ ЦИФРОВОЕ. ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СЕТЯХ КАБЕЛЬНОГО И НАЗЕМНОГО ТЕЛЕВИЗИОННОГО ВЕЩАНИЯ

Основные параметры. Технические требования

Digital video broadcasting (DVB). Requirements for information protection from non-authoriged access in the cable and terrestrial television broadcast networks. Basic parameters. Technical requirements

Дата введения — 2010—12—01

1 Область применения

Настоящий стандарт распространяется на оборудование систем защиты информации, передаваемой по сетям кабельного и наземного телевизионного вещания, от несанкционированного доступа.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 12.1.030 Система стандартов безопасности труда. Электробезопасность. Защитное заземление, зануление

ГОСТ 12.2.007.0 Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности

ГОСТ 21130 Изделия электротехнические. Зажимы заземляющие и знаки заземления. Конструкция и размеры

ГОСТ 22670 Сеть связи цифровая интегральная. Термины и определения

ГОСТ 28147 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования[1)]

ГОСТ Р 52023 Сети распределительные систем кабельного телевидения. Основные параметры. Технические требования. Методы измерений и испытаний

ГОСТ Р 52210 Телевидение вещательное цифровое. Термины и определения

ГОСТ Р 52591 Система передачи данных пользователя в цифровом телевизионном формате. Основные параметры

ГОСТ Р МЭК 60065[2)] Аудио-, видео- и аналогичная электронная аппаратура. Требования безопасности

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

[1)] Действуют ГОСТ 34.12—2018 «Информационная технология. Криптографическая защита информации. Блочные шифры», ГОСТ 34.13—2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».

[2)] Действует ГОСТ IEC 60065—2013.

Издание официальное

(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 22670, ГОСТ Р 52023, ГОСТ Р 52210, ГОСТ Р 52591, а также следующие термины с соответствующими определениями:

3.1.1 **абонентский приемник (приемник пользователя, хост):** Устройство, предназначенное для приема цифровых сигналов, передаваемых по сетям кабельного и наземного телевизионного вещания.

3.1.2 **букет программ:** Совокупность сервисов, предлагаемых абоненту как единый программный продукт.

3.1.3 **генератор конфиденциальных (Private) данных** (Private Data Generator; PDG): Генератор, который инициирует передачу сообщений, предоставляющих право доступа (EMM) от генератора сообщений EMM (EMMG) на мультиплексор (MUX).

3.1.4 **генератор специальной информации о службах** (Custom Service Information Generator; CSIG): Генератор, который инициирует формирование таблиц программно-зависимой информации (PSI).

3.1.5 **головная станция;** ГС: Совокупность технических средств и устройств, обеспечивающих усиление, преобразование и формирование радиосигналов телевидения, радиовещания, обработку других радиосигналов — часть кабельной распределительной сети.

3.1.6 **данные пользователя (телевизионной информации)** (user data): Данные, передаваемые по цифровому тракту вещательного телевидения вместе с видеоинформацией, звуковой и сервисной информацией и не зависящие от передаваемых телевизионных программ.

3.1.7 **дескремблер:** Устройство, предназначенное для восстановления исходной структуры цифрового сигнала, преобразованного скремблером.

3.1.8 **дескриптор** (descriptor), **описатель:** Кодовое слово, которое служит для описания основного содержания документа; средство описания мультимедийного контента.

3.1.9 **единый алгоритм скремблирования** (Common Scrambling Algoritm; CSA): стандартизованный в рамках DVB Project алгоритм скремблирования сигнала.

3.1.10 **единый интерфейс** (Common Interface; CI): Метод обеспечения доступа к скремблированному сигналу, при котором все узлы приемника, имеющие отношение к защите информации, устанавливаются в модуле защиты.

3.1.11 **идентификатор типа пакета** (Packet Identifier; PID): Тринадцатибитовый указатель в заголовке транспортного пакета, указывает на принадлежность пакета тому или иному потоку данных, является основным признаком, по которому демультиплексор на приемной стороне сортирует приходящие пакеты.

3.1.12 **Интернет протокол** (Internet Protocol; IP): Межсетевой протокол пакетной передачи, работает с 32 битовыми адресами, обеспечивает адресацию и маршрутизацию пакетов в сети; работает без установления соединения, не обеспечивает сохранение порядка следования пакетов, не гарантирует доставку пакетов.

3.1.13 **кабельное цифровое телевизионное вещание** (cable digital television broadcasting; cable digital TV broadcasting): Цифровое телевизионное вещание, осуществляемое с использованием кабельных сетей.

3.1.14 **канал** (channel): Прикладное специфическое представление открытого соединения по протоколу управления передачей (TCP).

3.1.15 **карусель данных:** Передача модулей данных с циклическим повторением.

3.1.16 **коммерческое пиратство:** Действия, направленные на копирование контента с целью последующего вещания или сдачи в прокат, несанкционированные провайдером (владельцем контента).

3.1.17 **контент:** Содержание, мультимедийный продукт (например, телевизионная программа).

3.1.18 **модуль** (module): Малогабаритное устройство, не работающее самостоятельно, предназначенное для выполнения специализированных задач в сотрудничестве с хостом (например, модуль подсистемы условного доступа, модуль приложения электронного путеводителя по программам телевидения).

3.1.19 **модуль защиты:** Микропроцессорное устройство с центральным процессором, дескремблером, интерфейсами транспортного потока и команд, с шинной организацией.

3.1.20 **мультиплекс** (multiplex): Транспортный поток, передающий один или более сервисов (услуг) в единственном физическом канале согласно ETSI [1].

3.1.21 **мультиплекс** (multiplex): Транспортный поток на выходе транспортного мультиплексора.

3.1.22 **мультиплексор** (multiplexer; MUX): Устройство, предназначенное для объединения нескольких потоков данных цифрового телевизионного сигнала в единый поток с добавлением служебных битов.

3.1.23 **основной персональный ключ** (Master Private Key; MPK): Ключ, который используется для шифрования слов управления (CW) и формирования сообщений, управляющих правом доступа (ECM).

3.1.24 **пакетированный элементарный поток;** ПЭП (Packetized Elementary Stream; PES): Поток, в котором данные разбиты на пакеты и снабжены заголовками.

3.1.25 **поле управления скремблированием** (Scrambling_control_field): Поле, передаваемое в таблице взаимосвязи (ассоциации) программ (PAT).

3.1.26 **программный поток данных (цифрового вещательного телевидения)** (Program Stream; PS): Поток данных, образованный путем мультиплексирования элементарных потоков видеоданных и звукоданных цифрового вещательного телевидения, имеющих одну общую тактовую частоту, и сформированный из программных пакетов вещательного телевидения переменной длины.

3.1.27 **ресурс** (resource): Набор функциональных возможностей, предоставляемых хостом (абонентским приемником) для использования модулем. Ресурс описывает набор объектов, которыми обмениваются модуль и хост и с помощью которых модуль использует ресурс.

3.1.28 **секция** (section): Синтаксическая структура, используемая для отображения таблиц информации о службах DVB (SI) и PSI с расширениями в пакетах транспортного потока согласно ETSI [1], ISO/IEC [2].

3.1.29 **сервер** (server): Программный объект, экспортирующий ресурс имеющихся данных. Программный объект устанавливается на физическое устройство. Компьютер, подключенный к сети и предоставляющий услуги другим устройствам, работающим в этой сети.

3.1.30 **сервис (служба, услуга)** (service): Набор элементарных потоков, предлагаемых пользователю как программа и связанных общей синхронизацией. Элементарные потоки состоят из различных данных: видео-, аудио-, субтитров, других данных.

3.1.31 **сервисная информация** (Service Information; SI): Цифровые данные о системе доставки, содержании и расписании передаваемых данных согласно ETSI [1].

3.1.32 **система администрирования (управления) абонентами** (Subscriber Management System; SMS): Система учета сведений об абонентах, содержащая базу данных об абонентах, о декодерах абонентов, о сервисах (службах), на которые они подписались, о расчетах с абонентами и об учете платежей, поступающих от абонентов.

3.1.33 **система ограничения доступа DVB Simulcrypt:** Система, обеспечивающая передачу в одном транспортном потоке нескольких отдельных сообщений, управляющих правом доступа (ECM), и сообщений EMM. Это дает возможность нескольким СОД управлять доступом к одной скремблированной передаче.

3.1.34 **система предоставления полномочий абоненту (авторизации абонента)** (Subscriber Authorrization System; SAS): Система, обеспечивающая организацию, упорядочение и доставку данных для формирования сообщений EMM и сообщений ECM.

3.1.35 **система управления сетью** (Network Management System; NMS): Система, обеспечивающая управление оборудованием СОД и мониторинг оборудования СОД. Система управления сетью сопрягается с системой предоставления полномочий абоненту (авторизации абонента) (SAS) и с системой администрирования (управления) абонентами (SMS).

3.1.36 **скремблер** (scrambler; SCR): Устройство, предназначенное для преобразования структуры цифрового сигнала электросвязи, без изменения скорости передачи символов этого сигнала, с целью приближения его свойств к свойствам случайного сигнала.

3.1.37 **скремблирование** (scrambling): Преобразование структуры цифрового сигнала электросвязи, без изменения скорости передачи символов этого сигнала, с целью приближения его свойств к свойствам случайного сигнала.

3.1.38 **слово управления** (Control Word; CW): Объект данных, используемый для скремблирования (операционный ключ низкого уровня, осуществляющий процесс скремблирования и дескремблирования. CW изменяется с периодичностью от 0,5 до 10 с).

3.1.39 **сообщение, предоставляющее право доступа** (Entitlement Management Message; EMM): Сообщение, которое содержит данные, разрешающие конкретному дескремблеру открыть для просмотра конкретную программу на предусмотренный срок.

3.1.40 **сообщение, управляющее правом доступа** (Entitlement Control Message; ECM): Сообщение, которое передает дескремблеру слово управления (CW), а также информацию о критериях доступа к программам и букетам.

3.1.41 **таблица байтов стаффинга** (Staffing Table; ST): Таблица, применяемая для замены или отмены существующих секций или таблиц SI.

3.1.42 **таблица взаимосвязи (ассоциации) программ** (Program Association Table; PAT): Таблица, содержащая информацию о программах, передаваемых в данном потоке, и идентификаторах, относящихся к этим программам.

3.1.43 **таблица текущего статуса** (Running Status Table; RST): Таблица, в секциях которой передаются сообщения об изменении текущего статуса одного или нескольких событий, передача происходит только в момент изменения статуса.

3.1.44 **таблица состава программы** (Program Map Table; PMT): Таблица, в которой перечислены все компоненты программы с их идентификаторами. Содержит PID всех составляющих конкретной программы. PMT идентифицирует и указывает местоположение потоков, входящих в каждый сервис. PMT указывает местоположение меток PCR каждого сервиса.

3.1.45 **ТЭГ** (tag): Служебный элемент, который размещен в начале заголовка и хранится вместе с данными, не может быть использован как самостоятельный элемент.

3.1.46 **транзакция** (transaction): Логическая единица работы, состоящая из запроса и получения результатов его обработки (короткое сообщение, передаваемое в диалоговом режиме между равноправными объектами прикладных уровней).

3.1.47 **транспортный поток (цифрового вещательного телевидения)** (Transport Stream; TS): Набор из нескольких программных потоков данных цифрового вещательного телевидения, сформированный из программных пакетов постоянной длины с коррекцией ошибок и независимым тактированием от своих источников синхронизации.

3.1.48 **элементарный поток видеоданных (звукоданных, специальных данных) цифрового вещательного телевидения** (Elementary Stream; ES): Последовательность битов видеоданных (звукоданных, специальных данных) цифрового вещательного телевидения.

3.1.49 **EDH-метод обнаружения и визуализации ошибок в последовательном транспортном потоке данных** (error detection and handling; EDH): Метод диагностики ошибок в последовательном транспортном потоке данных, заключающийся в сравнении контрольных слов кода избыточной циклической проверки, вычисляемых в процессе формирования текущего и следующего за ним кадров телевизионного изображения.

3.2 В настоящем стандарте использованы следующие сокращения:

ГС — головная станция;

ОД (CA) — ограниченный доступ;

ОЗУ — оперативное запоминающее устройство;

ПЗУ — постоянное запоминающее устройство;

ПЭП (PES) — пакетированный элементарный поток;

СОД (CAS) — система ограничения доступа; система защиты информации;

ТП (TS) — транспортный поток;

ЦТВ (DVB) — цифровое телевизионное вещание;

АК — Authorization Key (ключ авторизации);

ASI — Asynchronous Serial Interface (асинхронный последовательный интерфейс);

BAT — Bouquet Assotiation Table (таблица объединения букета программ);

BISS — Basic Interoperable Scrambling System (базовая интероперабельная система скремблирования);

CA — Conditional Access (ограниченный доступ; ОД);

CAS — Conditional Access System (система ограниченного доступа; СОД);

CAT — Conditional Access Table (таблица ограниченного доступа);

CI — Common Interface (единый интерфейс);

CiP — Carousel in the (P)SIG (карусель генератора таблиц PSI, SI);

CPSI — Custom PSI (специальная программно-зависимая информация),

CPSIG — Custom Program Specific Information Generator (генератор специальной программно-зависимой информации);

CRC — Cyclic Redudance Chek (проверка циклическим избыточным кодом);

CRC_16 — поле кода циклической проверки, контролирует ошибки пакетов PES при использовании генераторного полинома $x^{16} + x^{12} + x^5 + 1$,

CRC_32 — поле кода циклической проверки, контролирует ошибки в секции таблицы PSI при использовании генераторного полинома $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$;

CSA — Common Scrambling Algorithm (единый алгоритм скремблирования);

CSI — Custom SI (специальная информация о службах);

CSIG — Custom SI Generator (генератор специальной информации о службах);

CSMA-CD — Carrier Sense Multiple Access with Collision Detection (множественный доступ с контролем несущей и обнаружением коллизий (конфликтов));

CW — Control Word (слово управления);

CWG — Control Word Generator (генератор слова управления);

DVB — Digital Video Broadcasting (цифровое телевизионное вещание; ЦТВ);

EBU — European Broadcasting Union — Европейский союз радиовещания;

ECM — Entitlement Control Message (сообщение, управляющее правом доступа);

ECMG — Entitlement Control Message Generator (генератор сообщений ECM);

EDH — Error Detection and Handling (метод обнаружения и визуализации ошибок в последовательном транспортном потоке данных (цифрового вещательного телевидения));

EIS — Event Information Scheduler (планировщик управления событиями);

EIT — Event Information Table (таблица информации о событиях);

EMM — Entitlement Management Message (сообщение, предоставляющие право доступа);

EMMG — Entitlement Management Message Generator (генератор сообщений EMM);

ETR — ETSI Technical Report (технический отчет ETSI);

ES — Elementary Stream (элементарный поток видеоданных (звукоданных, специальных данных) цифрового вещательного телевидения);

ETSI — European Telecommunications Standards Institute (Европейский институт стандартизации электросвязи);

IEC — International Electrotechnical Commission/Committee (Международная электротехническая комиссия);

IETF — Internet Engineering Tack Force (Техническая комиссия Internet, разрабатывающая документы RFC);

ISO — International Organization for Standardization (Международная организация по стандартизации);

IP — Internet Protocol (Интернет протокол);

MPK — Master Private Key (основной персональный ключ);

MPEG — Motion Pictures Expert Group (группа стандартов сжатия видео- и аудиоданных);

MUX — Multiplexer (мультиплексор);

NIT — Network Information Table (таблица сетевой информации);

NMS — Network Management System (система управления сетью);

PAT — Program Assotiation Table (таблица взаимосвязи (ассоциации) программ);

PCMCIA — Personal Computer Memory Card (Международная ассоциация по разработке стандарта плат памяти персональных компьютеров; шина платы памяти персонального компьютера);

PCR — Program Clock Reference (ссылка на программные часы);

PD — Private Data (конфиденциальные (частные) данные);

PDG — Private Data Generator (генератор конфиденциальных (частных) данных);

PES — Packetized Elementary Stream (пакетированный элементарный поток; ПЭП);

PID — Packet Identifier (идентификатор типа пакета);

PMT — Program Map Table (таблица состава программы);

program_map_PID — программный идентификатор PID;

PS — Program Stream (программный поток данных (цифрового вещательного телевидения));

PSI — Program Specific Information (программно-зависимая информация, размещается в таблицах программно-зависимой информации, содержащих сведения о составе программ и идентификаторах их компонентов);

PSIG — Program Specific Information Generator (генератор программно-зависимой информации);

P-STD — Program Stream system target decoder (системный декодер программного потока);

RFC — Request for Comments (предложения для обсуждения, серия нормативных документов, стандартизирующих протоколы Internet);

RST — Running Status Table (таблица текущего статуса);

SAS — Subscriber Authorization System (система предоставления полномочий абоненту (авторизации абонента));

SCR — scrambler (скремблер);
SCS — Simulcrypt Synchronizer (синхронизатор Simulcrypt);
Scrambling_control_field — поле управления скремблированием; передается в таблице PAT;
SDT — Service Description Table (таблица описания служб DVB);
SI — Service Information (информация о службах DVB);
SIG — Service Information Generator (генератор информации о службах DVB);
SMS — Subscriber Management System (система администрирования (управления) абонентами);
SPI — Synchronous Parallel Interface (синхронный параллельный интерфейс);
table_id — флаг, составная часть заголовка, идентификатор таблицы транспортного потока;
ST — Staffing Table (таблица байтов стаффинга);
TCP — Transmission Control Protocol (протокол управления передачей (из стека протоколов TCP/IP));
TCP/IP — стек протоколов сетевого и транспортного уровня;
TDT — Time and Data Table (таблица времени и даты);
TOT — Time Offset Table (таблица смещения времени);
TS — Transport Stream (транспортный поток; ТП);
UDP — User Datagram Protocol (протокол передачи дейтаграмм пользователя).

4 Основные параметры оборудования защиты информации, передаваемой по сетям кабельного и наземного телевизионного вещания, от несанкционированного доступа

4.1 Определение системы

Система защиты информации (система ограничения доступа; СОД) представляет собой совокупность оборудования и программных средств, обеспечивающую ограничение доступа пользователей (абонентов) сетей цифрового вещания (сетей кабельного и наземного телевизионного вещания) к сервисам (службам), передаваемым в составе транспортного потока.

Процедура защиты информации, передаваемой по сетям цифрового вещания, от несанкционированного доступа включает два основных процесса:

- скремблирование транспортного потока — перед его передачей в каналы распределения или вещания;

- дескремблирование (восстановление) исходной структуры транспортного потока на выходе тракта передачи, защищаемого от несанкционированного доступа, — при приеме переданного сигнала.

Скремблирование транспортного потока в большинстве практических случаев выполняется в соответствии с единым алгоритмом скремблирования (CSA) согласно DVB [3], [4] и ETSI [5]. Единый алгоритм скремблирования в детализированном виде предоставляется Европейским институтом стандартизации электросвязи (ETSI) производителям оборудования систем ограниченного доступа под письменную гарантию неразглашения.

Структура и основные параметры транспортного потока, участвующего в процедурах скремблирования и дескремблирования, приведены в приложении А.

СОД может быть одноуровневой или многоуровневой.

4.1.1 Одноуровневая система ограничения доступа

Структурная схема одноуровневой СОД показана на рисунке 1.

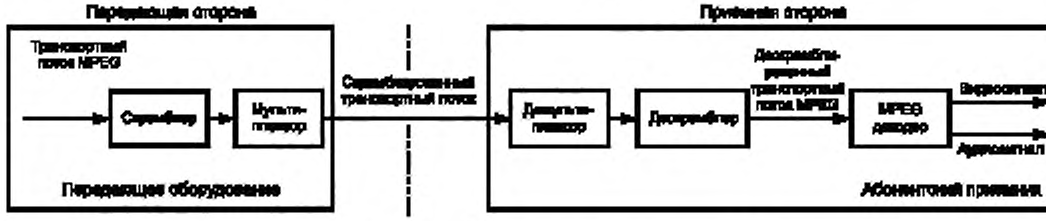


Рисунок 1 — Структурная схема одноуровневой СОД

Скремблирование транспортного потока выполняется в скремблере перемножением передаваемого транспортного потока с псевдослучайной последовательностью (ПСП), соответствующей слову

управления (CW). Слова управления являются открытыми (незашифрованными). Слова управления вводятся в скремблер и дескремблер вручную непосредственно с лицевых панелей этих устройств.

На приемной стороне абонентский приемник дескремблирует принятый мультиплекс перемножением мультиплекса с «местной» псевдослучайной последовательностью (ПСП), соответствующей тому CW, которое было применено при скремблировании передаваемого транспортного потока.

В связи с тем, что при использовании незашифрованных слов управления не обеспечивается достаточной защиты от несанкционированного доступа к словам управления, применение такой СОД может быть рекомендовано только для коротких сеансов передачи при условии периодической замены слов управления и на передающей и на приемной сторонах одновременно.

Выбор слов управления, способ и периодичность передачи слов управления от передающей к приемной части одноуровневой СОД определяются соглашением между провайдером и оператором. К одноуровневым СОД может быть отнесена система ограничения доступа BISS-1 согласно EBU [6].

4.1.2 Многоуровневые системы ограничения доступа

В двух- и более уровневых СОД применяется шифрование слов управления с различной (в зависимости от уровня) степенью секретности и с последующей передачей шифрованных слов управления в составе транспортного потока.

4.1.2.1 Двухуровневая система ограничения доступа

В двухуровневых СОД повышение уровня защиты системы от несанкционированного доступа обеспечивается повышением уровня защиты слов управления, определяющих конкретную криптографическую операцию. Повышение уровня защиты выполняется с помощью шифрования слов управления в шифраторе CW.

Структурная схема двухуровневой СОД показана на рисунке 2.

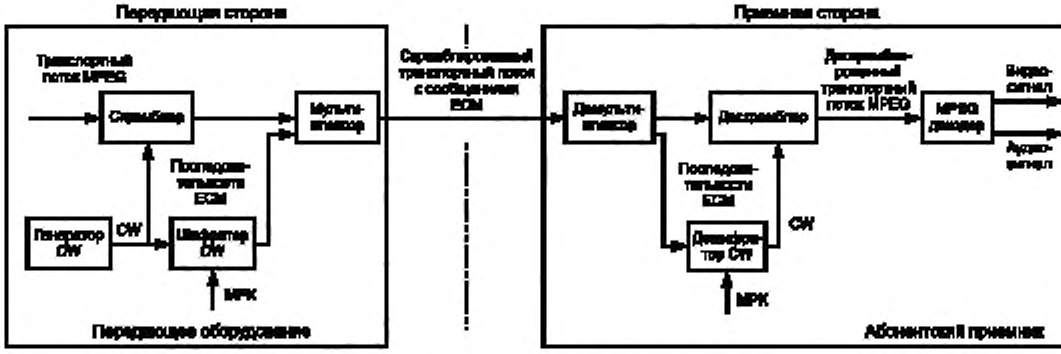


Рисунок 2 — Структурная схема двухуровневой СОД

Слова управления в шифраторе CW шифруются с применением основных персональных ключей (МРК) для формирования сообщения, управляющего правом доступа (ECM).

Сообщения ECM в мультиплексоре вводятся в состав скремблированного транспортного потока, который затем передается в каналы распределения или вещания и поступает на приемную сторону сети цифрового вещания.

На приемной стороне сети (в абонентском приемнике) сообщение ECM выделяется демультиплексором из транспортного потока и поступает на дешифратор CW, который использует ключ МРК и формирует слово управления CW. Дескремблер транспортного потока, используя слово управления CW, формирует дескремблированный транспортный поток.

Ключи МРК могут храниться в энергонезависимой памяти смарт-карт абонентских приемников или в энергонезависимой памяти модулей защиты, входящих в состав абонентских приемников.

В случае применения одно- и двухуровневых СОД допускается отсутствие сообщений ECM и EMM в мультиплексе транспортного потока.

К двухуровневым СОД может быть отнесена система ограничения доступа BISS-E согласно EBU [6].

4.1.2.2 Трехуровневая система ограничения доступа

Один из вариантов структурной схемы трехуровневой СОД показан на рисунке 3.

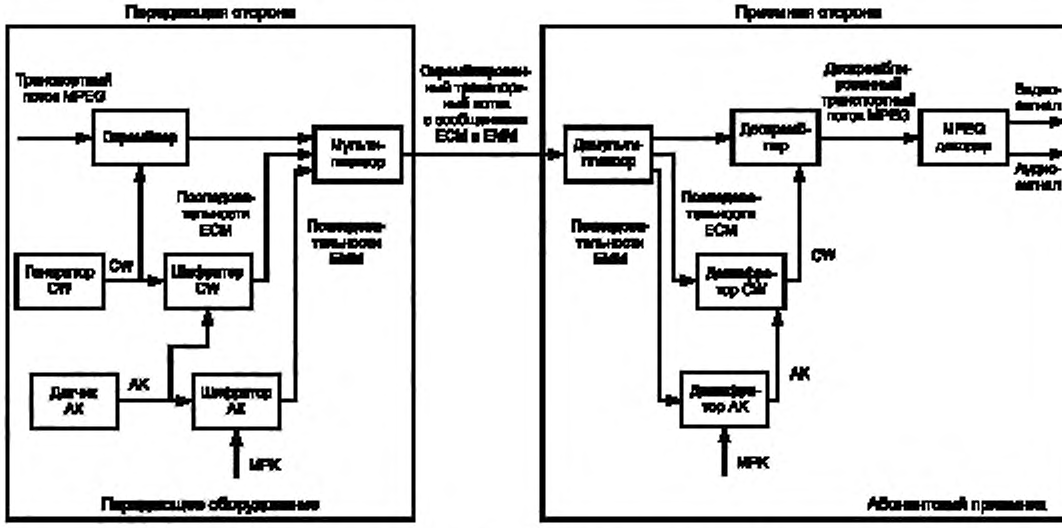


Рисунок 3 — Структурная схема трехуровневой СОД

В трехуровневой СОД шифрование слов управления CW выполняется с помощью ключей авторизации (АК), которые в свою очередь шифруются с помощью ключей МРК, действующих в течение длительных интервалов времени. Шифрованные слова управления CW в форме сообщений ECM и шифрованные ключи АК в форме сообщения EMM через мультиплексор вводятся в состав транспортного потока и передаются на приемную часть тракта по каналам вещания.

На приемной стороне в абонентском приемнике формирование АК из EMM происходит в дешифраторе АК с помощью ключей МРК.

4.1.3 Основные типы трехуровневых систем ограничения доступа

Трехуровневые системы ограничения доступа являются наиболее распространенными.

К основным типам трехуровневых систем ограничения доступа относятся системы Simulcrypt и Multicrypt. В обоих типах систем ограниченный доступ обеспечивается в соответствии с единым алгоритмом скремблирования (CSA) согласно DVB [3], [4] и ETSI [5].

В системе Simulcrypt управление доступом к пакету передаваемых программ в составе одного мультиплекса обеспечивается при одновременной работе нескольких СОД, использующих единый способ скремблирования (общий скремблер), в нескольких сетях вещания. Передача слов управления и кодирующих ключей от каждой СОД на приемники пользователей обеспечивается при передаче в составе одного транспортного потока нескольких независимых сообщений, управляющих правом доступа (ECM), и нескольких независимых сообщений, предоставляющих право доступа (EMM). Передаваемые программы принимаются и дескремблируются абонентскими приемниками, адаптированными для работы с необходимыми СОД.

Абонентские приемники сетей кабельного телевизионного вещания или наземного телевизионного вещания выбирают из принятого транспортного потока служебные сообщения ECM и EMM, соответствующие СОД, установленной в этом приемнике, демультиплексируют мультиплекс и дескремблируют необходимые транспортные потоки.

В системе Multicrypt ограничение доступа обеспечивается СОД, в которых скремблирование выполняется независимо друг от друга. Доступ абонентов к необходимым передаваемым программам достигается использованием сменных модулей абонентского приемника. В сменном модуле размещены узлы, участвующие в процедурах защиты информации.

Абонентский приемник выполняет функции приема, демодуляции и декодирования. Единый интерфейс (CI) между узлами цифрового приемника и сменным модулем (модулем защиты) выполняется в виде шины персонального компьютера PCMCIA, в слоты которой вставляются модули различных систем защиты (смарт-карты PCMCIA).

Допускается использование абонентского приемника системы Multicrypt для работы в системе Simulcrypt.

4.2 Структурные схемы передающих и приемных частей систем ограничения доступа

4.2.1 Структурная схема передающей части оборудования СОД Simulcrypt показана на рисунке 4.

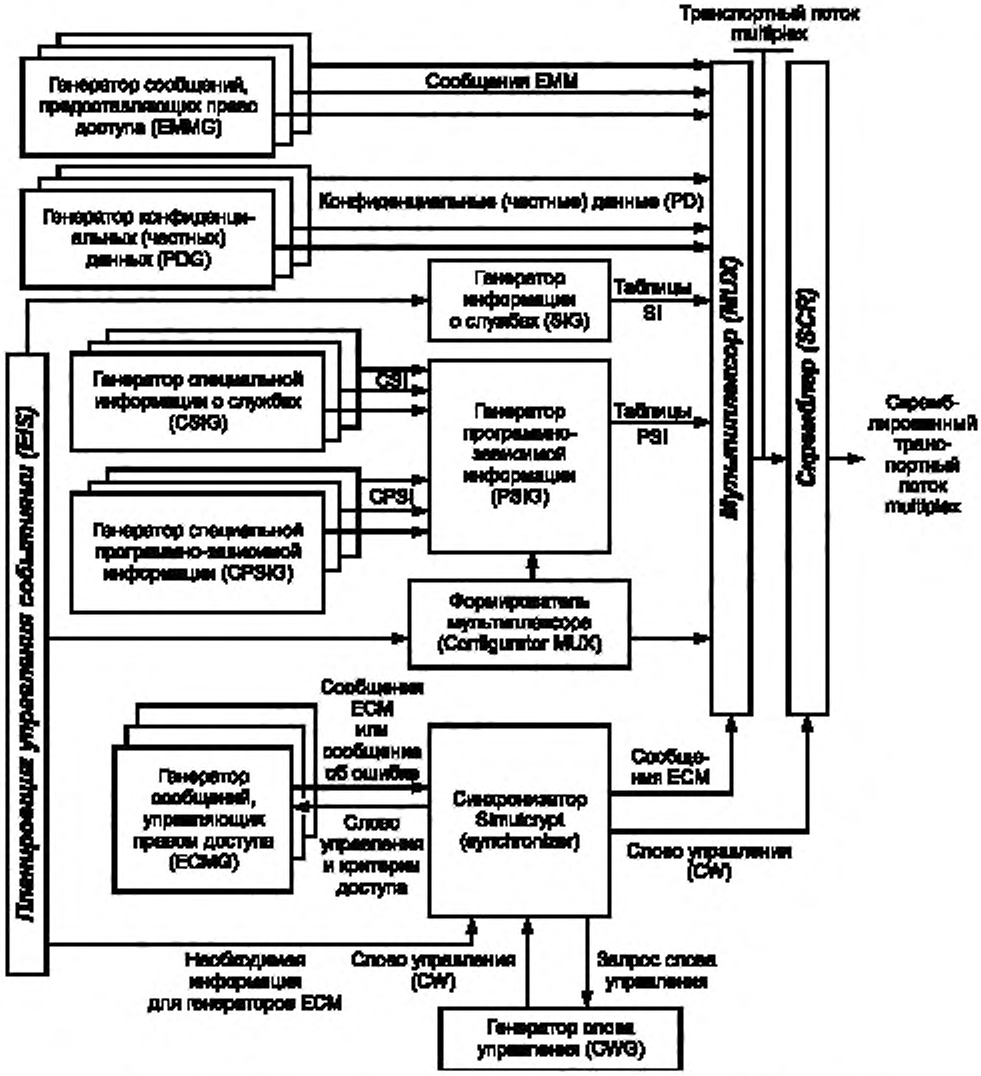


Рисунок 4 — Структурная схема передающей части оборудования СОД Simulcrypt

Передающая часть оборудования СОД Simulcrypt размещается на головных станциях сетей кабельного телевизионного вещания или в других узлах распределения программ вещания.

На рисунке 4 показаны компоненты, входящие в состав передающего оборудования СОД Simulcrypt согласно ETSI [7], [8], компоненты головной станции (ГС), взаимодействующие с оборудованием СОД Simulcrypt, и функциональные связи между компонентами.

Транспортные потоки подаются на вход мультиплексора оборудования СОД (на структурной схеме не показаны). Оборудование СОД формирует совокупности сообщений ECM и EMM и вводит их в состав транспортного потока.

4.2.2 В состав передающего оборудования трехуровневой СОД Simulcrypt входят следующие компоненты:

- планировщик управлением событиями (EIS). Представляет собой функциональную единицу, содержащую все данные о конфигурации СОД и специальную информацию, необходимую для создания СОД. Допускается перераспределение функций EIS между несколькими физическими единицами или терминалами. Функции EIS могут выполнять система предоставления полномочий абоненту (авторизации абонента) (SAS) и система администрирования (управления) абонентами (SMS),

- генератор сообщений ECM (ECMG) — формирует и передает на мультиплексор сообщения ECM;

- генератор сообщений EMM (EMMG) — формирует и передает на мультиплексор сообщения EMM;

- генератор частных данных (PDG) — инициирует передачу сообщений EMM от EMMG на мультиплексор;

- генератор SI (SIG) — формирует таблицы SI для передачи на мультиплексор. Сервер генератора таблиц SI (в составе SIG) получает исходные данные от EIS и от серверов Custom SI, представленные провайдерами услуг ограниченного доступа (ОД);

- генератор PSI (PSIG) — формирует таблицы PSI для передачи на мультиплексор, используя исходные данные, полученные сервером PSI (в составе PSIG) от формирователя мультиплексора (Configurator MUX), и дополнительные данные от серверов CSI и CPSI. Серверы CSI и CPSI входят в состав генератора специальной информации о службах (CSIG) и генератора специальной программно-зависимой информации (CPSIG) соответственно. Данные для серверов CSI и CPSI представляются провайдерами услуг ограниченного доступа;

- формирователь мультиплексора (Configurator MUX) — формирует топологию мультиплексора и определяет данные, вводимые в генератор программно-зависимой информации (PSIG), используя данные, получаемые от EIS. Правила соединения «Configurator MUX и MUX» и «Configurator MUX и PSIG» данный стандарт не определяет;

- синхронизатор Simulcrypt — получает слово управления (CW), сообщение, управляющее правом доступа (ECM), и обеспечивает их синхронную передачу на мультиплексор (MUX) и скремблер (SCR);

- генератор слова управления (CWG) — по запросу синхронизатора Simulcrypt формирует слово управления и передает его на синхронизатор Simulcrypt;

- мультиплексор (MUX) — формирует транспортный поток — мультиплекс, используя входной транспортный поток стандарта и данные, получаемые от генераторов EMM, ECM, PD, SI, PSI и синхронизатора Simulcrypt;

- скремблер (SCR) — обеспечивает скремблирование транспортного потока, поступающего от мультиплексора (MUX) с использованием слова управления (CW).

Количество генераторов ECMG, EMMG, PDG, CSIG, CPSIG, ECMG должно соответствовать количеству систем ограниченного доступа, участвующих в скремблировании мультиплекса.

Допускается выделение синхронизатора Simulcrypt, формирователя мультиплексора, мультиплексора, скремблера и EIS из состава оборудования СОД Simulcrypt и включение этих компонент в состав оборудования головной станции или других узлов распределения программ вещания.

На вход оборудования СОД Simulcrypt, кроме входных данных, получаемых через входные интерфейсы MPEG, подаются сигналы управления.

Управление и мониторинг компонент оборудования СОД Simulcrypt выполняются системой управления сетью (NMS). NMS на рисунке 4 не показана.

Выходными сигналами оборудования СОД на головной станции являются:

- скремблированные транспортные потоки;

- сигналы управления.

Взаимодействие между оборудованием СОД Simulcrypt нескольких головных станций должно выполняться в соответствии с моделью, включающей в себя следующие уровни:

- доступа к сети (физический и канальный);

- сетевой;

- транспортный;

- прикладной (сеансовый);

- приложений.

Интерфейс физического уровня должен быть интерфейсом локальной сети на основе протокола CSMA-CD. Спецификация уровня 10 Base-T (или другого полностью совместимого уровня) должна использоваться во всех интерфейсах, определенных в соответствии с настоящим стандартом.

Канальный уровень обеспечивает двум головным станциям возможность обмена информацией. Функциональные возможности канального уровня соответствуют протоколам локальной сети на основе протокола CSMA-CD.

Сетевой уровень обеспечивает средства, позволяющие двум головным станциям иметь доступ к информации о станции непосредственно или косвенно в сети через головные станции и шлюзы. Он обеспечивает также головным станциям возможность межсетевого взаимодействия (протокол маршрутизации в среде Интернет согласно IETF [9]). Головные станции в пределах протокола межсетевого взаимодействия идентифицированы их уникальными IP-адресами.

Перечень интерфейсов между компонентами оборудования и общие характеристики этих интерфейсов даны в таблице Б.1 (приложение Б). Для обмена данными между компонентами оборудования используются два типа протоколов: протокол, ориентированный на соединение (TCP), и протокол передачи дейтаграмм пользователя (UDP).

Должна обеспечиваться возможность взаимодействия передающей части оборудования СОД Simulcrypt с передающими частями оборудования СОД Simulcrypt головных станций верхнего и нижнего уровней. Интерфейсы передающей части оборудования СОД Simulcrypt должны соответствовать требованиям, приведенным в п. 5.2 настоящего стандарта.

Параметры сообщений протокола, ориентированного на соединение (TCP), приведены в таблице Б.2 (приложение Б).

4.2.3 Структурная схема передающего оборудования СОД Multicrypt, обеспечивающего вещание при использовании одной системы ограничения доступа, показана на рисунке 5. В состав передающего оборудования трехуровневой СОД Multicrypt входят следующие компоненты:

- планировщик управлением событиями (EIS);
- генератор сообщений ECM (ECMG);
- генератор сообщений EMM (EMMG);
- генератор частных данных (PDG);
- генератор таблиц SI (SIG);
- генератор таблиц PSI (PSIG);
- формирователь мультиплексора;
- синхронизатор;
- генератор слова управления (CWG);
- мультиплексор (MUX);
- скремблер (SCR).

Функциональное назначение этих компонент и их взаимодействие должно быть в соответствии с 4.2.2.

Допускается выделение синхронизатора, формирователя мультиплексора, мультиплексора, скремблера и EIS из состава оборудования СОД и включение этих компонент в состав оборудования головной станции или других узлов распределения программ вещания.

На вход оборудования СОД, кроме входных данных, получаемых через входные интерфейсы MPEG, подаются сигналы управления.

Управление и мониторинг компонент оборудования СОД выполняются системой управления сетью (NMS). NMS на рисунке 5 не показана.

Алгоритмы и протоколы обмена между компонентами передающей части СОД Simulcrypt рекомендованы для передающей части СОД Multicrypt с учетом того, что ограничение доступа должно обеспечиваться при использовании одной СОД.

4.2.4 Структурная схема приемного оборудования СОД, включающего абонентский приемник и модуль защиты, соединенные через единый интерфейс (CI), показана на рисунке 6.

Абонентский приемник выполняет прием, демодуляцию и декодирование цифрового сигнала.

Узлы приемного оборудования СОД, участвующие в процедурах защиты информации, выделяются в отдельный сменный модуль защиты.

Структурная схема модуля защиты представлена на рисунке 7.

Модуль защиты выполняется в виде устройства с центральным процессором, стираемым программируемым ПЗУ, энергонезависимым ОЗУ, дескремблером, узлом фильтрации сообщений, передаваемых в таблицах CAT, PMT, PAT, NIT, процессором защиты, интерфейсами входящего и исходящего транспортного потока TS и интерфейсом команд. Узел фильтрации сообщений выделяет из транспортного потока данные, разрешающие дескремблирование транспортного потока.

Дескремблирование пакетов транспортного потока TS или пакетов пакетированного элементарного потока PES запрещается, если флаги управления **transport_scrambling_control_flag** и **scrambling_control_flag** находятся в состоянии «00».

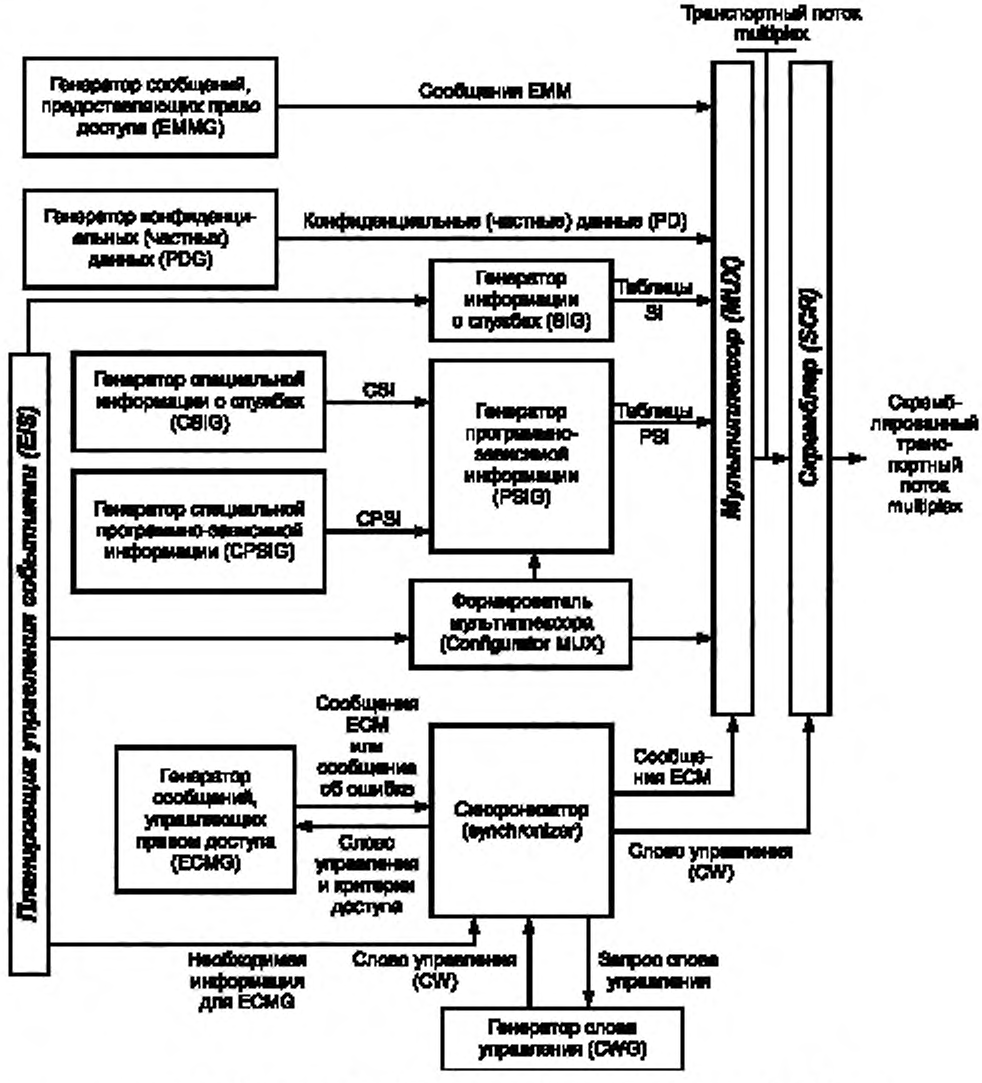


Рисунок 5 — Структурная схема передающей части оборудования СОД Multicrypt

Процессор защиты выполняет выделение и хранение ключей и заголовков пакетов. Допускается размещение процессора защиты в сменной смарт-карте.

Единый интерфейс (CI) включает в себя интерфейс транспортного потока и интерфейс команд.

4.2.4.1 Интерфейс транспортного потока должен быть организован по последовательно-шлейфовому типу. Взаимодействие между абонентским приемником и каждым модулем защиты должно осуществляться независимо от других модулей защиты. При отсоединении конкретного модуля защиты в интерфейсе команд не должны возникать нарушения, влияющие на работоспособность любого другого модуля защиты. При совместной работе с несколькими модулями защиты абонентский приемник должен отбирать модули защиты для корректного дескремблирования выбранных сервисов.

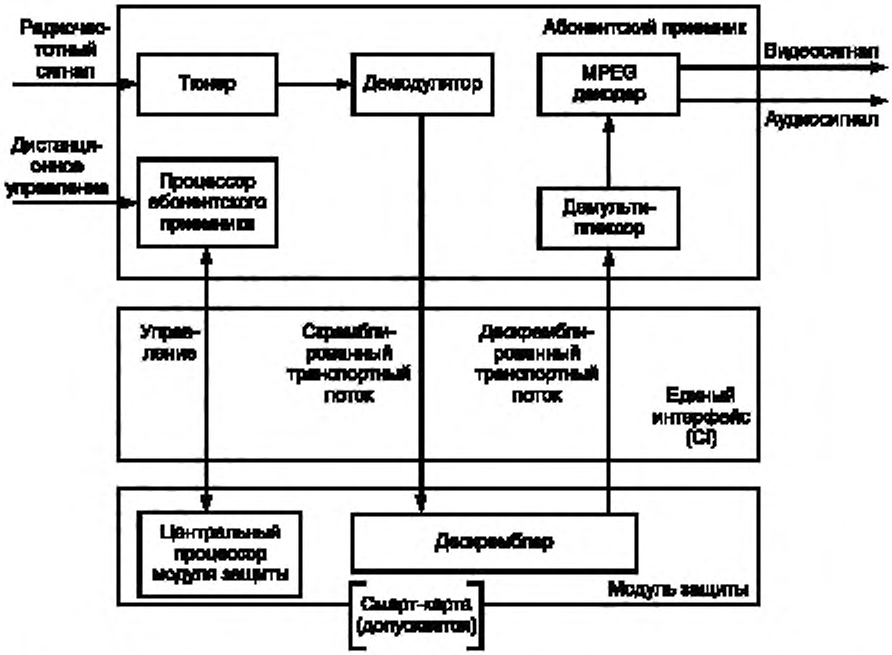


Рисунок 6 — Структурная схема приемного оборудования СОД с одним модулем защиты

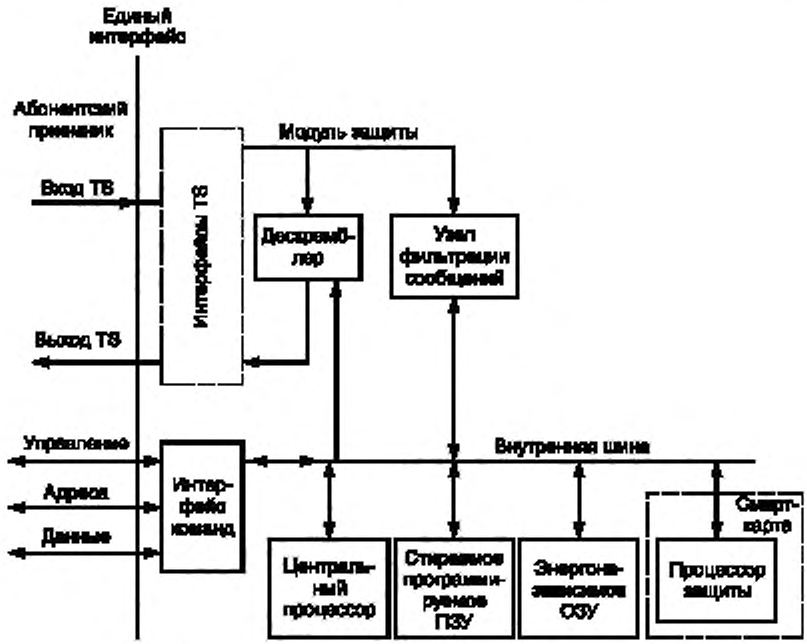


Рисунок 7 — Структурная схема модуля защиты

Интерфейс транспортного потока должен включать следующие уровни:

- транспортный уровень;
- соединительный уровень смарт-карты;
- физический уровень смарт-карты.

Интерфейсы транспортного потока модуля защиты должны иметь параллельные 8-разрядные входы и выходы совместно с сигналами управления и байтовой синхронизацией.

Скорость передачи данных между отдельным модулем защиты и абонентским приемником в каждом направлении должна быть не менее 3,5 Мбит/с.

Подсоединение и отключение модуля защиты должны обеспечиваться независимо от состояния абонентского приемника (включен/выключен). При этом должна обеспечиваться работоспособность модуля защиты, абонентского приемника и сохранность данных, записанных в модуле.

Если модуль защиты не подключен, то должен осуществляться его обход по интерфейсу транспортного потока. Передача команд на отсутствующий модуль защиты должна блокироваться. При подключении модуля защиты к абонентскому приемнику должна выполняться инициализация модуля путем проверки физических соединений и соответствия модуля защиты спецификации.

Включение модуля защиты в тракт обработки транспортного потока должно осуществляться абонентским приемником после успешного завершения этих процедур. Допускается потеря данных транспортного потока во время подключения и инициализации модуля защиты.

Если подключаемый модуль защиты не соответствует спецификации, то должна сохраняться работоспособность абонентского приемника. Процедура полной инициализации модуля при этом не проводится, а абонентский приемник сообщает пользователю о подключении неопознанного модуля защиты.

При отсоединении модуля защиты от абонентского приемника должен восстанавливаться исходный режим обработки транспортного потока. На момент отсоединения модуля защиты допускается потеря данных транспортного потока.

Детализированные требования к интерфейсу транспортного потока должны быть в соответствии с EN [10].

4.2.4.2 Интерфейс команд должен осуществлять обмен служебными сообщениями между абонентским приемником и модулем защиты.

Протоколы взаимодействия по интерфейсу команд должны быть разделены на следующие уровни:

- сеансовый уровень;
- транспортный подуровень;
- уровень смарт-карты;
- физический уровень смарт-карты;
- транспортный подуровень смарт-карты.

На физическом уровне единый интерфейс должен обеспечивать:

- формирование логических соединений для транспортных потоков и команд;
- необходимые скорости передачи данных;
- необходимые режимы соединения и разъединения цепей;
- инициализацию сигналов низкого уровня;
- возможность использования множества модулей защиты при их последовательном соединении (в том числе при использовании для работы в СОД).

Логические соединения должны обеспечивать независимую двунаправленную передачу транспортного потока и команд. При этом интерфейс транспортного потока должен обрабатывать транспортный поток в виде последовательности пакетов TS либо смежных, либо разделенных нулевыми байтами.

Транспортный поток от модуля защиты к абонентскому приемнику (исходящий транспортный поток) может содержать входящие пакеты TS, возвращаемые как в скремблированной форме, так и в дескремблированной форме.

Детализированные требования к интерфейсу команд должны быть в соответствии с EN [10].

Допускается выполнение модулей защиты со встроенными функциями смарт-карты.

Прикладной уровень интерфейса не накладывает ограничений на число модулей защиты, подключаемых к абонентскому приемнику. Они допускаются из-за особенностей конструкции абонентского приемника. При реализации абонентского приемника для работы в СОД Multicrypt рекомендуется обеспечение возможности установки в нем не менее 15 модулей защиты. Принцип подключения нескольких модулей защиты к абонентскому приемнику показан на рисунке 8.

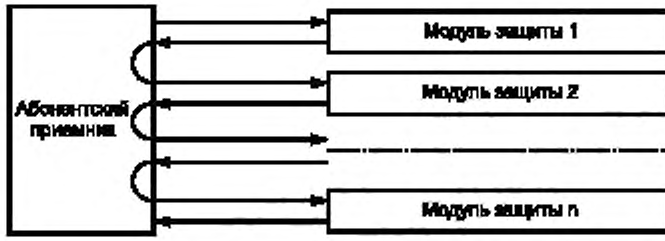


Рисунок 8 — Принцип подключения к абонентскому приемнику последовательно соединенных модулей защиты

Единый интерфейс в виде шины персонального компьютера должен выполняться в соответствии с EN [10] (приложение А).

4.2.5 При реализации оборудования одно-, двух-, четырех- и более уровневых систем ограничения доступа рекомендуется применять технические решения, соответствующие требованиям и рекомендациям настоящего стандарта.

4.2.6 Параметры транспортного потока на входе и выходе оборудования СОД соответствуют нормам в соответствии с приложением В для параметров первого и второго уровней приоритета.

4.3 Основные параметры

4.3.1 Правила скремблирования транспортного потока определены ETR [11], DVB [12], [15] и приведены в приложении Г.

Скремблирование транспортного потока допускается выполнять в соответствии с требованиями ГОСТ 28147.

4.3.2 Правила формирования слова управления в соответствии с ETSI [7], [8] приведены в приложении Г.

4.3.3 Взаимодействие между оборудованием СОД нескольких головных станций должно выполняться в соответствии с моделью, включающей следующие уровни согласно ETSI [7], [8]:

- доступа к сети (физический и канальный);
- сетевой;
- транспортный;
- прикладной (сеансовый);
- приложений.

Интерфейс физического и канального уровней должен быть интерфейсом локальной сети Ethernet 10 Base-T IEEE [14].

Сетевой уровень должен осуществлять головным станциям возможность межсетевого взаимодействия (протокол маршрутизации в среде Интернет в соответствии с IETF [9]). Головные станции в пределах протокола межсетевого взаимодействия должны быть идентифицированы их уникальными IP-адресами. Сетевой уровень должен обеспечивать двум головным станциям доступ к информации о станции непосредственно или косвенно в сети через шлюзы межсетевого взаимодействия.

Транспортный уровень должен обеспечивать обмен данными между двумя головными станциями, связанными непосредственно или через одну или несколько сетей.

Данный уровень должен обеспечиваться применением протокола управления передачей TCP в соответствии с IETF [9] или протокола передачи дейтаграмм пользователя UDP в соответствии IETF [15].

Перечень интерфейсов между компонентами оборудования и общие характеристики этих интерфейсов должны соответствовать данным, приведенным в таблице Б.1 (приложение Б).

4.3.4 Для обмена данными между компонентами оборудования должны использоваться протоколы TCP и UDP.

4.3.5 Параметры сообщений протоколов TCP должны соответствовать данным таблицы Б.2 (приложение Б).

4.3.6 Параметры первого и второго уровней приоритета транспортного потока на выходе передающей и приемной частей оборудования СОД в соответствии с ISO/IEC [2], ETR [16] должны соответствовать нормам, приведенным в приложении В.

5 Технические требования

5.1 Общие технические требования

5.1.1 Оборудование СОД и компоненты, входящие в него, должны изготавливаться в соответствии с требованиями настоящего стандарта.

5.1.2 Соединение компонент, входящих в состав оборудования СОД, должно выполняться симметричным кабелем или коаксиальным кабелем 50 Ом в соответствии с нормами, указанными в таблицах Д.1, Д.4 (приложение Д).

5.1.3 Должны обеспечиваться возможности перепрограммирования оборудования СОД и компонент, входящих в него, и восстановления программного обеспечения, установленного на заводе-изготовителе.

5.2 Требования к интерфейсам

5.2.1 Входными сигналами для оборудования СОД являются:

- транспортные потоки (интерфейсы типа ASI или SPI);
- сообщения, управляющие правом доступа (ECM) (интерфейсы доступа к сети передачи данных с использованием контроля несущей и обнаружением коллизий (Ethernet, Fast Ethernet));
- сигналы системы управления абонентами (интерфейсы доступа к сети передачи данных с использованием контроля несущей и обнаружением коллизий (Ethernet, Fast Ethernet), допускаются интерфейсы типа RS-232, RS-422;
- сигналы с сообщениями EMM от абонентов (передаются по телефонным линиям или по обратным каналам кабельного телевидения) (интерфейсы доступа к сети передачи данных с использованием контроля несущей и обнаружением коллизий (Ethernet, Fast Ethernet), допускаются интерфейсы типа RS-232, RS-422);
- сигналы системы администрирования (управления) абонентами (SMS) (интерфейсы доступа к сети передачи данных с использованием контроля несущей и обнаружением коллизий (Ethernet, Fast Ethernet), допускаются интерфейсы типа RS-232, RS-422).

5.2.2 Выходными сигналами для оборудования СОД являются:

- скремблированный транспортный поток, содержащий сигналы сообщений ECM и EMM (интерфейсы типа ASI или SPI);
- сигналы с сообщениями EMM от абонентов (передаются по телефонным линиям или по обратным каналам кабельного телевидения);
- сигналы системы администрирования (управления) абонентами (SMS) (интерфейсы доступа к сети передачи данных с использованием контроля несущей и обнаружением коллизий (Ethernet, Fast Ethernet, Gigabit Ethernet), допускаются интерфейсы типа RS-232, RS-422).

5.2.3 Параметры интерфейсов доступа к сети передачи данных с использованием контроля несущей и обнаружением коллизий должны соответствовать требованиям, изложенным в приложении Д.

5.2.4 Параметры интерфейсов передачи данных RS-232, RS-422, асинхронного последовательного интерфейса ASI и синхронного параллельного интерфейса SPI должны соответствовать требованиям, приведенным в приложении Е.

5.2.5 Описание интерфейсов между компонентами оборудования СОД:

- обмен данными между компонентами оборудования СОД DVB выполняется при использовании протоколов TCP, UDP;
- параметры интерфейсов между компонентами оборудования СОД должны соответствовать требованиям, приведенным в приложении Б.

5.3 Требования электромагнитной совместимости

Требования к параметрам электромагнитной совместимости оборудования СОД приведены в таблицах 1—3.

5.3.1 Допустимые уровни напряжения радиопомех, создаваемых оборудованием СОД на сетевых зажимах в полосе частот от 0,15 до 30 МГц, должны соответствовать требованиям, приведенным в таблице 1.

Таблица 1 — Допустимые уровни напряжения радиопомех, создаваемых оборудованием СОД на сетевых зажимах в полосе частот от 0,15 до 30 МГц

Полоса частот, МГц	Напряжение, U_c, дБмкВ, не более	
	Квазипиковое значение	Среднее значение
От 0,15 до 0,5	66—56	56—46
От 0,5 до 5	56	46
От 5 до 30	60	50

Примечания:

1 На граничной частоте нормой является меньше значение.

2 В полосе частот от 0,15 до 0,5 МГц норму напряжения радиопомех вычисляют по формулам:

- для квазипиковых значений:

$$U_c = 66 - 19{,}1 \cdot \lg\frac{f}{0{,}15};$$

- для средних значений:

$$U_c = 56 - 19{,}1 \cdot \lg\frac{f}{0{,}15},$$

где f — частота измерений, МГц.

5.3.2 Допустимые уровни напряжения радиопомех, создаваемых оборудованием СОД на входных зажимах, должны соответствовать требованиям, приведенным в таблице 2.

Таблица 2 — Допустимые уровни напряжения радиопомех, создаваемых оборудованием СОД на входных зажимах

Полоса частот, МГц	Частота гетеродина	Квазипиковое значение напряжения, $U_{вх}$, дБмкВ, не более
От 30 до 1750	Основная	46
От 30 до 1750	Гармоники	46

Примечание — Норму $U_{вх\,z}$ напряжения радиопомех для оборудования с номинальным входным сопротивлением, отличным от 75 Ом, вычисляют по формуле:

$$U_{вхz} = U_{вх} + 10 \cdot \lg\frac{z}{75},$$

где z — номинальное входное сопротивление оборудования, Ом.

5.3.3 Допустимые величины мощности радиопомех, создаваемых оборудованием СОД в сетевых проводах и соединительных кабелях, должны соответствовать требованиям, приведенным в таблице 3.

Таблица 3 — Допустимые величины мощности радиопомех, создаваемых оборудованием СОД в сетевых проводах и соединительных кабелях

Полоса частот, МГц	Мощность, P_c, дБпВт, не более	
	Квазипиковое значение	Среднее значение
От 30 до 300	45—55	35—45
От 300 до 1000	55	—

Примечание — В полосе частот от 30 до 300 МГц норму мощности радиопомех вычисляют по формулам:

- для квазипиковых значений:

$$P_c = 43{,}9 + \lg\frac{f}{27};$$

- для средних значений:

$$P_c = 33{,}9 + \lg\frac{f}{75},$$

где f — частота измерений, МГц.

5.4 Требования безопасности

5.4.1 При эксплуатации, хранении, транспортировании и испытаниях оборудование СОД должно соответствовать требованиям безопасности и санитарии по ГОСТ 12.1.030, ГОСТ Р МЭК 60065, ГОСТ 12.2.007.0.

5.4.2 При использовании оборудования СОД должна быть исключена возможность его воспламенения при случайном замыкании в цепях питания и при неправильном включении полярности электропитания.

5.4.3 Температура наружных поверхностей оборудования СОД во время работы при нормальных климатических условиях не должна превышать +45 °С в местах постоянного контакта оператора с поверхностью, +60 °С — в местах случайного прикосновения к поверхности оборудования.

5.4.4 Конструкция оборудования СОД должна исключать возможность прикосновения персонала к точкам с потенциалом более 35 В (пиковое значение) переменного тока.

5.4.5 Изоляция цепей электропитания оборудования должна выдерживать без пробоя в течение 1 мин действие испытательного напряжения постоянного тока величиной 1410 В, приложенного к элементу заземления оборудования и каждому из потенциальных полюсов ввода электропитания.

5.4.6 Для заземления оборудования СОД должны применяться болт (клемма) с резьбовым соединением, расположенный в безопасном и удобном для подключения заземляющего проводника месте, или заземляющий контакт в разъеме кабеля электропитания.

5.4.7 Сопротивление изоляции между элементом заземления и каждым из потенциальных полюсов ввода электропитания, измеренное в нормальных условиях, должно быть не менее 2 МОм.

5.4.8 Значения сопротивления между болтом (клеммой) заземления и каждой доступной прикосновению металлической нетоковедущей частью оборудования СОД, которая может оказаться под напряжением, не должны превышать 0,1 Ом.

5.4.9 Возле болта (клеммы) заземления (если он предусмотрен конструкторской документацией) должен быть помещен не стираемый при эксплуатации знак заземления по ГОСТ 21130.

5.4.10 Вокруг болта (клеммы) заземления должна быть контактная площадка для присоединения заземляющего проводника. Площадка должна быть защищена от коррозии и не иметь поверхностной окраски.

5.4.11 В оборудовании СОД должно быть обеспечено электрическое соединение всех доступных прикосновению металлических нетоконесущих частей, которые могут оказаться под напряжением, с элементами заземления.

5.5 Требования к электропитанию

5.5.1 Электропитание оборудования СОД должно осуществляться от сети переменного однофазного тока напряжением $220^{+10\%}_{-15\%}$ В с частотой (50 ± 2) Гц.

5.6 Требования по стойкости к климатическим и механическим воздействиям

5.6.1 Оборудование СОД должно сохранять работоспособность при климатических и механических воздействиях, параметры которых приведены в таблице 4.

Таблица 4 — Параметры климатических и механических воздействий

Воздействующий фактор	Величина параметра
1 Температура окружающего воздуха в диапазоне значений, °С	5—40
2 Относительная влажность воздуха, %, при температуре, °С	80 25
3 Атмосферное давление, мм рт. ст.	450—800
4 Воздействие синусоидальной вибрации: - амплитуда ускорения, g; - в диапазоне частот, Гц	 4 5—80

Приложение А
(справочное)

Структура и основные параметры транспортного потока, основные параметры таблиц программно-зависимой информации (PSI) и таблиц информации о службах (SI), дескриптор ограниченного доступа

Настоящее приложение содержит данные в объеме, необходимом для нормирования характеристик программного и транспортного потоков, касающихся вопросов защиты информации от несанкционированного доступа.

А.1 Описание формализованного языка

Элементарные группы данных кодированного транспортного потока описываются именем, длиной в битах и мнемоническим обозначением типа.

Мнемоническое обозначение типа группы данных и его описание показаны в таблице А.1.

Таблица А.1

Мнемоника	Описание типа группы данных
bslbf	Строка битов, левый бит обрабатывается первым. Строки битов написаны в виде цепочек цифр 1 или 0, заключенных в одинарные кавычки. Пробелы в пределах цепочек цифр проставлены для простоты чтения и не имеют другого значения
rpchof	Перечень коэффициентов полинома ненулевых степеней, начиная с коэффициента с самой высокой степенью
tcimsbf	Два целых числа дополнения, сначала старший значащий бит
uimsbf	Целое число без знака, сначала записывается старший значащий бит

Численные значения постоянных величин выражаются в шестнадцатеричном исчислении. Примерами такой записи являются: 0x47, 0xFF, 0xEF.

Фигурные скобки { } обозначают начало и конец блока полей.

В тех случаях, когда имя синтаксической конструкции обозначается сочетанием нескольких слов, эти слова объединяются в непрерывную последовательность символов с использованием символа «_», например **transport_error_indicator.**

Наличие в синтаксисе секции таблиц PSI или SI конструкции «**descriptor()**» означает, что в этом месте должно появиться несколько дескрипторов.

При описании синтаксиса полей используются следующие операторы:

а) + — добавление, накопление;
б) + + — возрастание, приращение;
в) — — понижение, уменьшение;
г) || — логическое «или»;
д) = = — равно;
е) = — оператор назначения;
ж) > — больше чем;
з) < — меньше чем.

А.2 Структура и основные параметры транспортного потока

Структура и основные параметры транспортного потока приведены в объеме, необходимом для описания и нормирования характеристик оборудования систем защиты информации, передаваемой по сетям кабельного и наземного телевизионного вещания, от несанкционированного доступа.

А.2.1 Транспортный поток отдельной программы формируется при мультиплексировании пакетированных элементарных потоков (PES) и служебной информации.

Допускается формирование транспортного потока отдельной программы объединением элементарных потоков ES.

Мультиплексирование PES выполняется транспортным мультиплексором. Транспортные потоки нескольких отдельных программ могут объединяться в системный транспортный поток (мультиплекс).

Структура основных полей пакета PES и размеры этих полей в битах показаны на рисунке А.1.

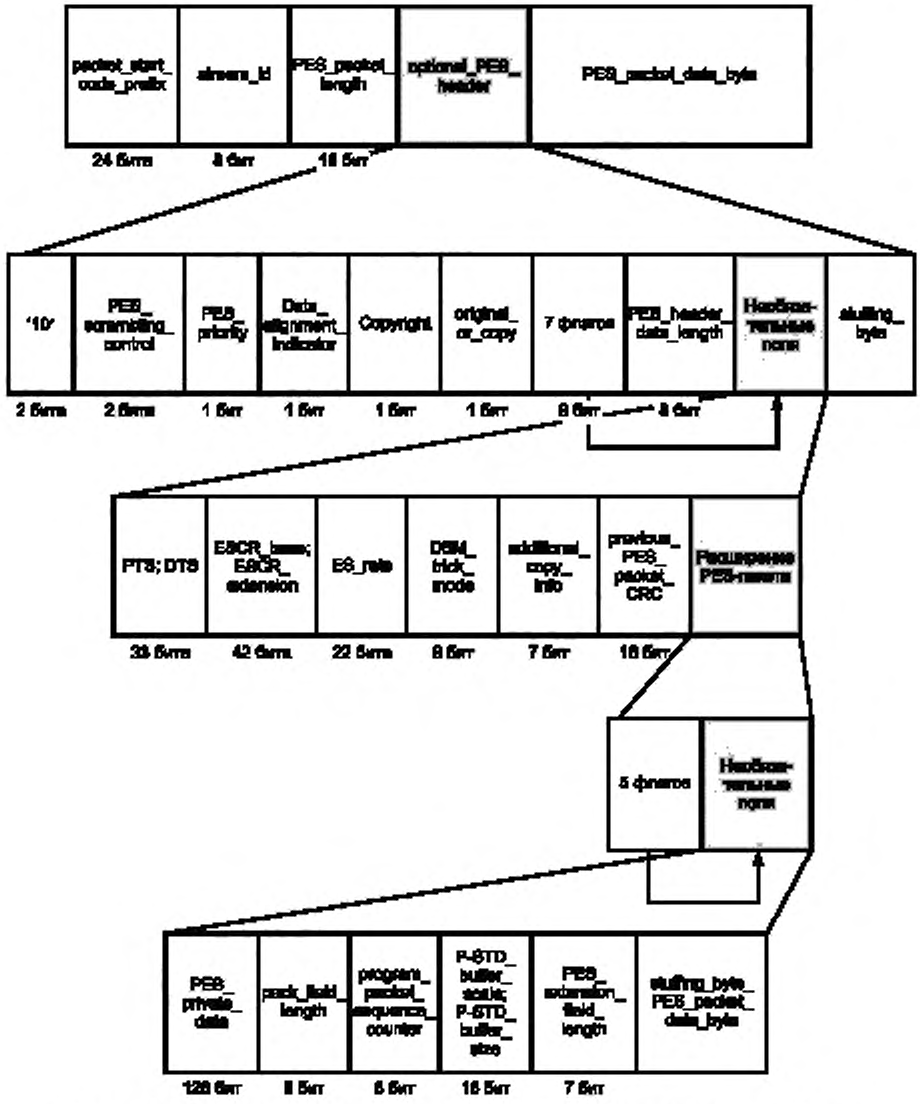


Рисунок А.1 — Структура основных полей пакета PES и размеры этих полей в битах

Пакет PES состоит из заголовка пакета и блока полезной нагрузки.

Синтаксис пакета PES определяется в соответствии с ISO/IEC [2] (подпункт 2.4.3.6, таблицы 2—17).

Ниже приведены определения семантики основных полей заголовка пакета PES и поля полезной нагрузки **PES_packet_data_bytes.**

Заголовок пакета PES включает в себя поля:

- **packet_start_code_prefix:** префикс кода начала пакета — фиксированная кодовая комбинация постоянной длины 24 бита (0x000001);

- **stream_id:** идентификатор потока — в программных потоках определяет тип и номер элементарного потока. Значение идентификатора потока **stream_id** в транспортном потоке в части, касающейся таблиц PSI, должно определяться в соответствии с таблицей А.2.

- **PES_packet_lenght:** поле длиной 16 бит — длина PES пакета в байтах, следующего после этого поля;

- **optional_PES_header:** необязательный заголовок пакета, имеет переменную длину и содержит поля:

- **PES_scrambling_control:** управления скремблированием пакета PES — поле указывает режим скремблирования PES пакета (значения поля, определяющие режимы скремблирования, приведены в таблице А.3).

Таблица А.2 — Значения идентификатора **stream_id**

stream_id	Идентификатор **stream_id**
1011 1100	**program_stream_map** (Примечание 1)
1011 1111	**private_stream_2** (Примечание 2)
1111 0000	**ECM_stream** (Примечание 2)
1111 0001	**EMM_stream** (Примечание 2)
Примечания 1 Синтаксис пакетов PES типа **program_stream_map** определен в соответствии с ISO/IEC [2] (подпункт 2.5.4.1). 2 PES пакеты private_stream_2, ECM_stream и EMM_stream подобны PES пакету private_stream_1. Синтаксис этих пакетов идентичен синтаксису поля PES_packet_length, определяемому в соответствии с ISO/IEC [17], [18].	

Таблица А.3 — Значения поля **PES_scrambling_control**

Значение	Описание
00	Скремблирование отсутствует
01	Определяет пользователь
10	Определяет пользователь
11	Определяет пользователь

- **PES_priority:** приоритет пакета PES — величина 1 означает более высокий приоритет полезной нагрузки в данном PES пакете по сравнению с пакетом PES, у которого величина приоритета полезной нагрузки установлена в 0;

- **data_alignment_indicator:** флаг на 1 бит — определяет необходимость или отсутствие необходимости выравнивания потока данных в зависимости от наличия или отсутствия дескриптора data_stream_alignment_descriptor (ISO/IEC [2] (пункт 2.6.10, таблица 2—46). Типы выравнивания установлены в ISO/IEC [2] (пункт 2.6.10, таблицы 2—47, 2—48);

- **copyright:** поле на 1 бит — величина поля 1 означает, что материал полезной нагрузки пакета PES защищен авторским правом;

- **original_or_copy:** оригинал или копия — поле на 1 бит, если поле установлено в 1, то содержание полезной нагрузки пакета PES является оригиналом; если поле установлено в 0, то содержание полезной нагрузки пакета PES является копией;

- 7 флагов, в том числе:

- **PTS_DTS_flags:** поле длиной 2 бита — величина поля 10 означает, что в заголовке пакета PES должны присутствовать поля метки времени воспроизведения PTS; величина поля 11 означает, что в заголовке пакета PES должны присутствовать и поля метки времени PTS, и поля метки времени декодирования DTS; величина поля 00 означает, что в заголовке пакета PES не должны присутствовать поля метки времени PTS и поля метки времени DTS; величина поля 01 запрещена;

- **ESCR_flag:** поле длиной 1 бит — величина поля 1 означает, что поле ESCR и поля расширения присутствуют в заголовке пакета PES; величина 0 означает, что поле ESCR и поля расширения отсутствуют в заголовке пакета PES;

- **ES_rate_flag:** поле длиной 1 бит — величина поля 1 означает, что поле ES_rate присутствует в заголовке пакета PES; величина 0 означает, что поле ES_rate отсутствует в заголовке пакета PES;

- **DSM_trick_mode_flag:** поле длиной 1 бит — величина поля 1 означает, что в заголовке пакета PES установлен режим **DSM_trick;** величина 0 означает, что в заголовке пакета PES не установлен режим **DSM_trick;**

- **additional_copy_info_flag:** поле длиной 1 бит — величина поля 1 означает, что в заголовке пакета PES присутствует поле additional_copy_info; величина 0 означает, что в заголовке пакета PES отсутствует поле additional_copy_info;

- **PES_CRC_flag:** поле длиной 1 бит — величина поля 1 означает, что в пакете PES присутствует поле проверки циклическим избыточным кодом (CRC); величина 0 означает, что в пакете PES отсутствует поле CRC;

- **PES_extension_flag:** поле длиной 1 бит — величина поля 1 означает, что в пакете PES присутствует поле расширения пакета; величина поля 0 означает, что в заголовке пакета PES отсутствует поле расширения пакета;

- **PES_header_data_length:** размер поля 8 бит — поле характеризует длину данных заголовка пакета PES и определяет число байтов необязательных полей и байтов стаффинга, содержащихся в заголовке пакета PES;

- необязательные поля, которые включают в себя:

- **PTS (presentation time stamp):** поле длиной 33 бита — характеризует метку воспроизведения;

- **DTS (decoding time stamp):** поле длиной 33 бита — характеризует метку декодирования;

- **ESCR_base; ESCR_extension:** поля содержат сигналы синхронизации;

- **ES_rate (elementary stream rate):** поле длиной 22 бита — характеризует скорость, с которой целевой системный декодер получает байты пакета PES до появления нового поля **ES_rate.** Единица скорости пакета PES равна 50 байт/с;

- **DSM_trick_mode:** поле длиной 8 бит — характеризует режим обработки видеопотока;

- **additional_copy_info:** поле длиной 7 бит — содержит частные данные об авторском праве на передаваемый контент;

- **previous_PES_packet_CRC:** поле длиной 16 бит — содержит результаты проверки предыдущего пакета PES на наличие ошибок при использовании кода CRC-16 с порождающим полиномом вида $x^{16} + x^{12} + x^5 + 1$;

- **PES extension (расширение пакета PES):** поле включает в себя:

- пять флагов, в том числе:

- **PES_private_data_flag:** поле (флаг) длиной 1 бит, которое имеет значение 1, если заголовок пакета PES содержит частные данные, и 0, если частные данные отсутствуют;

- **program_packet_sequence_counter_flag:** поле (флаг) длиной 1 бит, которое имеет значение 1, если заголовок пакета PES содержит поля **program_packet_sequence_counter, MPEG1_MPEG2_identifier** и **original_stuff_length,** и 0, если перечисленные поля в заголовке пакета PES отсутствуют;

- **P-STD_buffer_flag:** поле (флаг) длиной 1 бит, которое имеет значение 1, если заголовок пакета PES содержит поля **P-STD_buffer_scale** и **P-STD_buffer_size**, и 0, если перечисленные поля отсутствуют в заголовке пакета PES;

- **PES_extension_flag_2:** поле (флаг) длиной 1 бит, которое имеет значение 1, если заголовок пакета PES содержит поле **PES_extension_field_length** и связанные с ним поля, и значение 0, если перечисленные поля в заголовке пакета PES отсутствуют;

- необязательные поля:

- **PES_private_data:** поле длиной 128 бит — содержит частные данные;

- **pack_field_length:** поле длиной 8 бит — указывает длину в байтах поля **pack_header_field;**

- **program_packet_sequence_counter:** поле длиной 8 бит необязательное, является дополнительным счетчиком непрерывности, записанное в нем число увеличивается с каждым следующим пакетом PES потока в соответствии с ISO/IEC [19] или пакетом PES транспортного потока, обеспечивая функциональные возможности, подобные счетчику непрерывности согласно ISO/IEC [2] (подпункт 2.4.3.2);

- **MPEG1_MPEG2_identifier:** поле (флаг) длиной 1 бит — имеет значение 1, если пакет PES несет информацию потока в соответствии с ISO/IEC 11172-1 [17], и значение 0, если пакет PES несет информацию программного потока;

- **original_stuff_length:** поле длиной 6 бит — определяет число байтов стаффинга, используемых в оригинальных заголовках пакета PES по ISO/IEC [2] или ISO/IEC [19];

- **P-STD_buffer_scale:** поле длиной 1 бит — в соответствии с ISO/IEC [2] (подпункт 2.4.3.7);

- **P-STD_buffer_size:** целое число без знака длиной 13 бит — в соответствии с ISO/IEC [2] (подпункт 2.4.3.7);

- **PES_extension_field_length:** поле длиной 7 бит — определяет длину данных, следующих за этим полем в поле расширения пакета PES, включая любые резервные байты;

- **stuffing_byte:** поле длиной 8 бит — имеет величину 11111111, в необходимых случаях вставляется кодером. Поле **stuffing_byte** игнорируется декодером. Количество байтов стаффинга в заголовке пакета PES не должно превышать 32.

Поле полезной нагрузки **PES_packet_data_bytes** должно содержать непрерывный поток байтов данных полезной нагрузки (элементарного потока), индицированный как **stream_id** или **PID**. Количество байт N поля **PES_packet_data_bytes** определяется в соответствии с выражением:

$$N = M_{\mathbf{PES_packet_length}} - L_{\mathbf{optional_PES_header}},$$

где $M_{\mathbf{PES_packet_length}}$ — количество байтов, указанное в поле **PES_packet_length;**

$L_{\mathbf{optional_PES_header}}$ — количество байтов, занимаемых полями **optional_PES_header.**

В случае передачи в составе поля полезной нагрузки **PES_packet_data_bytes** полей **private_stream_1, private_stream_2, ECM_stream** или **EMM_stream** содержание поля **PES_packet_data_byte** определяется пользователем.

Детализированное описание семантики этих полей и флагов приведено в ISO/IEC [2] (подпункт 2.4.3.7).

А.2.2 Пакеты транспортного потока имеют постоянную длину 188 байтов. Они включают в себя заголовок длиной 4 байта и область полезных данных длиной 184 байта. Структура основных полей транспортного потока MPEG в соответствии с ISO/IEC [2] показана на рисунке А.2.

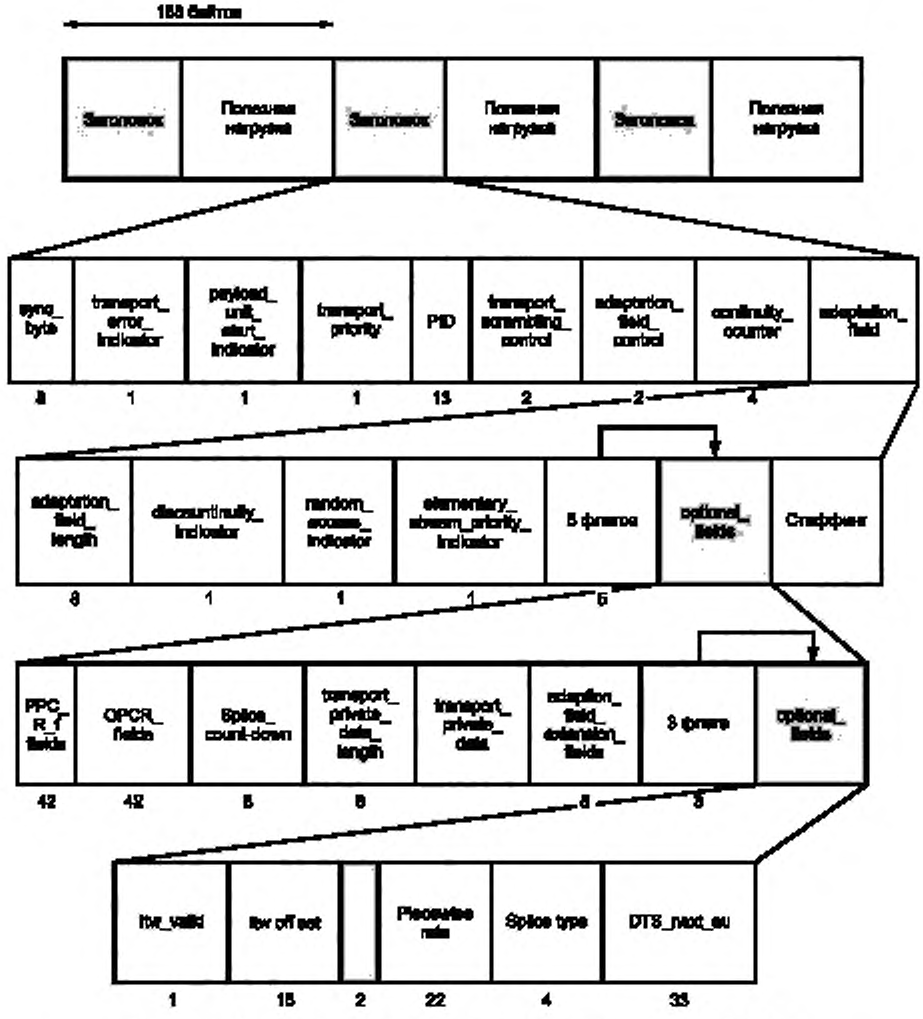


Рисунок А.2 — Структура основных полей транспортного потока MPEG

А.2.2.1 Синтаксис пакетов транспортного потока представлен в таблице А.4.

Таблица А.4 — Синтаксис пакетов транспортного потока

Синтаксис	Количество бит	Мнемоника
transport_packet(){		
sync_byte	**8**	**bslbf**
transport_error_indicator	**1**	**bslbf**
payload_unit_start_indicator	**1**	**bslbf**
transport_priority	**1**	**bslbf**
PID	**13**	**uimsbf**
transport_scrambling_control	**2**	**bslbf**
adaptation_field_control	**2**	**bslbf**
continuity_counter	**4**	**uimsbf**
if(adaptation_field_control = = '10' || adaptation_field_control = = '11'){		
adaptation_field() }		

Окончание таблицы А.4

Синтаксис	Количество бит	Мнемоника

if(adaptation_field_control = = '01' || adaptation_field_control = = '11')
{
for (i = 0; i < N; i++){
data_byte
}
}
}
	8	**bslbf**

А.2.2.2 Определения семантики основных полей транспортного потока:

- **sync_byte:** байт синхронизации, в поле должно быть записано кодовое число 0x47;
- три флага заголовка пакета несут информацию:
- **transport_error_indicator:** поле (флаг) длиной 1 бит об ошибках передачи — имеет значение 1, если в пакете транспортного потока имеется хотя бы одна ошибка в битах;
- **payload_unit_start_indicator:** поле (флаг) длиной 1 бит — является индикатором содержания блока полезной нагрузки:
- в случае передачи в полезной нагрузке транспортного потока пакетов PES:
- величина флага 1 означает, что полезная нагрузка этого пакета транспортного потока начнется с первым байтом пакета PES;
- величина флага 0 означает, что в этом пакете транспортного потока не будет начала пакета PES;
- в случае передачи в полезной нагрузке транспортного потока сервисной информации SI:
- величина флага 1 означает, что пакет транспортного потока содержит первый байт секции SI и что первый байт полезной нагрузки этого пакета содержит поле указателя **pointer_field;**
- величина флага 0 означает, что пакет транспортного потока не содержит первый байт секции SI и что первый байт полезной нагрузки этого пакета не содержит поле указателя **pointer_field;**
- **transport_priority:** поле (флаг) длиной 1 бит — имеет значение 1, если связанный с ним пакет имеет больший приоритет, чем пакеты с тем же самым PID, но с флагом **transport_priority,** не установленным в 1;
- **PID:** поле длиной 13 бит, идентификатор пакета — сообщает о типе данных программно-зависимой информации PSI, передаваемых в полезной нагрузке пакета. Значения идентификатора **PID** приведены в таблице А.5.

Таблица А.5 — Значения идентификатора **PID**

Численное значение	Описание значений идентификатора **PID**
0x0000 (Примечание 1)	Таблица взаимосвязи программ PAT
0x0001 (Примечание 1)	Таблица ограниченного доступа CAT
0x0002	Таблица описания транспортного потока в соответствии с ISO/IEC [2] (пункт 2.4.4). Не обязательна для применения.
0x0003 — 0x000F	Зарезервировано
0x0010—0x1FFE (Примечание 1)	Может быть присвоено: сетевому идентификатору **network_PID;** идентификатору структуры программы **program_map_PID;** идентификатору элементарного потока **elementari_PID**
0x1FFF	Присваиваются пустым (нулевым) пакетам
Примечание — Транспортные пакеты со значениями PID 0x0000, 0x0001, 0x0010 — 0x1FFE допускается использовать для переноса меток PCR.	

- **transport_scrambling_control:** поле длиной 2 бита — является указателем режима скремблирования полезной нагрузки. Заголовок пакета транспортного потока и поле адаптации (при его наличии) не должны быть скремблированы. Значения поля приведены в таблице А.6. В случае передачи пустого пакета значение поля **transport_scrambling_control** должно быть установлено в 00;
- **adaptation_field_control:** поле длиной 2 бита — является указателем наличия или отсутствия полей адаптации и/или нагрузки пользователя в полезной нагрузке пакета. Значения поля **adaptation_field_control** показаны в таблице А.7.

Таблица А.6 — Значения поля **transport_scrambling_control**

Значение	Описание
00	Скремблирование отсутствует
01	Определяет пользователь
10	Определяет пользователь
11	Определяет пользователь

Таблица А.7 — Значения поля **adaptation_field_control**

Значение	Описание
00	Зарезервировано для применения в будущем
01	Поле **adaptation_field** отсутствует. Передается только полезная нагрузка
10	Передается только поле **adaptation_field.** Полезная нагрузка не передается
11	Передается поле **adaptation_field**. Передается полезная нагрузка

- **continuity_counter:** поле длиной 4 бита — является счетчиком непрерывности пакетов, при приеме каждого следующего пакета с данным PID счетчик увеличивает свое значение на единицу и после 15-го пакета сбрасывается в состояние «0»; значение поля **continuity_counter** не должно изменяться, когда значение поля адаптации **adaptation_field_control** установлено в 00 или 10;

- **data_byte:** поле **data_byte** может содержать смежные байты пакетов PES (подпункт 2.4.3.6 ISO/IEC 13818-1, байты секций PSI (подпункт 2.4.4, ISO/IEC 13818-1), байты стаффинга пакета после секций PSI или частные данные, не маркированные идентификатором PID.

Количество N_{data_byte} байтов поля **data_byte** определяется в соответствии с выражением:

$$N = 184 - M_{adaptation_field},$$

где $M_{adaptation_field}$ — количество байтов в поле адаптации **adaptation_field;**

- **adaptation_field:** поле адаптации включает в себя следующие поля:
- **adaptation_field_length:** указатель длины поля, 8 бит;
- **discauntinuity_indicator:** указатель непрерывности счета времени во временных метках, 1 бит; значение «1» указывает на изменение базы отсчета времени;
- **random_access_indicator:** указатель случайного доступа, 1 бит;
- **elementary_stream_priority_indicator:** указатель приоритета элементарного потока, 1 бит;
- пять флагов;
- **optional_fields** дополнительные поля:
- **PCR_fields:** поля PCR, 42 бита;
- OP**CR_fields:** поля OPCR, 42 бита;
- **Splice_count-down:** указатель числа пакетов до стыка, 8 бит — указывает число пакетов с тем же PID в транспортном потоке, оставшихся до точки бесшовного входа в поток;
- **transport_private_data_lenght:** длина поля данных пользователя, 8 бит;
- **transport_private_data:** поле данных пользователя;
- **adaption_field_extension_fields:** длина расширения поля адаптации (данных), 8 бит;
- три флага.

Оставшуюся часть поля адаптации занимают поля служебных данных: **ltw_valid, ltw off set, Piecewise rate, Splice type, DTS_next_au.** Детализированное описание семантики поля адаптации приведено в ISO/IEC [2] (подпункт 2.4.3.5).

А.3 Основные параметры таблиц программно-зависимой информации (PSI) и таблиц информации о службах (SI)

А.3.1 Данные, необходимые для декодирования транспортного потока, передаются в его составе в виде трех таблиц программно-зависимой информации (информации о программах) PSI: PAT, CAT, PMT. Программно-зависимая информация (PSI) передается в области полезных данных транспортного потока.

В дополнение к таблицам PSI, в соответствии с EN [1], в транспортном потоке передаются обязательные таблицы информации о службах SI: NIT, SDT, EIT, TDT, а также необязательные таблицы информации о службах: BAT, TOT, RST.

А.3.2 Все таблицы PSI и SI передаются в отдельных пакетах. Предварительно таблицы сегментируются в секции. Длина секции должна быть не более 1024 байтов. Секция таблицы EIT равна 4096 байтов. Если пакет не заполняется секцией полностью, то незаполненная часть пакета должна заполняться байтами стаффинга 0xFF.

А.3.3 Каждая таблица идентифицируется сочетанием полей, приведенным в таблице А.8.

Таблица А.8 — Идентификаторы таблиц

Идентификатор	Назначение идентификатора
table_id	Определяет содержание секции PSI транспортного потока. Значения идентификатора **table_id** секции PSI представлены в таблице А.9
table_id_extension	Применяется для идентификации субтаблиц **sub_table**
section_number	Определяет номера субсекции
version_number	Определяет номер версии данных при передаче обновленной информации с теми же идентификаторами, как и в предыдущей **sub_table**, но со следующим значением номера поля **version_number**
current_next_indicator	Определяет секции, которые действуют в настоящее время или вступят в действие в ближайшее время

Таблица А.9 — Значения идентификатора **table_id** секции PSI транспортного потока

Значение	Описание секции
0x00	**program_association_section**
0x01	**conditional_access_section (CA_section)**
0x02	**TS_program_map_section**
0x03	**TS_description_section**
0x38—0x3F	Определено ISO/IEC [2]
0x06—0x37	Зарезервировано ISO/IEC [2]
0xFF	Запрещенное значение

А.3.4 PAT — таблица взаимосвязи (ассоциации) программ, содержит данные о всех программах, передаваемых в транспортном потоке в виде идентификаторов PID этих программ. Каждый такой PID определяет местонахождение таблицы состава программы PMT.

Таблица PAT определяет местоположение таблиц сетевой информации NIT.

Структура полей секции таблицы PAT показана на рисунке А.3.

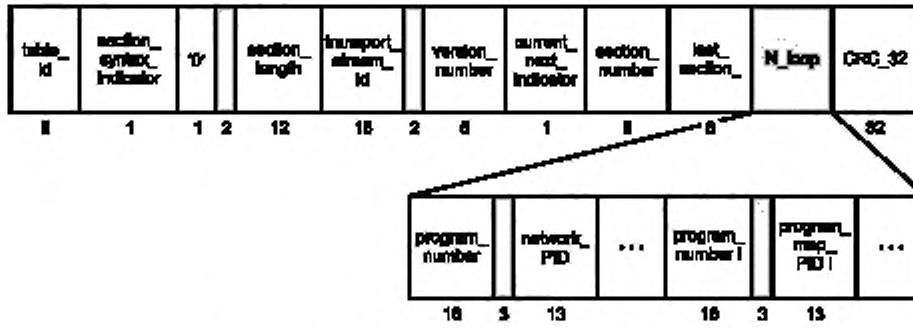


Рисунок А.3 — Структура полей секции таблицы PAT

Секции уникально идентифицированы комбинацией элементов.

В таблице А.10 представлены характеристики полей секции PAT.

Таблица А.10 — Характеристики полей секции PAT

Синтаксис	Количество бит	Мнемоника
program_association_section() {		
table_id	**8**	**uimsbf**
section_syntax_indicator	**1**	**bslbf**
'0'	**1**	**bslbf**
reserved	**2**	**bslbf**
section_length	**12**	**uimsbf**
transport_stream_id	**16**	**uimsbf**
reserved	**2**	**bslbf**
version_number	**5**	**uimsbf**
current_next_indicator	**1**	**bslbf**
section_number	**8**	**uimsbf**
last_section_number	**8**	**uimsbf**
for (i = 0; i < N; i++) {		
program_number	**16**	**uimsbf**
reserved	**3**	**bslbf**
if (program_number = = '0') {		
network_PID	**13**	**uimsbf**
}		
else {		
program_map_PID	**13**	**uimsbf**
}		
}		
CRC_32	**32**	**rpchof**
}		

В таблице А.11 приведены определения семантики полей секции таблицы PAT.

Таблица А.11 — Определения семантики полей секции таблицы PAT

Идентификаторы полей	Назначение, выполняемые функции
1 **table_id**	8 бит: определяет таблицу, к которой принадлежит секция; секции **PAT** соответствует значение 0x00
2 **section_syntax_indicator**	1 бит: секции **PAT** соответствует значение 0x00
3 **section_length**	12 бит: длина секции **PAT**
4 **transport_stream_id**	16 бит: используется как метка для выделения конкретного TS из всех доступных в сети. Значение определяется пользователем
5 **version_number**	5 бит: номер версии таблицы **PAT**; фиксирует каждое изменение содержания таблицы
6 **current_next_indicator**	1 бит: определяет назначение секции — для применения «сейчас» или для применения в будущем («следующая»)
7 **section_number**	8 бит: определяет номер данной секции в таблице **PAT**
8 **last_section_number**	8 бит: содержит номер section_number для последней секции таблицы **PAT**
9 **program_number**	16 бит: определяет программу, к которой применим идентификатор **program_map_PID**
10 **network_PID**	13 бит: поле (используется только в случае, если величина **program_number** равна 0x0000) определяет PID пакетов транспортного потока, которые содержат таблицы NIT. Величина поля **network_PID** определяется пользователем. Величина поля может принимать значения только в соответствии с таблицей А.5
11 **program_map_PID**	13 бит: поле определяет PID пакетов транспортного потока, который должен содержать **program_map_section,** применимый для программы, как определено **program_number**

Окончание таблицы А.11

Идентификаторы полей	Назначение, выполняемые функции
12 **N_loop,** содержит N пар полей данных. В каждой паре полей: - первое поле: **program_number,** - второе поле: **network_PID** или **program_map_PID**	переменная длина 16 байт: содержит номер программы 13 байт: содержит сетевой PID 13 байт: содержит программный PID Сетевой (программный) PID необходим для воспроизведения программы
13 **CRC_32**	32 бита: поле кода циклической проверки, контролирует ошибки во всей секции таблицы PAT при использовании генераторного полинома $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

А.3.5 CAT — таблица ограниченного доступа, содержит PID всех сообщений EMM всех систем ограниченного доступа и информацию о всех системах ограниченного доступа, применяемых в данном мультиплексе. Таблица CAT включает в себя одну или более секций.

Структура полей секции таблицы CAT показана на рисунке А.4.

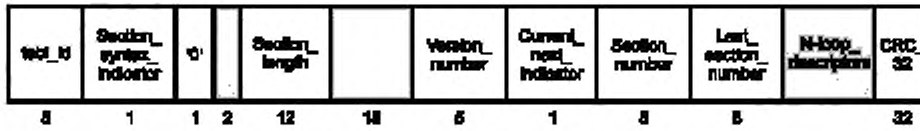


Рисунок А.4 — Структура полей секции таблицы CAT

В таблице А.12 приведены характеристики полей секции CAT.

Таблица А.12 — Характеристики полей секции CAT

Синтаксис	Количество бит	Мнемоника
CA_section (){		
table_id	8	uimsbf
Section_syntax_indicator	1	bslbf
'0'	1	bslbf
reserved	2	bslbf
Section_length	12	uimsbf
reserved	18	bslbf
Version_number	5	uimsbf
Current_next_indicator	1	bslbf
Section_number	8	uimsbf
Last_section_number	8	uimsbf
for(i=0;i<N;i++) {		rpchof
descriptor()		
}		
CRC_32	32	rpchof
}		

В таблице А.13 представлены определения семантики полей секции таблицы CAT.

Таблица А.13 — Определения семантики полей секции таблицы CAT

Идентификаторы полей	Назначение, выполняемые функции
1 **table_id**	8 бит: определяет таблицу, к которой принадлежит секция; секции таблицы CAT соответствует значение 0x01
2 **section_syntax_indicator**	1 бит: секции CAT соответствует значение 0x01
3 **reserved**	2 бита: зарезервировано ISO/IEC [2]

Окончание таблицы А.13

Идентификаторы полей	Назначение, выполняемые функции
4 **section_length**	12 бит: длина секции CAT; определяет число байт секции, начинающейся сразу после поля **section_length** и включающей в себя CRC, первые два бита должны быть «00»; величина этого поля не должна превышать 1021 (0x3FD)
5 **version_number**	1 бит: определяет номер версии таблицы CAT; фиксирует каждое изменение содержания таблицы с возрастанием номера версии на 1. В случае значения поля **current_next_indicator**, равного «1», поле **version_number** должно быть в текущей таблице CAT. В случае значения поля **current_next_indicator**, равного «0», поле **version_number** должно быть в следующей таблице CAT
6 current_next_indicator	1 бит: определяет назначение секции; если поле находится в позиции «1», то таблица CAT должна применяться «сейчас»; если поле находится в позиции «0», то в настоящее время таблица CAT не используется и должна применяться в будущем («следующая»)
7 **section_number**	8 бит: полю присваивается номер секции; номер первой секции **section_number** в таблице CAT всегда должен устанавливаться в 0x00; при добавлении каждой новой секции в таблицу CAT поле секции **section_number** должно возрастать на «1»
8 **last_section_number**	8 бит: поле определяет номер последней секции **section_number**
9 **N-loop descriptors**	Поле переменной длины: в соответствии с ISO/IEC [2]
10 **CRC_32**	32 бита: поле кода циклической проверки; контролирует ошибки во всей секции таблицы CAT при использовании генераторного полинома $x^{32} + x^{26} + x^{23} + x^{22} + + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

А.3.6 PMT — таблица структуры программы, содержит идентификаторы PID всех компонентов конкретной программы. Таблица PMT идентифицирует и индицирует местоположение потоков каждой службы и указывает местоположение меток PCR.

Секции таблицы PMT уникально идентифицированы комбинацией элементов.

Структура полей секции таблицы PMT показана на рисунке А.5.

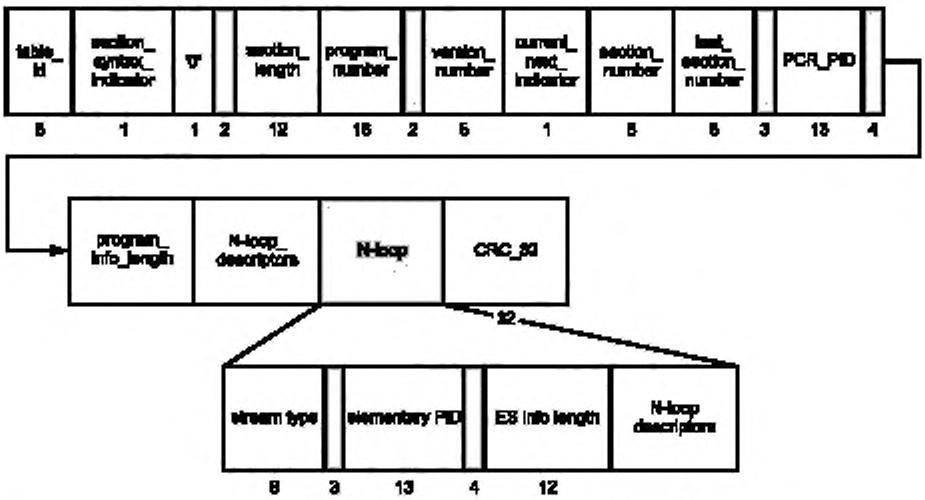


Рисунок А.5 — Структура полей секции таблицы PMT

В таблице А.14 представлены характеристики полей секции PMT.

Таблица А.14 — Характеристики полей секции PMT

Синтаксис	Количество бит	Мнемоника
TS_program_map_section() {		
table_id	**8**	**uimsbf**
section_syntax_indicator	**1**	**bslbf**
'0'	**1**	**bslbf**
reserved	**2**	**bslbf**
section_length	**12**	**uimsbf**
program_number	**16**	**uimsbf**
reserved	**2**	**bslbf**
version_number	**5**	**uimsbf**
current_next_indicator	**1**	**bslbf**
section_number	**8**	**uimsbf**
last_section_number	**8**	**uimsbf**
reserved	**3**	**bslbf**
PCR_PID	**13**	**uimsbf**
reserved	**4**	**bslbf**
program_info_length	**12**	**uimsbf**
for (i = 0; i < N; i++) {		
descriptor()		
}		
for (i = 0; i < N1; i++) {		
stream_type	**8**	**uimsbf**
reserved	**3**	**bslbf**
elementary_PID	**13**	**uimsbf**
reserved	**4**	**bslbf**
ES_info_length	**12**	**uimsbf**
for (i = 0; i < N2; i++) {		
descriptor()		
}		
}		
CRC_32	**32**	**rpchof**
}		

В таблице А.15 представлены семантические определения полей секции таблицы PMT.

Таблица А.15 — Семантические определения полей секции таблицы PMT

Идентификаторы полей	Назначение, выполняемые функции
1 **table_id**	8 бит: определяет таблицу, к которой принадлежит секция; секции PMT соответствует значение 0x02
2 **section_syntax_indicator**	1 бит: секции PMT соответствует значение 0x01
3 **section_length**	12 бит: длина секции PMT; определяет число байт секции, начинающихся сразу после поля section_length и включающей в себя CRC, первые два бита должны быть «00»; величина этого поля не должна превышать 1021 (0x3FD).
4 **program_number**	16 бит: определяет номер программы, к которой применим идентификатор **program_map_PID**
5 **version_number**	5 бит: номер версии таблицы PMT; фиксирует каждое изменение содержания таблицы; определяется аналогично таблице
6 **current_next_indicator**	1 бит: определяет назначение секции — для применения «сейчас» или для применения в будущем («следующая»)
7 **section_number**	8 бит: всегда установлен в 0x00
8 **last_section_number**	8 бит: всегда установлен в 0x00
9 **PCR_PID**	13 бит: определяет PID пакетов ТП, который содержит эталонные метки времени PCR программы, описываемой в поле **program_number**

Окончание таблицы А.15

Идентификаторы полей	Назначение выполняемые функции
10 **program_info_length**	12 бит: первые два бита имеют значение 00; остальные 10 бит определяют число байтов в дескрипторах программы, следующих непосредственно за этим полем
11 **N_loop_descriptors**	Переменная длина: определяет дескрипторы в соответствии с ISO/IEC [2]
12 **stream_type**	8 бит: определяет тип элементарного потока со значением PID в соответствии с ISO/IEC [2] (таблица 2—29)
13 **elementary_PID**	13 бит: определяет идентификатор PID транспортного потока, который несет взаимосвязанный транспортный поток
14 **ES_info_length**	12 бит: первые два бита имеют значение 00; остальные 10 бит определяют количество дескрипторов взаимосвязанного транспортного потока, следующего непосредственно за этим полем
15 **N_loop,** содержит поля данных: stream_type; elementary_PID; ES_info_length	 8 бит: определяет тип элементарного потока или полезной нагрузки; 13 бит: определяет идентификатор PID транспортного потока, который несет взаимосвязанный элементарный поток или полезную нагрузку; 12 бит: определяет число байтов дескриптора взаимосвязанного элементарного потока, следующего непосредственно за полем **ES_info_length**
16 **CRC_32**	32 бита: поле кода циклической проверки, контролирует ошибки во всей секции таблицы PMT при использовании генераторного полинома $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

А.3.7 NIT — таблица сетевой информации, содержит данные:

- об имени сети **(network_id);**
- о параметрах всех передаваемых транспортных потоков, на которые возможна настройка декодера абонентского приемника: о физических параметрах кабельной или наземной сети вещания.

Таблица NIT имеет две версии:

- таблица NIT данной сети: она обязательна для передачи и имеет **network_id** = 0x40;
- таблица NIT других сетей: она не обязательна для передачи и имеет **network_id** = 0x41.

А.3.8 EIT — таблица информации о событиях, содержит сведения о начале и окончании текущего, следующего и будущего событий. Описание событий включает данные: идентификатор события **event_id,** время начала, длительность события, код языка, индикатор скремблирования, название события, краткое описание.

Таблица EIT имеет две версии:

- укороченная версия таблицы EIT: содержит описание только текущего и следующего событий. Она обязательна для передачи и имеет **network_id** = 0x40;
- полная версия таблицы EIT: содержит описание планируемых событий на период от 1 до 7 суток. Она не обязательна для передачи и имеет **network_id** = 0x41.

Таблица EIT в укороченной версии передается в двух секциях. Номер секции текущих событий — 0x00, номер секции следующих событий — 0x01.

Таблица EIT в полной версии передается:

- для данного потока в составе 16 субтаблиц со значениями **table_id** от 0x50 до 0x5F;
- для планируемого потока событий в составе 16 субтаблиц со значениями **table_id** от 0x60 до 0x6F.

Таблица для планируемого потока событий может скремблироваться.

Каждая субтаблица содержит 256 секций (32 сегмента по 8 секций). Длина секции 4096 байт. Каждый сегмент включает информацию о событиях, которые произойдут на интервале отрезка времени, равного 3 ч.

А.3.9 SDT — таблица описания служб, описывает сервисы, передаваемые в транспортном потоке. Таблица SDT имеет две версии:

- о данном транспортном потоке: она обязательна для передачи;
- о других транспортных потоках данной сети или данного букета: она не обязательна для передачи.

А.3.10 TDT — таблица времени и даты, содержит данные о всемирном кодированном времени UTC, которое может использоваться в декодере транспортного потока для обновления текущего времени. Таблица TDT обязательна для передачи.

А.3.11 Таблицы BAT, TOT, RST, ST не обязательны для передачи.

А.3.12 Детализированная информация о таблицах NIT, EIT, SDT, TDT, BAT, TOT, RST, ST приведена в EN [1] (подраздел 5.2).

А.4 Дескриптор ограниченного доступа

Синтаксис описания данных таблиц PSI и SI для обозначения дескрипторов использует тэги (tags). Независимо от секций и таблиц, в которых находятся дескрипторы, значения тэгов не должны изменяться.

Дескрипторы ограниченного доступа используются для определения видов сообщений управления системой ограниченного доступа EMM и ECM. Дескриптор ОД должен появляться в таблице CAT, если в транспортном потоке передается какая-либо информация управления системой ОД.

Дескрипторы ОД могут использоваться в **TS_program_map_section**, **Program_stream_map,** а также в программе, содержащей элементарный поток, если он был скремблирован.

В том случае, когда дескриптор ОД оказывается в **TS_program_map_section (table_id** = 0x02) таблицы PMT, фрагменты пакетов транспортного потока должны содержать ECM.

В том случае, когда дескриптор ОД оказывается в **CA_section** (**table_id** = 0x01) программного потока, фрагменты пакетов транспортного потока должны содержать EMM.

Параметры дескрипторов ограниченного доступа приведены в таблице А.16.

Таблица А.16 — Дескрипторы ограниченного доступа

Синтаксис	Количество бит	Мнемоника
CA_descriptor (){		
descriptor_tag	**8**	**uimsbf**
descriptor_length	**8**	**uimsbf**
CA_system_ID	**16**	**uimsbf**
reserved	**3**	**bslbf**
CA_PID	**13**	**uimsbf**
for(i = 0; i < N; i++) {		
private_data_byte	**8**	**uimsbf**
}		
}		

Определения семантики дескрипторов ограниченного доступа приведены в таблице А.17.

Таблица А.17 — Определения семантики дескрипторов ограниченного доступа

Идентификаторы полей	Назначение, выполняемые функции
descriptor_tag:	Поле на 8 бит, которое идентифицирует каждый дескриптор в соответствии с ISO/IEC [2] (таблица 2—39)
descriptor_length	Поле на 8 бит, которое определяет число байтов в блоке дескриптора, следующих непосредственно после поля **descriptor_length**
CA_system_ID	Поле на 16 бит, указывает тип системы условного доступа, применимой для любых взаимодействующих с ней потоков ECM и/или EMM
CA_PID	Поле на 13 бит, указывает PID пакетов транспортного потока, которые должны содержать ECM или EMM систем условного доступа, как определено во взаимодействующем поле **CA_system_ID**

Приложение Б
(обязательное)

Параметры интерфейсов между компонентами оборудования системы ограничения доступа Simulcrypt

Б.1 Перечень интерфейсов между компонентами оборудования и общие характеристики этих интерфейсов представлены в таблице Б.1.

Таблица Б.1 — Перечень интерфейсов между компонентами оборудования и общие характеристики этих интерфейсов

Интерфейс	Условия применения
ECMG<=>SCS	1) Используется протокол TCP. 2) Допускается кодирование слова управления CW в протоколе, если CW кодируется в соответствии с ETSI [8] (приложение D)
EMMG<=>MUX	Интерфейс может выполняться в двух вариантах: 1) протокол TCP используется для передачи данных и для управления; 2) протокол UDP используется для передачи данных (совместно с протоколами IP), а протокол TCP используется для управления
C(P)SIG<=>(P)SIG	Используется протокол TCP
(P)SIG<=>MUX	Формирование таблиц PSI/SI генератором PSIG и мультиплексором MUX должно выполняться методом карусели ETSI [8]. Тип интерфейса (P)SIG<=>MUX определяется коммерческим соглашением (между оператором и провайдером) при выборе из двух вариантов: 1) протокол TCP применяется для передачи данных и управления; 2) интерфейс ASI применяется для передачи данных, протокол TCP применяется для управления.
EIS<=>SCS	Применяется протокол TCP

Б.2 Параметры сообщений протоколов TCP, ориентированных на соединение (параметры протоколов обмена данными между компонентами оборудования DVB COD Simulcrypt), приведены ниже.

Б.2.1 Типичные величины сообщений для протокола, ориентированного на соединение, приведены в таблице Б.2.

Таблица Б.2 — Типичные величины сообщений для протокола, ориентированного на соединение

generic_message
{
protocol_version 1 байт
message_type 2 байта
message_length 2 байта
for (i=0; i < n; i++)
{
parameter_type 2 байта parameter_length 2 байта
parameter_value <parameter_length> байта }
}

Примечания 1 Для параметров, имеющих размер более 1 байта, первый байт будет главным. 2 Сообщение protocol_version, размером 8 бит, описывающее версию протокола, должно иметь величину 0x03.

Б.2.2 Типичные параметры сообщений для протокола TCP, ориентированного на соединение, приведены в таблице Б.3.

Таблица Б.3 — Типичные параметры сообщений для протокола, ориентированного на соединение

Тип сообщения	Содержание сообщения
message_type:	Поле 16 бит, определяет тип сообщения. Список величин типов сообщения определен в таблице Б.4.
message_length:	Поле на 16 бит, определяет число байтов в сообщении, которое следует непосредственно после поля **message_length**
parameter_type:	Поле 16 бит, определяет тип следующего параметра. Неизвестные параметры должны игнорироваться объектом приема. Данные, связанные с этим параметром, будут отвергнуты
parameter_length:	Поле на 16 бит, определяет число байтов в сообщении, которое следует за полем **parameter_value**
parameter_value:	Поле переменной длины, определяет фактическую величину параметра. Его семантика определяется величиной, характеризующей тип параметра

Б.2.3 Типичные величины предусмотренных сообщений протокола TCP, ориентированного на соединение, представлены в таблице Б.4.

Таблица Б.4 — Типичные величины предусмотренных сообщений протокола TCP

Тип интерфейса	Величина сообщения	Тип сообщения
Зарезервировано	0x0000	Зарезервировано
ECMG<=>SCS	0x0001 0x0002 0x0003 0x0004 0x0005	**channel_setup** **channel_test** **channel_status** **channel_close** **channel_error**
Зарезервировано	0x0006 to 0x0010	Зарезервировано
EMMG<=>MUX	0x0011 0x0012 0x0013 0x0014 0x0015	**channel_setup** **channel_test** **channel_status** **channel_close** **channel_error**
Зарезервировано	0x0016 to 0x0100	Зарезервировано
ECMG<=>SCS	0x0101 0x0102 0x0103 0x0104 0x0105 0x0106	**stream_setup** **stream_test** **stream_status** **stream_close_request** **stream_close_response** **stream_error**
Зарезервировано	0x107 to 0x110	Зарезервировано
EMMG<=>MUX	0x0111 0x0112 0x0113 0x0114 0x0115 0x0116 0x0117 0x0118	**stream_setup** **stream_test** **stream_status** **stream_close_request** **stream_close_response** **stream_error** **stream_BW_request** **stream_BW_allocation**
Зарезервировано	0x0119 to 0x0200	Зарезервировано
ECMG<=>SCS	0x0201 0x0202	**CW _provision** **ECM_response**
Зарезервировано	0x0203 to 0x0210	Зарезервировано
EMMG<=>MUX	0x0211	**data_provision**

Продолжение таблицы Б.4

Тип интерфейса	Величина сообщения	Тип сообщения
Зарезервировано	0x0212 to 0x0300	Зарезервировано
C(P)SIG<=> (P)SIG	0x0301 0x0302 0x0303 0x0304 0x0305	**channel_setup** **channel_status** **channel_test** **channel_close** **channel_error**
Зарезервировано	0x0306 to 0x0310	Зарезервировано
C(P)SIG<=> (P)SIG	0x0311 0x0312 0x0313 0x0314 0x0315 0x0316 0x0317 0x0318 0x0319 0x031A 0x031B 0x031C 0x031D 0x031E 0x031F 0x0320 0x0321	**stream_setup** **stream_status** **stream_test** **stream_close** **stream_close_request** **stream_close_response** **stream_error** **stream_service_change** **stream_trigger_enable_request** **stream_trigger_enable_response** **trigger** **table_request** **table_response** **descriptor_insert_request** **descriptor_insert_response** **PID_provision_request** **PID_provision_response**
Зарезервировано	0x0322 to 0x0400	Зарезервировано
EIS<=>SCS	0x0401 0x0402 0x0403 0x0404 0x0405 0x0406 0x0408 0x0409 0x040A 0x040B 0x040C 0x040D	**channel_set-up** **channel_test** **channel_status** **channel_close** **channel_error** **channel_reset** **SCG_ provision** **SCG_test** **SCG_status** **SCG_error** **SCG_list_request** **SCG_list_response**
Зарезервировано	0x040E to 0x410	Зарезервировано
(P)SIG<=>MUX	0x0411 0x0412 0x0413 0x0414 0x0415 0x0416 to 0x0420 0x0421 0x0422 0x0423 0x0424 0x0425 0x0426 0x0427 to 0x0430	**channel_set_up** **channel_test** **channel_status** **channel_close** **channel_error** Зарезервировано **stream_setup** **stream_test** **stream_status** **stream_close_request** **stream_close_response** **stream_error** Зарезервировано
(Carousel in the MUX — CiM)	0x0431 0x0432 0x0433 to 0x040	**CiM_stream_section_provision** **CiM_channel_reset** Зарезервировано

Окончание таблицы Б.4

Тип интерфейса	Величина сообщения	Тип сообщения
(Carousel in the (P)SIG — CiP)	0x0441 0x0442 0x0443	**CiP_stream_BW_request** **CiP_stream_BW_allocation** **CiP_stream_data_provision**
Зарезервировано	0x0444 to 0x7FFF	Зарезервировано
Определяется пользователем	0x8000 to 0xFFFF	Определяется пользователем

Приложение В
(обязательное)

Требования к параметрам транспортного потока на входе и выходе оборудования системы ограничения доступа

В.1 Параметры транспортного потока на входе и выходе оборудования СОД должны соответствовать нормам, указанным в таблице В.1.

Таблица В.1 — Параметры транспортного потока на входе и выходе оборудования СОД

Наименование параметра	Величина параметра
Параметры первого уровня приоритета	
1 Обеспечение режима синхронизации	Захват цепи синхронизации. Индикатор невыполнения требования: потеря синхронизации **(TS_sync_loss)**
2 Размер синхробайта	0x47. Индикатор невыполнения требований: потеря синхробайта **(Syn_byte_error)**
3 Параметры PAT: 3.1 Период появления секций с идентификатором **table_id** 0x00, с, не менее; 3.2 Секции с идентификатором **table_id** 0x00, не равным 0x00, не появляются под **PID** 0x0000; 3.3 Поле **Scrambling_control_field** равно 00 для значения **PID** 0x0000	0,5 Отсутствие секций с идентификатором **table_id** 0x00, не равным 0x00, под **PID** 0x0000 Поле **Scrambling_control_field** для значения **PID** 0x0000 равно 00. Индикатор невыполнения требований: ошибка **PAT (PAT_error)**
4 Непрерывность счета пакетов	Пакет не появляется более чем дважды. Отсутствует потеря пакетов. Верный порядок следования пакетов. Индикатор невыполнения требований: ошибка непрерывности счета **(Continuiti_count_error)**
5 Параметры PMT: 5.1 Период появления секций с идентификатором **table_id** 0x02 в каждом идентификаторе **program_map_PID**, указанном в **PAT**, с, не менее 5.2 Поле **scrambling_control_field** для всех пакетов, содержащих информацию о секциях с идентификатором **table_id** 0x02 в каждом **program_map_PID**, указанном в **PAT**, равно 00	0,5 Поле **scrambling_control_field** для всех пакетов, содержащих информацию о секциях с идентификатором **table_id** 0x02 в каждом **program_map_PID**, указанном в **PAT**, равно 00. Индикатор невыполнения требований: ошибка **PMT (PMT_error)**
6 Период появления **PID**, с, не более	5 или не более одного периода, определенного пользователем. Индикатор невыполнения требований: ошибка **PID (PID_error)**
Параметры второго уровня приоритета	
7 Отсутствие ошибок в транспортном потоке	**Transport_error_indicator** — индикатор ошибки в заголовке транспортного потока установлен на «0». Индикатор невыполнения требований: ошибка транспортного потока **(Transport_error)**

Окончание таблицы В.1

Наименование параметра	Величина параметра
8 Отсутствие ошибок при проверке контрольных сумм CRC в таблицах **PAT**, **PMT**, **CAT**, **NIT**, **EIT**, **BAT**, **SDT** или **TOT**	Обеспечивается безошибочная проверка контрольных сумм. Индикатор невыполнения требований: ошибка контрольных сумм **(CRC_error)**
9 Безошибочное повторение меток PCR: интервал времени между двумя последовательными метками PCR не должен превышать интервал времени между двумя последовательными метками PCR транспортного потока на входе оборудования СОД более чем на, мс	5,0
10 Максимальная ошибка точности PCR выбранной программы должна быть не более, нс	± 10
11 При появлении пакетов с ненулевым значением флага **transport_scrambling_control** в таблице CAT должны формироваться секции с флагом **table_id** 0x01	При появлении пакетов с ненулевым значением флага **transport_scrambling_control** в таблице CAT формируются секции с флагом **table_id** 0x01. Индикатор невыполнения требований: ошибка CAT **(CAT_error)**
12 В пакетах с PID 0x0001 должны формироваться данные только в таблицах CAT	В пакетах с PID 0x0001 формируются данные только в таблицах CAT. Индикатор невыполнения требований: ошибка CAT **(CAT_error)**

Приложение Г
(рекомендуемое)

Правила скремблирования транспортного потока. Правила формирования слова управления

Г.1 Правила скремблирования транспортного потока

Г.1.1 Транспортный поток рекомендуется скремблировать при выполнении следующих условий:

- скремблирование транспортных потоков должно выполняться только на одном уровне: или на уровне пакетов PES, или на уровне пакетов TS;
- не должны скремблироваться заголовки пакетов PES или пакетов TS;
- длина заголовка скремблированного пакета PES должна быть не более 184 байт;
- не допускается включать в пакеты TS поля адаптации, содержащие части скремблированных пакетов PES, за исключением тех случаев, когда пакеты TS соответствуют окончанию пакета PES;
- допускается включать в пакеты TS поля адаптации, если пакеты TS соответствуют окончанию пакета PES. Это позволяет использовать пакет TS с окончанием скремблированного пакета PES с полем адаптации для синхронизации конца пакета PES по концу пакета TS;
- все пакеты PES со значениями PID, имеющими значение **CA_PID**, должны содержать информацию только о системе ограниченного доступа;
- две разные системы ограниченного доступа не должны использовать в одном транспортном потоке одинаковые значения **CA_PID**.

Информация о скремблировании должна передаваться двумя однобитовыми флагами в заголовках пакетов PES или пакетов TS в соответствии с таблицей А.3.

Г.2 Правила формирования слова управления

Г.2.1 Слово управления, применяющееся для скремблирования транспортного потока, для внешнего наблюдателя должно представлять собой случайную последовательность.

Г.2.2 Правила формирования слова управления должны исключать для внешнего наблюдателя возможность предсказания знака следующего бита при известном алгоритме формирования и известной аппаратурной реализации генератора слова управления.

Г.2.3 Конкретная последовательность слова управления не должна воспроизводиться при повторном запуске генератора слова управления при использовании того же сигнала запроса слова управления.

Г.2.4 Слово управления рекомендуется формировать генератором CW от физического источника шума с гауссовским распределением при амплитудной неравномерности спектра не более ±1 дБ в полосе частот от 0,1 до 120 кГц.

Г.2.5 При формировании слова управления генератором псевдослучайной последовательности проверку выполнения рекомендаций по Г.2.1—Г.2.3 рекомендуется выполнять с использованием следующих критериев:

- объем последовательности слова управления при обработке программой-архиватором не должен уменьшаться более чем на (1—2) %;
- на преобладание «1»/«0» в последовательности слова управления в соответствии с ETSI [8] (приложение С, подпункт С.4.1);
- по виду автокорреляционной функции последовательности слова управления в соответствии с ETSI [8] (приложение С, подпункт С.4.2).

Перечисленные проверки последовательности слова управления рекомендуется выполнять при вводе слова управления в генератор ECM.

Приложение Д
(обязательное)

Требования к параметрам интерфейсов доступа к сети передачи данных с использованием контроля несущей и обнаружением коллизий (Ethernet, Fast Ethernet, Gigabit Ethernet)

Д.1 Кадр Ethernet состоит из полей вспомогательной и служебной информации, а также поля данных. Минимальный размер поля данных — 46 байт, максимальный размер поля данных —1500 байт. Размер полей адреса назначения и адреса источника — 6 байт.

Д.2 Параметры интерфейсов доступа к сети передачи данных с использованием контроля несущей и обнаружением коллизий приведены в таблицах Д.1—Д.6.

Таблица Д.1 — Требования к параметрам электрических интерфейсов Ethernet

Наименование параметра	Величина параметра		
	10 BASE-5	10 BASE-2	10 BASE-T
1 Среда передачи	Коаксиальный кабель 0,5 дюйма (50 Ом)	Коаксиальный кабель 0,25 дюйма (50 Ом)	Незкранированная симметричная пара кабеля категории 3
2 Топология	Шинная	Шинная	Звездообразная
3 Код	Манчестерский	Манчестерский	Манчестерский
4 Линейная скорость передачи данных, Мбит/с	10	10	10
5 Максимальная длина сегмента, м	500	185	100

Таблица Д.2 — Требования к параметрам оптических интерфейсов 10BASE-F

Наименование параметра	Величина параметра	
	10 BASE-FP	10 BASE-FL
1 Топология	Точка-точка	Точка-точка
2 Линейная скорость, Мбит/с	100	100
3 Диапазон центральных длин волн, нм	800—910	800—910
4 Тип волокна	MMF	MMF
5 Код	Манчестерский	Манчестерский
6 Уровень средней мощности на передаче, дБм:		
1) максимальный 2) минимальный	Минус 11 Минус 15	Минус 12 Минус 20
7 Минимальный коэффициент экстинкции, дБ	13	13
8 Уровень средней мощности на приеме, дБм: 1) максимальный 2) минимальный	 Минус 27 Минус 41	 Минус 12,0 Минус 32,5
9 Максимальная протяженность линии, м	2000	2000

Таблица Д.3 — Требования к параметрам оптических интерфейсов 100 BASE-X

Наименование параметра	Величина параметра		
	100 BASE-FX	100 BASE-LX10	100 BASE-BX10
1 Топология	Точка-точка	Точка-точка	Точка-точка
2 Линейная скорость, Мбит/с	125	125	125
3 Диапазон центральных длин волн, нм	770—860	1260—1360	1480—1580 (DS) 1260—1360 (US)
4 Тип волокна	MMF	SMF	SMF

Окончание таблицы Д.3

Наименование параметра	Величина параметра		
	100 BASE-FX	100 BASE-LX10	100 BASE-BX10
5 Код	NRZI, 4B/5B		
6 Уровень средней мощности на передаче, дБм: 1) максимальный 2) минимальный	 Минус 14 Минус 20	 Минус 8 Минус 15	 Минус 8 Минус 14
7 Минимальный коэффициент экстинкции, дБ	10	5	6,6
8 Уровень средней мощности на приеме, дБм: 1) максимальный 2) минимальный	 Минус 14 Минус 31	 Минус 8 Минус 25	 Минус 8 Минус 28,2
9 Максимальная протяженность линии, м	100	10 000	10 000

Таблица Д.4 — Требования к параметрам электрических интерфейсов 100 BASE-T

Наименование параметра	Величина параметра	
	100 BASE-TX	100 BASE-T4
1 Среда передачи	2 симметричные пары (STP или UTP) кабеля категории 5	4 симметричные пары кабеля категории 3
2 Топология	Звездообразная	Звездообразная
3 Код	MLT3, 4B/5B	8B/6T
4 Линейная скорость передачи данных, Мбит/с	125	100
5 Максимальная длина сегмента, м	100	100

Таблица Д.5 — Требования к параметрам оптических интерфейсов 1000 BASE-X

Наименование параметра	Величина параметра		
	1000 BASE-SX	1000 BASE-LX	1000 BASE-ZX
1 Топология	Точка-точка	Точка-точка	Точка-точка
2 Линейная скорость, ГБод	$1,25 \times (1 \pm 100 \times 10^{-6})$	$1,25 \times (1 \pm 100 \times 10^{-6})$	$1,25 \times (1 \pm 100 \times 10^{-6})$
3 Диапазон центральных длин волн, нм	770—860	1270—1355	1520—1580
4 Тип волокна	MMF	SMF	SMF
5 Код	Двоичный NRZ, 8B/10B		
6 Уровень средней мощности на передаче, дБм: 1) максимальный 2) минимальный	 0 Минус 9,5	 Минус 3,0 Минус 11,0	 5,0 Минус 4,0
7 Минимальный коэффициент экстинкции, дБ	9,0	9,0	9,0
8 Уровень средней мощности на приеме, дБм: 1) максимальный 2) минимальный	 0 Минус 17,0	 Минус 3,0 Минус 19,0	 Минус 23,0 Минус 3,0
9 Максимальная протяженность линии, м	550	5000	70 000*
* При протяженности линии свыше 70 км уровень средней мощности на передаче больше 5 дБм.			

Таблица Д.6 — Требования к параметрам электрических интерфейсов GBE

Наименование параметра	Величина параметра	
	1000 BASE-T	1000 BASE-CX
1 Среда передачи	4 симметричные пары кабеля категории 5	2 симметричные пары кабеля категории 5
2 Топология	Точка-точка	Точка-точка
3 Код	4D-PAM5	NRZ, 8B/10B
4 Линейная скорость передачи данных, Мбит/с	1000	1250
5 Максимальная длина сегмента, м	100	25

Приложение Е
(обязательное)

Требования к параметрам интерфейсов передачи данных RS-232, RS-422, асинхронного последовательного интерфейса (ASI) и синхронного параллельного интерфейса (SPI)

Е.1 Требования к параметрам интерфейсов передачи данных RS-232, RS-422 приведены в таблицах Е.1, Е.2.

Таблица Е.1 — Параметры интерфейса RS-232

Наименование параметра	Величина параметра
1 Скорость передачи данных, кбит/с, не более	20*
2 Допустимые значения напряжения логической единицы на входе приемника, В	От минус 12 до минус 3
3 Допустимые значения напряжения логического нуля на входе приемника, В	От 3 до 12
4 Допустимые значения напряжения логической единицы на выходе передатчика, В	От минус 12 до минус 5
5 Допустимые значения напряжения логического нуля на выходе передатчика, В	От 5 до 12
6 Выходное сопротивление передатчиков сигналов данных и синхронизации, Ом, не более	100
7 Допустимые значения входного сопротивления приемников, кОм	От 3 до 7
8 Разность потенциалов между «сигнальными землями» (SG) соединяемых устройств, В, не менее	2
* При использовании современных адаптеров допускается увеличение скорости передачи данных до 115 кбит/с.	

Таблица Е.2 — Параметры интерфейса RS-422

Наименование параметра	Величина параметра
1 Напряжение логической единицы на входе приемника, мВ	200
2 Скорость передачи данных, Мбит/с, не более	10
3 Напряжение логического нуля на входе приемника, мВ	200
4 Допустимые значения напряжений входного сигнала приемника, В	± 7
5 Максимальное входное сопротивление приемника, кОм	4
6 Чувствительность приемника, мВ, не менее	± 200
7 Сопротивление нагрузки передатчика, Ом, не более	100
8 Максимальный ток короткого замыкания передатчика, мА	150
9 Максимальный размах сигнала на выходе передатчика, В	± 5
10 Минимальный размах сигнала на выходе передатчика, В	± 2
11 Максимальное относительное отклонение выходного сопротивления, %	± 5
12 Допустимые значения размаха сигнала на выходе, В	От 3 до 5
13 Максимальный выходной джиттер, нс	20

Е.2 Требования к параметрам асинхронного последовательного интерфейса (ASI) для цифрового компрессированного сигнала изображения приведены в таблице Е.3.

Таблица Е.3 — Параметры асинхронного последовательного интерфейса (ASI) для цифрового компрессированного сигнала изображения

Наименование параметра	Величина параметра
1 Тип	Электрический или оптический

Окончание таблицы Е.3

Наименование параметра	Величина параметра
2 Число байт в пакете	188 или 204
3 Номинальное значение скорости передачи общего цифрового потока, Мбит/с	270
4 Максимальное относительное отклонение скорости передачи	$\pm$ 100 $\times$ 10^{-6}
5 Эффективная скорость передачи (полезных данных), Мбит/с, не менее	213
6 Глазковая диаграмма (дрожание уровней цифрового сигнала), %, не более	80
7 Общий джиттер на выходе, % , от длительности тактового интервала, не более	10
8 Размах сигнала, мВ	800 $\pm$ 80

Е.3 Требования к параметрам синхронного параллельного интерфейса (SPI) для цифрового компрессированного сигнала изображения приведены в таблице Е.4.

Таблица Е.4 — Параметры синхронного параллельного интерфейса (SPI) для цифрового компрессированного сигнала изображения

Наименование параметра	Величина параметра
1 Эффективная скорость передачи (полезных данных), бит/с, не более	108 $\times$ 10^{6}
2 Длительность фронта импульса на выходе, %, от тактового интервала, не более	14
3 Разрядность данных, бит	8
4 Глазковая диаграмма (дрожание уровней цифрового сигнала), %, не более	80
5 Общий джиттер на выходе, % , от длительности тактового интервала, не более	10,8
6 Размах сигнала на выходе, мВ	454—908
7 Постоянная составляющая на выходе, В	1,250 $\pm$ 0,125
8 Постоянная составляющая на входе, В	1,250 $\pm$ 0,5
9 Сопротивление нагрузки, Ом	111 $\pm$ 21

Библиография

[1]	ETSI EN 300 468 V1.8.1 (2007-10)	Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems, Final draft
[2]	ISO/IEC 13818-1:1996	Information technology — Generic coding of moving pictures and associated audio information: Systems
[3]	Recommendations of the European DVB Project — DVB Doc. A011 rev.1, 1996	Digital Video Broadcasting (DVB); DVB Common Scrambling Algorithm (Distribution Agreement)
[4]	DVB document a007 february 1997	Support for use of scrambling and conditional access within digital broadcasting systems
[5]	ETSI TECHNICAL REPORT ETR 289 October 1996	DVB; Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems
[6]	Tech 3292 rev. 2 Technical Specification, August 2002 European Broadcasting Union	Basic Interoperable Scrambling System with Encrypted keys
[7]	ETSI TS 101 197 V1.2.1 (2002-02)	Digital Video Broadcasting (DVB); DVB SimulCrypt; Head-end architecture and synchronization. Technical Specification
[8]	ETSI TS 103 197 V1.3.1 (2003-01)	Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt. Technical Specification
[9]	Техническая комиссия Internet (IETF) RFC 793	«Transmission Control Protocol»
[10]	EUROPEAN STANDARD EN 50221 February 1997	Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications
[11]	ETR 289 Technical Report October 1996	Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems
[12]	Recommendations of the European DVB Project — DVB DOCUMENT A007	Support for use of scrambling and conditional access within digital broadcasting systems. February 1997
[13]	Recommendations of the European DVB Project — DVB Doc. A0061, rev.1, Oct. 95.	Digital Video Broadcasting (DVB). Antipiracy legislation for digital video broadcasting
[14]	IEEE 802.3	Ethernet Working Group. Методы доступа и физическая передача сигналов. Метод доступа CSMA-CD
[15]	IETF RFC 768	«User Datagram Protocol», J. Postel
[16]	ETR 290 Technical Report, May 1997	Digital Video Broadcasting (DVB); Measurement guidelines for DVB systems
[17]	ISO/IEC 13818-2: 1996	Information technology — Generic coding of moving pictures and associated audio information: Video.
[18]	ISO/IEC 13818-3:1998	Information technology — Generic coding of moving pictures and associated audio information — Part 3: Audio
[19]	ISO/IEC 11172-1:1993	Information technology — Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s — Part 1: Systems

УДК 621.397:004.056:006.354 ОКС 33.170

Ключевые слова: телевидение вещательное цифровое, защита информации, доступ, транспортный поток

Редактор переиздания *Е.И. Мосур*
Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 19.05.2020. Подписано в печать 23.07.2020 Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 5,58. Уч.-изд. л. 5,02.
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.
www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru