ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 55695— 2013

ТЕЛЕВИДЕНИЕ ВЕЩАТЕЛЬНОЕ ЦИФРОВОЕ. ОБЕСПЕЧЕНИЕ СКРЕМБЛИРОВАНИЯ И ОГРАНИЧЕНИЯ ДОСТУПА В СИСТЕМАХ ЦИФРОВОГО ТЕЛЕВИЗИОННОГО ВЕЩАНИЯ

Основные параметры

Издание официальное

Москва
Стандартинформ
2019

Предисловие

1 РАЗРАБОТАН Федеральным государственным унитарным предприятием «Ордена Трудового Красного Знамени Научно-исследовательский институт радио» (ФГУП НИИР)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 480 «Связь»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 г. № 1336-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта Recommendation ITU-R BT.1852 (09/2009) «Системы условного доступа для цифрового радиовещания» (Recommendation ITU-R BT.1852 (09/2009) «Conditional-access systems for digital broadcasting», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Декабрь 2018 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 (www.gost.ru)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТЕЛЕВИДЕНИЕ ВЕЩАТЕЛЬНОЕ ЦИФРОВОЕ. ОБЕСПЕЧЕНИЕ СКРЕМБЛИРОВАНИЯ И ОГРАНИЧЕНИЯ ДОСТУПА В СИСТЕМАХ ЦИФРОВОГО ТЕЛЕВИЗИОННОГО ВЕЩАНИЯ

Основные параметры

Digital video broadcasting. Scrambling and access restriction for digital television broadcasting systems. Basic parameters

Дата введения — 2014—09—01

1 Область применения

Настоящий стандарт распространяется на системы ограничения доступа, применяемые на сетях цифрового телевизионного вещания: спутниковых, эфирных и кабельных.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 28147 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

ГОСТ Р 52210 Телевидение вещательное цифровое. Термины и определения

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

ГОСТ Р 53531 Телевидение вещательное цифровое. Требования к защите информации от несанкционированного доступа в сетях кабельного и наземного телевизионного вещания. Основные параметры. Технические требования

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по ГОСТ Р 52210, ГОСТ Р 52591, ГОСТ Р 53531, а также следующие термины с соответствующими определениями.

3.1.1 **абонентское устройство:** Устройство, предназначенное для приема цифровых сигналов телерадиовещания.

3.1.2 **алгоритм криптографического преобразования:** Алгоритм шифрования данных, стандартизованный в соответствии с ГОСТ 28147.

Издание официальное

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

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

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

3.1.6 **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.

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

3.1.8 **имплементация:** Внедрение и/или реализация одного устройства на базе другого.

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

3.1.10 **модуль ограничения доступа:** Устройство, предназначенное для дескремблирования сервисов транспортного потока.

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

3.1.12 **мастер ключ:** Ключ, предназначенный для шифрования слов управления (CW), который хранится в защищенной памяти оборудования передающей и приемной сторон.

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

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

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

3.1.16 **система ограничения доступа:** Система, обеспечивающая скремблирование и дескремблирование транспортного потока.

3.1.17 **система управления сетью** (Network Management System; NMS): Система, обеспечивающая управление и мониторинг оборудования СОД.

3.1.18 **скремблер** (scrambler; SCR): Устройство, предназначенное для скремблирования с целью защиты этого сигнала для исключения несанкционированного обратного преобразования.

3.1.19 **скремблирование** (scrambling): Преобразование структуры цифрового транспортного потока MPEG2 TS, без изменения его скорости, с целью защиты этого сигнала для исключения несанкционированного обратного преобразования.

3.1.20 **слово управления** (Control Word; CW): Объект данных, используемый для скремблирования.

3.1.21 **сообщение разрешения доступа** (EMM): Сообщение, содержащее команды управления дескремблером.

3.1.22 **сообщение управления доступом** (ECM): Сообщение, содержащее слово управления (CW) и вектор начальной загрузки.

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

3.1.24 **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 независимых тактирований от своих источников синхронизации.

3.2 В настоящем стандарте применены следующие сокращения:

CAT (Conditional Access Table) — таблица ограничения доступа;

CI (Common Interface) — единый интерфейс;

C(P)SIG (Custom Program Specific Information Generator) — генератор специальной программно-зависимой информации;

CRC (Cyclic Redundancy Check) — циклический избыточный код;
CW (Control Word) — слово управления;
CWG (Control Word Generator) — генератор слова управления;
CSMA-CD (Carrier Sense Multiple Access with Collision Detection) — множественный доступ с контролем несущей и обнаружением коллизий;
DVB (Digital Video Broadcasting) — цифровое телевизионное вещание;
ECM (Entitlement Control Message) — сообщение управления доступом;
ECMG (Entitlement Control Message Generator) — генератор сообщений ECM;
EMM (Entitlement Management Message) — сообщение разрешения доступа;
EMMG (Entitlement Management Message Generator) — генератор сообщений EMM;
EN (European Standard) — европейский стандарт;
ETR (ETSI Technical Report) — технический отчет ETSI;
ETSI (European Telecommunications Standards Institute) — Европейский институт стандартов электросвязи;
IEC (International Electrotechnical Commission) — Международная электротехническая комиссия;
IEEE (Institute of Electrical and Electronics Engineers) — Институт инженеров по электротехнике и радиоэлектронике;
IETF (Internet Engineering Task Force) — целевая группа по инженерным вопросам Интернета;
ISO (International Standardization Organization) — Международная организация по стандартизации;
MPEG (Moving Picture Experts Group) — Экспертная группа по движущемуся изображению;
MUX (Multiplexer) — мультиплексор;
NMS (Network Management System) — система управления сетью,
PCR (Program Clock Reference) — ссылка на программные часы;
PID (Packet Identifier) — идентификатор пакета;
PMT (Program Map Table) — таблица состава программы;
PSI (Program Specific Information) — программно-зависимая информация;
RFC (Request for Comments) — запрос для комментариев;
SDT (Service Description Table) — таблица описания служб;
SI (Service Information) — информация о службах;
TCP (Transmission Control Protocol) — протокол управления передачей;
TS (Technical Specification) — техническая спецификация;
UDP (User Datagram Protocol) — протокол дейтаграмм пользователя;
АКП — алгоритм криптографического преобразования;
ВНЗ — вектор начальной загрузки;
ГВНЗ — генератор вектора начальной загрузки;
ГСК — генератор сервисного ключа;
МК — мастер ключ;
МОД — модуль ограничения доступа;
ОД — ограничение доступа;
СК — сервисный ключ;
СОД — система ограничения доступа;
ТП — транспортный поток;
ЦТВ — цифровое телевизионное вещание.

4 Основные параметры оборудования систем ограничения доступа к информации, передаваемой по сетям цифрового телевизионного вещания (ЦТВ)

4.1 Определение системы

Система ограничения доступа (СОД) представляет собой совокупность оборудования и программных средств, обеспечивающую ограничение доступа пользователей (абонентов) к контенту и/или сервисам сетей ЦТВ.

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

- скремблирование транспортного потока (ТП) на передающей стороне;
- дескремблирование ТП на приемной стороне.

Скремблирование транспортного потока выполняется в соответствии с алгоритмом криптографического преобразования (АКП) согласно ГОСТ 28147.

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

4.2 Принципы построения систем ограничения доступа

4.2.1 Передающая сторона СОД

Структурная схема передающей части СОД приведена на рисунке 1. На схеме показаны логические взаимосвязи между компонентами. Другие компоненты, относящиеся к оборудованию для формирования цифрового телевизионного транспортного потока на передающей стороне (например, мультиплексор, кодер, модулятор и т.п.), на схеме не показаны.

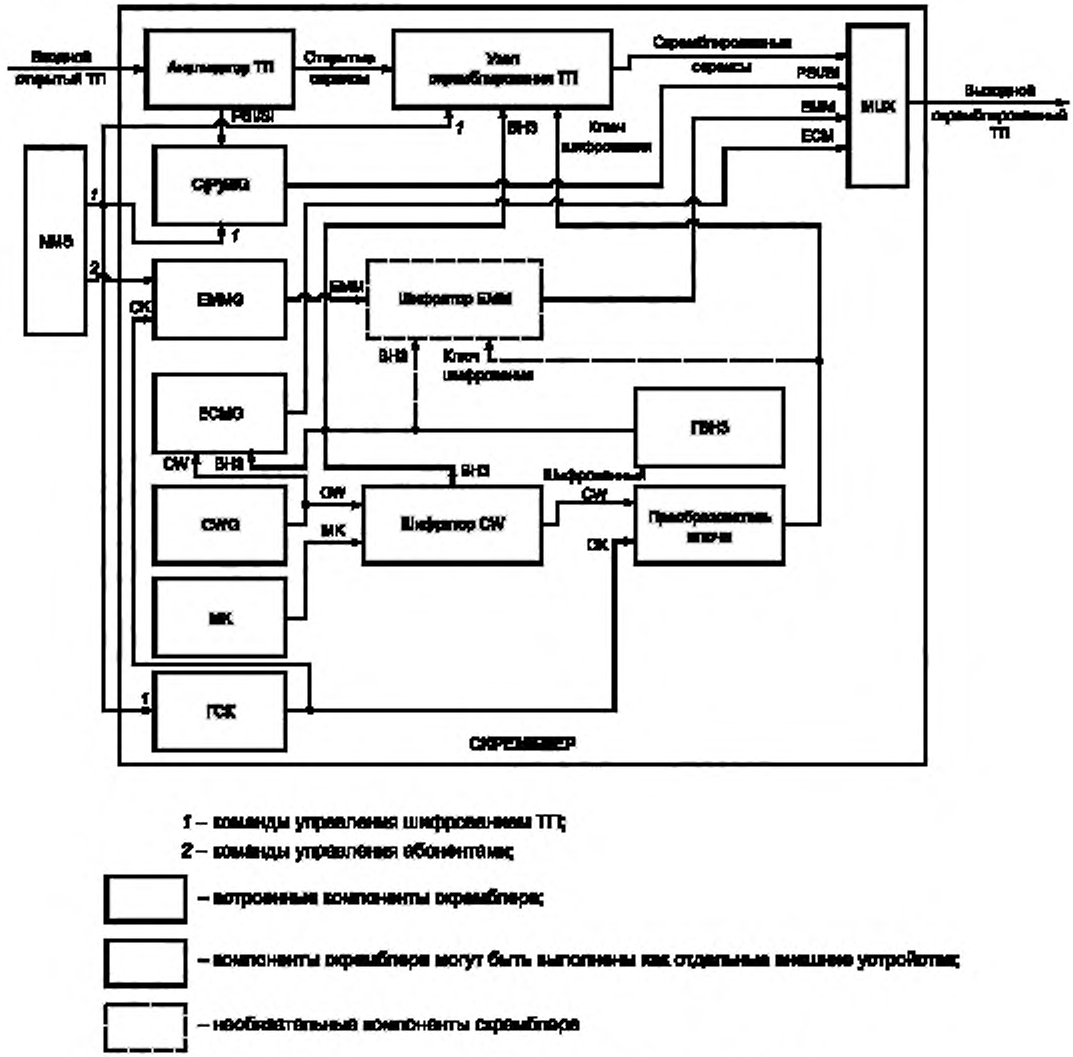

Рисунок 1 — Структурная схема передающей стороны СОД

Передающая часть оборудования СОД

В состав передающего оборудования СОД входят следующие компоненты:

- анализатор ТП — выделяет из входного ТП открытые сервисы и таблицы PSI/SI;
- генератор PSI/SI таблиц (C(P)SIG) — формирует пользовательские MPEG-2 PSI/SI таблицы под управлением NMS;
- генератор сообщений EMM (EMMG) — формирует сообщения EMM под управлением NMS;
- генератор сообщений ECM (ECMG) — формирует сообщения ECM,
- генератор слова управления (CWG) — формирует слово управления;
- мастер ключ (МК) — хранит мастер ключ;
- генератор сервисного ключа (ГСК) — формирует сервисный ключ под управлением NMS;
- узел скремблирования ТП — обеспечивает скремблирования открытых сервисов ТП с использованием ключа шифрования и ВНЗ под управлением NMS;
- шифратор EMM — обеспечивает шифрование таблиц EMM с использованием ключа шифрования и ВНЗ;
- шифратор CW — обеспечивает шифрование слова управления CW с использованием МК и ВНЗ;
- генератор вектора начальной загрузки (ГВНЗ) — формирует вектор начальной загрузки по ГОСТ 28147;
- преобразователь ключа — преобразует шифрованный CW в ключ шифрования при помощи СК;
- мультиплексор MUX — объединяет скремблированные сервисы и таблицы PSI/SI, EMM и ECM в выходной скремблированный поток.

Генераторы таблиц EMM и ECM могут быть выполнены как отдельные внешние устройства.

Основные параметры передающей стороны

Скремблирование ТП и шифрование CW, таблиц EMM выполняется в соответствии с требованиями ГОСТ 28147. При скремблировании ТП по командам управления от NMS в элементарные пакеты ТП (видео, звук) вводится указатель режима скремблирования согласно [1]. Правила скремблирования транспортного потока и формирования слова управления приведены в приложении Б.

Генератор PSI/SI таблиц (C(P)SIG), формирующий пользовательские PSI/SI таблицы под управлением NMS, вводит дескриптор ограничения доступом в таблицы CAT, PMT и устанавливает значение выделенного бита, определяющего факт скремблирования в данном сервисе, в таблицу SDT. Структура дескриптора и таблиц приведена в приложении А.

Управление и мониторинг скремблера выполняются системой управления сетью (NMS).

Выходным сигналом оборудования СОД на передающей станции является скремблированный ТП.

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

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

Интерфейс физического уровня должен быть интерфейсом локальной сети на основе протокола CSMA-CD согласно [2]. Спецификация уровня 10/100 Base-T должна использоваться во всех интерфейсах, определенных в соответствии с настоящим стандартом.

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

Сетевой уровень обеспечивает средства, позволяющие двум СОД на передающих станциях иметь доступ к информации о станции непосредственно или косвенно в сети через передающие станции и шлюзы. Он обеспечивает также СОД возможность межсетевого взаимодействия (протокол маршрутизации в среде Интернет согласно [3]). СОД в пределах протокола межсетевого взаимодействия идентифицированы их уникальными IP-адресами.

Для передачи ТП используется транспортный уровень согласно [4]. Параметры ТП на входе и выходе скремблера должны соответствовать [5].

Для обмена данными между NMS и компонентами оборудования СОД используются два типа протоколов: протокол, ориентированный на соединение (TCP), и протокол передачи дейтаграмм пользователя (UDP) согласно [3], [6].

4.2.2 Приемная сторона СОД

Структурная схема приемной части СОД (модуль ограничения доступа — МОД) приведена на рисунке 2. На схеме показаны логические взаимосвязи между компонентами. Другие компоненты, относящиеся к приемному оборудованию, на схеме не показаны.

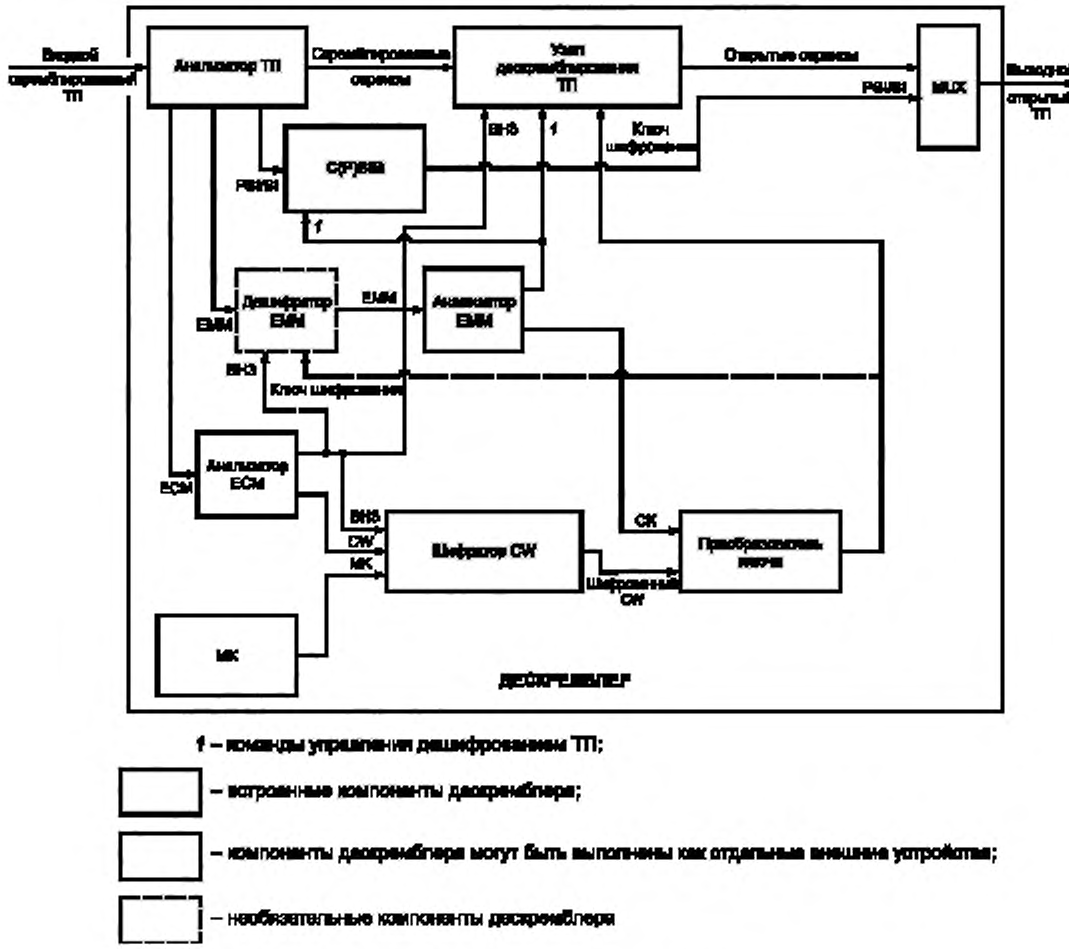

Рисунок 2 — Структурная схема МОД

В состав МОД входят следующие компоненты:

- анализатор ТП — выделяет из входного ТП скремблированные сервисы и шифрованные таблицы PSI/SI, EMM, ECM; обеспечивает сеансовый уровень между МОД и приемным устройством;
- генератор PSI/SI таблиц (C(P)SIG) — формирует пользовательские MPEG-2 PSI/SI таблицы по командам управления;
- анализатор EMM — выделяет из сообщения EMM команды управления и СК;
- анализатор ECM — выделяет из сообщения ECM CW и ВНЗ;
- мастер ключ (МК) — хранит мастер ключ;
- узел дескремблирования ТП — обеспечивает дескремблирование сервисов ТП с использованием ключа шифрования, ВНЗ и команд управления;
- дешифратор EMM — обеспечивает дешифрование таблиц EMM с использованием ключа шифрования и ВНЗ;
- шифратор CW — обеспечивает шифрование слова управления CW с использованием МК и ВНЗ;

- преобразователь ключа — преобразует шифрованный CW в ключ шифрования при помощи СК;
- мультиплексор MUX — объединяет дескремблированные сервисы и дешифрованные таблицы PSI/SI в выходной открытый поток.

Анализатор таблиц ECM и мастер ключ (МК) могут быть выполнены как отдельное внешнее устройство. Взаимодействие между внешними и встроенными компонентами МОД осуществляется согласно [7].

Основные параметры приемной стороны

Шифрование CW, дешифрование таблиц EMM и дескремблирование ТП выполняется в соответствии с требованиями ГОСТ 28147. При дескремблировании ТП по командам управления в элементарных пакетах ТП (видео, звук) снимается указатель режима скремблирования.

Генератор PSI/SI таблиц (C(P)SIG), формирующий пользовательские PSI/SI таблицы по командам управления, снимает дескриптор ограничения доступом в таблицах CAT, PMT и устанавливает значение «0» выделенному биту в таблице SDT.

Взаимодействие между МОД и приемным устройством должно выполняться в соответствии с моделью, включающей в себя следующие уровни:

- транспортный;
- сеансовый.

Для передачи ТП используется транспортный уровень согласно [4]. Параметры ТП на входе и выходе МОД должны соответствовать [5].

В случае взаимодействия МОД с приемным устройством по CI-интерфейсу сеансовый уровень реализуется согласно [8]. В случаях имплементации МОД в приемное устройство протокол реализации сеансового уровня определяется разработчиком.

Приложение А
(справочное)

Основные параметры PSI/SI таблиц, содержащих информацию о системе ограничения доступом, дескриптор ограничения доступа

Настоящее приложение содержит данные о параметрах PSI/SI таблиц, касающихся вопросов защиты информации от несанкционированного доступа.

А.1 Структура транспортного потока

Пакеты транспортного потока имеют постоянную длину 188/204 байта. Они включают в себя заголовок длиной 4 байта и область полезных данных длиной 184 байта. Структура основных полей транспортного потока MPEG-2 соответствует [1].

А.2 Основные параметры PSI/SI таблиц, содержащих информацию о СОД

А.2.1 Данные, необходимые для скремблирования транспортного потока и корректной работы приемного оборудования, передаются в составе трех таблиц: CAT, PMT, SDT.

Таблицы передаются в отдельных пакетах. Предварительно таблицы сегментируются в секции. Длина секции должна быть не более 1024 байта. Если пакет не заполняется секцией полностью, то незаполненная часть пакета должна заполняться байтами стаффинга 0xFF.

А.2.2 CAT — таблица ограничения доступа, содержит информацию о СОД, применяемых в данном ТП, и PID сообщений EMM этих СОД. В таблице А.1 приведена структура секции CAT.

Таблица А.1 — Структура 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 ++) {		
descriptor()		
}		
CRC 32	**32**	**rpchof**
}		

В таблице А.2 представлены определения семантики полей секции таблицы CAT.

Таблица А.2 — Определения семантики полей секции таблицы CAT

Идентификаторы полей	Назначение, выполняемые функции
table_id	8 бит: поле, которому должно быть присвоено значение 0x01 согласно [1] (таблица 2-26)
section_syntax_indicator	1 бит: поле, значение которого должно быть «1»
section_length	12 бит: поле, первые два бита которого должны быть «00». Остальные 10 бит определяют число байт секции, начинающейся сразу после поля **section_length** и включающей в себя CRC, величина этого поля не должна превышать 1021 (0x3FD)
version_number	5 бит: поле, которое определяет номер версии таблицы CAT; описание приведено в [1] (пункт 2.4.4.7)

Окончание таблицы А.2

Идентификаторы полей	Назначение, выполняемые функции
current_next_indicator	1 бит: если значение поля равно «1», то переданная таблица CAT должна применяться в настоящее время; если поле равно «0», то переданная таблица CAT еще не используется, и должна быть следующая таблица CAT, чтобы стать действительной
section_number	8 бит: поле, которое определяет номер секции; значение поля первой секции таблицы CAT должно быть 0x00; значение поля должно увеличиваться на «1» с каждой дополнительной секцией таблицы CAT
last_section_number	8 бит: поле определяет номер последней секции таблицы CAT
N-loop descriptors	Поле переменной длины: в соответствии с [1]
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.2.3 PMT — таблица структуры программы, содержит идентификаторы всех компонентов конкретной программы.

В таблице А.3 представлена структура секции PMT.

Таблица А.3 — Структура секции PMT

Синтаксис	Количество бит	Мнемоника
TS_program_map_section() {		
table_id	**8**	**uimsbf**
sectsection_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 0 = 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.4 представлены определения семантики полей секции таблицы PMT.

Таблица А.4 — Определения семантики полей секции таблицы PMT

Идентификаторы полей	Назначение, выполняемые функции
table_id	8 бит: поле, которому должно быть присвоено значение 0x02 согласно [1] (таблица 2-26)
section_syntax_indicator	1 бит: поле, значение которого должно быть «1»
section_length	12 бит: поле, первые два бита которого должны быть «00». Остальные 10 бит определяют число байт секции, начинающейся сразу после поля **section_length** и включающей в себя CRC, величина этого поля не должна превышать 1021 (0x3FD)
program_number	16 бит: поле, которое определяет программу, к которой идентификатор **program_map_PID** применим; описание приведено в [1] (пункт 2.4.4.9)
version_number	5 бит: определяет номер версии секции PMT; описание приведено в [1] (пункт 2.4.4.9)
current_next_indicator	1 бит: если значение поля равно «1», то переданная секция таблицы PMT должна применяться в настоящее время; если поле равно «0», то переданная секция таблицы PMT еще не используется, и должна быть следующая секция таблицы PMT, чтобы стать действительной
section_number	8 бит: поле, значение которого должно быть 0x00
last_section_number	8 бит: поле, значение которого должно быть 0x00
PCR_PID	13 бит: поле, которое определяет идентификатор пакетов ТП, которые должны содержать действующие поля PCR программы, определяемой дескриптором **program_number**; описание приведено в [1] (пункт 2.4.4.9)
program_info_length	12 бит: поле, первые два бита которого должны быть «00»; остальные 10 бит определяют количество байт дескрипторов, следующих непосредственно за полем **program_info_length**.
N_loop_descriptors	Переменная длина: определяет дескрипторы в соответствии с [1]
stream_type	8 бит: поле, которое определяет тип элемента программы, передаваемого в пакетах с идентификатором, значение которого определяется полем elementary_PID. Значение данного поля определено в таблице 2-29 [1]
elementary_PID	13 бит: поле, которое определяет идентификатор пакетов ТП, которые содержат взаимосвязанный элемент программы
ES_info_length	12 бит: поле, первые два бита которого должны быть «00»; остальные 10 бит определяют количество байт дескрипторов взаимосвязанного элемента программы, следующих непосредственно за полем **ES_info_length**
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.2.4 SDT — таблица описания сервисов. Таблица содержит описание программ, присутствующих в ТП. Программы могут быть частью текущего ТП или других ТП. В таблице А.5 представлена структура секции SDT.

Таблица А.5 — Структура секции SDT

Синтаксис	Количество бит	Мнемоника
Service_description_ section() {		
table id	**8**	**uimsbf**
section_ syntax_ indicator	**1**	**bf bslbf**
reserved_future_use	**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**
original_network_id	**16**	**uimsbf**
reserved_ future_use	**8**	**bslbf**
for (i = 0; i < N; i++){		
service_id	**16**	**uimsbf**
reserved_ future_use	**6**	**bslbf**
EIT_schedule_flag	**1**	**bslbf**
EIT_present_following_flag	**1**	**bslbf**
running_status	**3**	**uimsbf**
free_CA_mode	**1**	**bslbf**
descriptors_loop_length	**12**	**uimsbf**
for (i = 0; i < N; i++){		
descriptor()		
}		
}		
CRC_32	**32**	**rpchof**
}		

В таблице А.6 представлены определения семантики полей секции таблицы SDT.

Таблица А.6 — Определения семантики полей секции таблицы SDT

Идентификаторы полей	Назначение, выполняемые функции
table_id	8 бит: поле, которому должно быть присвоено значение согласно [10] (таблица 2)
section_ syntax_ indicator	1 бит: поле, значение которого должно быть «1»
section_length	12 бит: поле, первые два бита которого должны быть «00». Поле определяет число байт секции, начинающейся сразу после поля **section_length** и включающей в себя CRC, величина этого поля не должна превышать 1021 (0x3FD)
transport_stream_id	16 бит: поле, которое служит в качестве метки для определения, к какому мультиплексированному ТП относится таблица SDT
version_number	5 бит: определяет номер версии поля **sub_table**; описание приведено в [10] (пункт 5.2.3)
current_next_indicator	1 бит: если значение поля равно «1», то переданная секция таблицы SDT должна применяться в настоящее время; если поле равно «0», то переданная секция таблица SDT еще не используется, и должна быть следующая секция таблицы SDT, чтобы стать действительной
section_number	8 бит: поле, которое определяет номер секции; значение поля первой секции таблицы SDT должно быть 0x00; значение поля должно увеличиваться на «1» с каждой дополнительной секцией
last_section_number	8 бит: определяет номер последней секции таблицы SDT

Окончание таблицы А.6

Идентификаторы полей	Назначение, выполняемые функции
original_network_id	16 бит: поле со значением идентификатора сети
service_id	16 бит: поле, которое служит в качестве метки для идентификации данного сервиса
EIT_schedule_flag	1 бит: поле со значением «1» означает в потоке присутствие таблиц EIT с информацией о кратком расписании передач для сервисов ТП, при значении «0» — информация о кратком расписании передач в таблицах EIT отсутствует
EIT_present_following_flag	1 бит: поле со значением «1» означает в потоке присутствие таблиц EIT с информацией о текущем и дальнейшем расписании передач для сервисов ТП, при значении — «0» информация о текущем и дальнейшем расписании передач в таблицах EIT отсутствует
running_status	3 бит: указывает на статус сервиса в соответствии с [10] (таблица 6)
free_CA_mode	1 бит: поле, при значении «0» указывает, что все компоненты потока не скремблированы; если установлено значение «1», это означает, что доступ к одному или более компонентам потока скремблируется с помощью СОД
descriptors_loop_length	12 бит: поле, которое определяет общую длину в байтах последующих дескрипторов
CRC_32	32 бит: поле кода циклической проверки, контролирует ошибки во всей секции таблицы SDT 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 Дескриптор ограничения доступа

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

Если в транспортном потоке содержится какая-либо СОД, в таблице CAT должны присутствовать соответствующие дескриптор ОД и идентификатор таблицы EMM.

Дескриптор ОД должен присутствовать в таблице PMT скремблированных сервисов с указанием идентификатора таблицы ECM. Структура дескриптора ограничения доступа приведена в таблице А.7.

Таблица А.7 — Структура дескриптора ограничения 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 полей дескриптора ограничения доступа приведены в таблице А.8.

Таблица А.8 — Определения семантики полей дескриптора ограничения доступа

Идентификаторы полей	Назначение, выполняемые функции
descriptor_tag:	8 бит: поле, которое идентифицирует каждый дескриптор в соответствии с [1] (таблица 2—39)

Окончание таблицы А.8

Идентификаторы полей	Назначение, выполняемые функции
descriptor_length	8 бит: поле, которое определяет число байт в блоке дескриптора, следующих непосредственно после поля **descriptor_length**
CA_system_ID	16 бит: определяет тип системы условного доступа, применимой для любых взаимодействующих с ней потоков ECM и/или EMM
CA_PID	13 бит: определяет PID пакетов транспортного потока, которые должны содержать ECM или EMM систем условного доступа, как определено во взаимодействующем поле **CA_system_ID**

Приложение Б
(обязательное)

Правила скремблирования транспортного потока и формирования слова управления

Б.1 Правила скремблирования транспортного потока

Б.1.1 Скремблирование транспортного потока может осуществляться либо на уровне PES пакетов, либо на уровне пакетов ТП. Рекомендуется скремблировать на уровне пакетов ТП.

Б.1.2 Не допускается скремблирование заголовков пакетов ТП.

Б.1.3 Не допускается скремблирование поля адаптации ТП.

Информация о скремблировании пакетов ТП и PES пакетов должна передаваться двубитовым флагом в заголовках этих пакетов в соответствии с [9] (пункт 5.1, таблицы 1 и 2).

Б.2 Правила формирования слова управления

Б.2.1 Слово управления, применяющееся в процессе скремблирования транспортного потока, должно представлять собой случайную последовательность.

Б.2.2 Правила формирования слова управления должны исключать возможность предсказания значения следующего байта.

Б.2.3 Конкретная последовательность слова управления не должна воспроизводиться при повторном запуске генератора слова управления.

Б.2.4 Требования к параметрам слова управления:

- 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 [11] (приложение С, пункт С.4.1);
- по виду автокорреляционной функции последовательности слова управления в соответствии с [11] (приложение С, пункт С.4.2).

Библиография

[1]	ISO/IEC 13818 (2000-12)	Information technology — Generic coding of moving pictures and associated audio information: Systems
[2]	IEEE Std 802.3™ (2008)	IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements. Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications
[3]	IETF RFC 793 (1981-09)	Transmission Control Protocol
[4]	ETSI TS 101 154 v.1.9.1 (2009-09)	Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in Broadcasting Applications based on the MPEG-2 Transport Stream
[5]	ETSI ETR 290 (1997-05)	Digital Video Broadcasting (DVB); Measurements guidelines for DVB systems
[6]	IETF RFC 768 (1980-08)	User Datagram Protocol
[7]	ISO/IEC 7816	Identification cards — Integrated circuit cards
[8]	EN 50221 (1997-02)	Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications
[9]	ETSI ETR 289 (1996-10)	Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems
[10]	ETSI EN 300 468 v.1.11.1 (2010-04)	Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems
[11]	ETSI TS 103 197 v.1.5.1 (2008-10)	Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt

УДК 621.397:004.056:006.354 ОКС 33.170 35.040 ОКП 65 7400

Ключевые слова: цифровое телевизионное вещание, скремблирование и ограничение доступа в системах цифрового телевизионного вещания, основные параметры

Редактор *Н.В. Таланова*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 19.12.2018 Подписано в печать 28.01.2019. Формат 60×84 1/8 Гарнитура Ариал
Усл. печ. л. 2,33. Уч.-изд. л. 1,86.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов. 117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru