ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56948— 2016

ТЕЛЕВИДЕНИЕ ВЕЩАТЕЛЬНОЕ ЦИФРОВОЕ

Алгоритмы скремблирования контента служб DVB-IPTV, использующих транспортные потоки MPEG2

Основные параметры

(ETSI TS 103 127 V1.1.1 (2013-05), NEQ)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Автономной некоммерческой организацией «Научно-технический центр информатики» (АНО «НТЦИ»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 480 «Связь»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 7 июня 2016 г. № 541-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений стандарта Европейского института по стандартизации в области телекоммуникаций (ETSI) ЕТСИ ТС 103 127 V1.1.1 (2013-05) «Телевидение вещательное цифровое. Алгоритмы скремблирования контента служб DVB-IPTV, использующих транспортные потоки MPEG2» [ETSI TS 103 127 V1.1.1 (2013-05) «Digital Video Broadcasting (DVB); Content Scrambling Algorithms for DVB-IPTV Services using MPEG2 Transport Streams», NEQ]

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Февраль 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, 2016, 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 1
4 Основные положения 2
5 Аппаратно-ориентированные алгоритмы скремблирования 3
5.1 Введение 3
5.2 Общий алгоритм скремблирования DVB версии 3 3
5.3 Общий алгоритм скремблирования DVB версии 1 4
6 Общий программно-ориентированный алгоритм скремблирования IPTV (CISSA) версии 1 4
6.1 Введение 4
6.2 Общее описание 5
6.3 Нормативные элементы 6
7 Сигнализация 8
7.1 Дескриптор скремблирования 8
7.2 Применение дескриптора скремблирования 8
Приложение А (справочное) Рекомендации по применению CISSA 9
Приложение Б (справочное) Тестовые последовательности CISSA для скремблирования на уровне транспортного потока 10
Библиография 14

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТЕЛЕВИДЕНИЕ ВЕЩАТЕЛЬНОЕ ЦИФРОВОЕ

Алгоритмы скремблирования контента служб DVB-IPTV, использующих транспортные потоки MPEG2

Основные параметры

Digital Video Broadcasting. Content Scrambling Algorithms
for DVB-IPTV Services using MPEG2 Transport Streams. Basic parameters

Дата введения — 2017—06—01

1 Область применения

Настоящий стандарт определяет спецификации скремблирования контента распространяемых в сетях DVB-IPTV услуг реального времени и услуг доставки контента по запросу на базе транспортного потока MPEG2. Также данный стандарт определяет требования к сигнализации, которая позволяет обеспечивать системам условного доступа и системам цифрового управления правами защиту своего контента при использовании методов скремблирования, описанных ниже.

Требования настоящего стандарта следует учитывать при разработке, изготовлении и эксплуатации оборудования DVB-IPTV.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 52210 Телевидение вещательное цифровое. Термины и определения

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

ГОСТ Р 54994 Телевидение вещательное цифровое. Передача служб DVB по сетям с IP протоколами. Общие 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 54994, а также следующие термины с соответствующими определениями:

3.1.1 **алгоритм скремблирования** (scrambling algorithm): Алгоритм на основе шифра, используемый для шифрования аудиовизуального и сопутствующего контента DVB.

Издание официальное

3.1.2 **аппаратно-ориентированный алгоритм скремблирования** (hardware-oriented scrambling algorithm): Алгоритм, который легко реализуется аппаратно на специализированном оборудовании и эта реализация оказывается эффективнее, проще и дешевле, чем его программная реализация на процессорах общего применения.

3.1.3 **общий алгоритм скремблирования версии 1** (Common Scrambling Algorithm version 1; CSA1): Устройство, аппарат или механизм (реализованное как аппаратное или программное средство), разработанное или специально адаптированное, полностью или частично, делающее невозможной для восприятия какую-либо соответствующую текущим стандартам услугу путем применения технологии скремблирования CSA1, а также любых модификаций и модернизаций этой технологии, и эта услуга может быть дескремблирована общей дескремблирующей системой в форме, одобренной Руководящим советом DVB по стандартам.

3.1.4 **общий алгоритм скремблирования версии 3** (Common Scrambling Algorithm version 3; CSA3): Устройство, аппарат или механизм (реализованное как аппаратное или программное средство), разработанное или специально адаптированное, полностью или частично, делающее невозможной для восприятия какую-либо соответствующую текущим стандартам услугу путем применения технологии скремблирования CSA3, а также любых модификаций и модернизаций этой технологии, и эта услуга может быть дескремблирована общей дескремблирующей системой в форме, одобренной Руководящим советом DVB по стандартам.

3.1.5 **программно-ориентированный алгоритм скремблирования** (software-oriented scrambling algorithm): Алгоритм, который легко реализуется как аппаратно на специализированном оборудовании, так и программно на процессорах общего применения, и обе реализации оказываются эффективными.

3.1.6 **шифр** (cipher): Алгоритм, используемый для обеспечения конфиденциальности элементов данных определенного размера.

3.2 В настоящем стандарте применены следующие сокращения:

AES — улучшенный стандарт шифрования (Advanced Encryption Standard);

CBC — сцепление блоков шифра (Cipher Block Chaining);

CISSA — общий программно-ориентированный алгоритм скремблирования IPTV (Common IPTV Software-oriented Scrambling Algorithm);

CSA — общий алгоритм скремблирования (Common Scrambling Algorithm);

CSA3 — общий алгоритм скремблирования версии 3 (Common Scrambling Algorithm version 1);

CSA3 — общий алгоритм скремблирования версии 3 (Common Scrambling Algorithm version 3);

DVB — телевидение вещательное цифровое (Digital Video Broadcasting);

ETSI — Европейский институт по стандартизации в области телекоммуникаций (European Telecommunications Standards Institute);

IPTV — телевещание по протоколу Интернет (Internet Protocol TeleVision);

MPEG — экспертная группа по движущемуся изображению, стандарт сжатия видео- и аудиоданных (Moving Picture Experts Group);

PES — пакетизированный элементарный поток (Packetized Elementary Stream);

TS — транспортный поток (Transport Stream);

uimsbf — целое без знака, старший значащий бит первый (unsigned integer, most significant bit first);

XRC — устойчивый шифр расширенной эмуляции (eXtended emulation Resistant Cipher).

4 Основные положения

Настоящий стандарт определяет два аппаратно-ориентированных алгоритма скремблирования и один программно-ориентированный алгоритм скремблирования, предназначенных для контента IPTV, передаваемого в контейнерах MPEG2-TS. Соответствие оборудования данному стандарту следует считать выполненным, если в нем использован хотя бы один из алгоритмов.

В качестве определений аппаратно-ориентированного и программно-ориентированного алгоритмов скремблирования следует считать следующие положения:

- аппаратно-ориентированный алгоритм скремблирования реализуется исключительно аппаратно на специализированном оборудовании и должен обеспечивать необходимую производительность для всех общих условий применения. Предполагается, что его программные реализации на процессорах общего применения будут иметь недопустимо низкое быстродействие;

- программно-ориентированный алгоритм скремблирования реализуется преимущественно программно, но может иметь и аппаратную реализацию. Он должен обеспечивать необходимую производи-

тельность для всех общих условий применения, независимо от используемых технологий, аппаратного и программного обеспечения. В частности, требование исключительно программной реализации, без использования специализированного оборудования, не должно ограничивать применяемость алгоритма скремблирования. Использование специализированного оборудования не должно быть обязательным, первичной основой должна быть программная реализация.

В приведенных выше определениях аппаратно-ориентированный алгоритм скремблирования должен интерпретироваться как «исключительно аппаратный», в то время как программно-ориентированный алгоритм скремблирования должен интерпретироваться как «программный и аппаратный».

5 Аппаратно-ориентированные алгоритмы скремблирования

5.1 Введение

Настоящий стандарт определяет два алгоритма, для которых метод дескремблирования является аппаратно-ориентированным.

Раздел 5 настоящего стандарта содержит описание элементов дескремблирования, защищенных правами на интеллектуальную собственность с соблюдением условий лицензирования.

Некоторые части элементов дескремблирования из раздела 5 являются конфиденциальными и полное их описание публично недоступно. Детали изложены в 5.2.3, 5.3.3.

В качестве алгоритмов скремблирования в сетях DVB-IPTV следует использовать два алгоритма: - общий алгоритм скремблирования DVB версии 3 (Common Scrambling Algorithm version 3; CSA3), который следует применять в современных условиях;

- общий алгоритм скремблирования DVB версии 1 (Common Scrambling Algorithm version 1; CSA1), который следует применять только для обратной совместимости и поддержки устаревшего оборудования.

5.2 Общий алгоритм скремблирования DVB версии 3

5.2.1 Введение

Алгоритм скремблирования CSA3 состоит из DVB CSA3 дескремблирующей системы и технологии скремблирования. Спецификации для них распространяются отдельно по соглашению с Европейским институтом по стандартизации в области телекоммуникаций (European Telecommunications Standards Institute; ETSI), который действует в интересах компаний, разработавших алгоритм DVB CSA3.

5.2.2 Технические детали

Алгоритм скремблирования CSA3 был разработан для приложений DVB, чтобы минимизировать вред от пиратских атак в течение длительного периода времени, поэтому содержит строго защищаемую информацию. Технические детали этого алгоритма скремблирования могут стать доступными только для надежных пользователей после подписания с ETSI соглашения о неразглашении.

Данный раздел содержит общую информацию о методах скремблирования и некоторые особенности реализации.

Алгоритм скремблирования должен воздействовать на полезную нагрузку пакета транспортного потока (Transport Stream; TS) в случае скремблирования на уровне TS. CSA3 должен использовать 128-битный ключ (контрольное слово) для шифрации и дешифрации блоков данных размером 16 байтов и выше (с дискретностью 1 байт).

Алгоритм шифрования должен быть основан на двух блоках шифров:

- на разновидности «Улучшенного стандарта шифрования» (AES128), описанного в [1], называемого «AES»;

- на «Устойчивом шифре расширенной эмуляции» (XRC), который является конфиденциальным шифром DVB.

Механизм получения ключа CSA3 должен использовать подмножество блочного шифра IDEA-NXT согласно [2].

5.2.3 Лицензирование

Изготовители декодеров и их компонентов, провайдеры услуг, разработчики и иные лица, имеющие отношение к условному доступу, должны иметь лицензию на систему дескремблирования CSA3.

Изготовители скремблеров должны иметь лицензию на технологию скремблирования CSA3 и передавать сублицензию покупателям скремблеров.

Доступ к CSA3 может быть получен надежными пользователями после подписания с ETSI соглашения о неразглашении. Контактная информация ETSI:

Algorithms and Codes service
650 Route de Lucioles
F-06921 Sophia Antipolis Cedex
FRANCE
Tel.: +33 4 92 94 42 16
Fax: +33 4 92 94 42 70

5.2.4 CSA3 для скремблирования DVB IPTV

Для целей скремблирования DVB IPTV алгоритм CSA3 следует применять только в стандартном режиме согласно [3].

5.3 Общий алгоритм скремблирования DVB версии 1

5.3.1 Введение

Алгоритм скремблирования CSA1 состоит из общей дескремблирующей системы и технологии скремблирования. Спецификации для них распространяются отдельно по соглашению с ETSI, который действует в интересах четырех компаний, разработавших общий алгоритм скремблирования.

5.3.2 Технические детали

Алгоритм скремблирования CSA1 был разработан, чтобы минимизировать вред от пиратских атак в течение длительного периода времени (как минимум 10 лет от начала использования), поэтому содержит строго защищаемую информацию. Технические детали этого алгоритма скремблирования могут стать доступными только для надежных пользователей после подписания с ETSI соглашения о неразглашении.

Алгоритм скремблирования должен воздействовать на полезную нагрузку пакета TS в случае скремблирования на уровне TS. В случае скремблирования на уровне пакетизированного элементарного потока (Packetized Elementary Stream; PES) должно применяться структурирование пакетов PES с тем же алгоритмом скремблирования.

CSA1 должен использовать 64-битный ключ (контрольное слово) для шифрации и дешифрации блоков данных размером 8 байтов и выше (с дискретностью 1 байт).

5.3.3 Лицензирование

Изготовители декодеров и их компонентов, провайдеры услуг, разработчики и иные лица, имеющие отношение к условному доступу, должны иметь лицензию на систему дескремблирования CSA1.

Изготовители скремблеров должны иметь лицензию на технологию скремблирования и передавать сублицензию покупателям скремблеров.

Доступ к CSA1 может быть получен надежными пользователями после подписания с ETSI соглашения о неразглашении. Контактная информация ETSI:

Algorithms and Codes service
650 Route de Lucioles
F-06921 Sophia Antipolis Cedex
FRANCE
Tel.: +33 4 92 94 42 16
Fax: +33 4 92 94 42 70

5.3.4 CSA1 для скремблирования DVB IPTV

Учитывая новые современные достижения в технологиях, алгоритм CSA1 не может обеспечить адекватную защиту в течение последующих 10 лет. Поэтому он не рекомендуется для нового оборудования IPTV, за исключением случаев, когда нужно обеспечить обратную совместимость и поддержку устаревшего оборудования.

6 Общий программно-ориентированный алгоритм скремблирования IPTV (CISSA) версии 1

6.1 Введение

Настоящий раздел описывает общий программно-ориентированный алгоритм скремблирования IPTV (Common IPTV Software-oriented Scrambling Algorithm; CISSA) версии 1, который является про-

граммно-дружественным алгоритмом скремблирования и который следует применять для услуг IPTV, передаваемых в транспортных потоках MPEG2. CISSA представляет собой алгоритм, для которого метод дескремблирования является программно-дружественным, т.е. он подходит для эффективной реализации в программном исполнении на процессорах общего применения, а также может быть эффективно реализован в аппаратном исполнении.

В разделе 6 настоящего стандарта приводится общее описание использования CISSA для шифрации/дешифрации транспортного потока MPEG2 и дается детальное формальное описание данного алгоритма.

Рекомендации по применению CISSA даны в приложении А настоящего стандарта.

6.2 Общее описание

Общий программно-ориентированный алгоритм скремблирования IPTV (CISSA) должен использовать шифр AES, описанный в [1], как базовый блок с 128-битными (16-байтовыми) ключами, называемыми контрольными словами.

6.2.1 Скремблирование на уровне TS

Базовой единицей скремблирования (или дескремблирования) должен быть пакет транспортного потока MPEG2. Каждый пакет должен скремблироваться отдельно от остальных, обеспечивая тем самым возможность случайного доступа. Каждый пакет содержит заголовок и опциональное поле адаптации, которые должны оставаться без изменений, и следующую за ними полезную нагрузку, которая должна обрабатываться описанным ниже способом.

Для шифрования блоков данных длиной 16 байтов пакета TS следует применять шифр AES128 [1]. На рисунке 1 приведен скремблированный пакет TS. Только полезная нагрузка пакета TS, кратная 16 байтам, должна шифроваться процессом скремблирования. Оставшаяся часть (до 15 байт) должна оставаться без изменений. Если полезная нагрузка пакета TS менее 16 байтов, то она должна оставаться без изменений.



Рисунок 1 — Скремблированный пакет TS

Целое число 16-байтовых смежных блоков полезной нагрузки должно шифроваться с помощью техники сцепления блоков шифра (Cipher Block Chaining; CBC) согласно [4]. Вектор инициализации должен иметь постоянное значение.

Тестовые последовательности CISSA для скремблирования на уровне транспортного потока даны в приложении Б настоящего стандарта.

6.2.2 Скремблирование на уровне PES

При скремблировании на уровне PES заголовок пакета PES не должен скремблироваться и пакеты TS, содержащие части скремблированного пакета PES, не должны содержать поле адаптации (за исключением, когда пакет TS содержит окончание пакета PES). Заголовок скремблированного пакета PES не должен быть разделен по нескольким пакетам TS. Пакет TS, содержащий начало скремблированного пакета PES, должен быть заполнен заголовком пакета PES и начальной частью полезной нагрузки пакета PES. В этом случае начальная часть полезной нагрузки пакета PES должна скремблироваться точно так же, как пакет TS с полезной нагрузкой такого же размера. Остальная часть полезной нагрузки пакета PES должна быть поделена на суперблоки размером по 184 байта. Каждый такой суперблок должен скремблироваться точно также, как пакет TS с полезной нагрузкой размером 184 байта. Окончание полезной нагрузки пакета PES должно выравниваться по концу пакета TS путем вставки в его начало (после заголовка) поля адаптации подходящего размера. Если длина пакета PES не кратна 184 байтам, оставшаяся часть полезной нагрузки пакета PES (от 1 до 183 байтов) должна скремблироваться точно так же, как пакет TS с полезной нагрузкой такого же размера.

Схематичная диаграмма, показывающая распределение скремблированного пакета PES по пакетам TS, приведена на рисунке 2.



*Присутствуют не всегда.

Рисунок 2 — Скремблированный пакет PES

Для приложений, которые скремблируют секции MPEG2, существует проблема отсутствия в синтаксисе MPEG2 контрольных битов скремблирования. Поэтому скремблирование секций следует выполнять на уровне TS, и это должно быть сигнализировано битами поля управления скремблированием. Секции без изменений и скремблированные секции не должны содержаться в одном пакете TS. Для обеспечения этого требования следует применять определенный в MPEG2 механизм заполнения незначащими данными (padding). Это означает, что конец пакета TS, содержащего секцию, должен быть заполнен байтами со значением 0xFF, для разделения секций без изменений и скремблированных секций по разным пакетам TS.

В контексте DVB CISSA скремблирование на уровне PES обычно применяют в профессиональных приложениях с динамически конфигурируемыми услугами и не применяют в бытовой электронике.

6.3 Нормативные элементы

В данном подразделе приведены нормативные параметры CISSA версии 1.

6.3.1 Элементы шифрования

6.3.1.1 Блочный шифр

В качестве исходного блочного шифра для CISSA следует применять AES128 согласно [1].

6.3.1.2 Вектор инициализации

Вектор инициализации должен содержать следующее значение:

0x445642544d4350544145534349535341

6.3.1.3 Режим сцепления

В качестве режима сцепления следует применять сцепление блоков шифра (CBC) согласно [4].

6.3.2 Скремблирование и дескремблирование пакетов TS

Каждый пакет TS должен быть обработан отдельно.

Заголовок пакета TS и поле адаптации (если используется) должны оставаться без изменений.

Размеры полезной нагрузки *payload_size* и шифрованной полезной нагрузки *encrypted_payload_size* рассчитывают по формулам:

$$payload_size = 188 - (header_size + adaptation_field_size), \quad (1)$$

$$encrypted_payload_size = payload_size - (payload_size \bmod 16), \quad (2)$$

где *header_size* — размер заголовка TS в байтах;
adaptation_field_size — размер поля адаптации в байтах;
операция $x \bmod y$ возвращает остаток от целочисленного деления x на y.

Следующие непосредственно после поля адаптации (или, если поле адаптации отсутствует, после заголовка пакета TS) байты шифрованной полезной нагрузки в количестве *encrypted_payload_size* должны шифроваться или дешифроваться с помощью элементов шифрования согласно 6.3.1.

Все оставшиеся байты должны быть оставлены без изменений.

Пример 1: Если поле адаптации отсутствует, размер шифрованной полезной нагрузки *encrypted_payload_size* равен 176 байтам, то в конце транспортного пакета должно остаться 8 неизмененных байтов.

Пример 2: Если размер поля адаптации равен 17 байтам, размер шифрованной полезной нагрузки *encrypted_payload_size* равен 160 байтам, то в конце транспортного пакета должно остаться 7 неизмененных байтов.

Пример 3: Если размер поля адаптации равен 24 байтам, размер шифрованной полезной нагрузки *encrypted_payload_size* равен 160 байтам, то в конце транспортного пакета не должно быть неизмененных байтов.

Пример 4: Если размер поля адаптации равен 169 байтам, шифрованная полезная нагрузка должна отсутствовать и в конце транспортного пакета должно остаться 15 неизмененных байтов полезной нагрузки.

6.3.3 Скремблирование и дескремблирование на уровне PES

Перед применением скремблирования/дескремблирования на уровне PES следует убедиться в соблюдении следующих условий:

- скремблирование должно выполняться только на одном уровне (TS или PES), одновременное скремблирование на обоих уровнях не допускается;
- заголовок скремблированного пакета PES не должен превышать 184 байтов;
- пакеты TS, содержащие части скремблированного пакета PES не должны содержать поле адаптации, за исключением, когда пакет TS содержит окончание пакета PES. Пакет TS, содержащий окончание скремблированного пакета PES, может содержать поле адаптации для выравнивания окончания пакета PES по окончанию пакета TS.

Примечание — Данные условия неприменимы для нескремблированных пакетов PES или в случае скремблирования на уровне TS.

Каждый пакет PES должен быть обработан отдельно.

Заголовок пакета PES должен оставаться без изменений.

Размеры полезной нагрузки *payload_size* и шифрованной полезной нагрузки *encrypted_payload_size* рассчитывают по формулам:

- для пакета TS, содержащего заголовок пакета PES:

$$payload_size = 184 - pes_header_size, \quad (3)$$

$$encrypted_payload_size = payload_size - (payload_size \bmod 16), \quad (4)$$

где *pes_header_size* — размер заголовка пакета PES в байтах;

- для последующих пакетов TS, за исключением пакета TS, содержащего окончание пакета PES:

$$payload_size = 184, \quad (5)$$

$$encrypted_payload_size = 176, \quad (6)$$

- для пакета TS, содержащего окончание пакета PES:

$$payload_size = pes_tail_size, \quad (7)$$

$$encrypted_payload_size = payload_size - (payload_size \bmod 16), \quad (8)$$

где *pes_tail_size* — размер окончания пакета PES в байтах.

Если значение *pes_tail_size* не равно 184, в начале пакета TS, содержащего окончание пакета PES, должно быть добавлено поле адаптации размером (184 — *pes_tail_size*).

Байты в количестве *encrypted_payload_size*, которые:

- следуют непосредственно за заголовком пакета PES в пакете TS, содержащего заголовок пакета PES;
- следуют непосредственно за заголовками пакетов TS, за исключением пакета TS, содержащего окончание пакета PES;
- следуют непосредственно за заголовком пакета TS или за полем адаптации (если есть) в пакете TS, содержащем окончание пакета PES,

должны быть зашифрованы или дешифрованы с помощью шифрующих элементов согласно 6.3.1.

Все остальные байты должны оставаться без изменений.

7 Сигнализация

7.1 Дескриптор скремблирования

В данном разделе объясняется механизм выбора передачи сигнальной информации, указывающей, какой использован алгоритм скремблирования DVB IPTV.

Дескриптор скремблирования должен информировать о выбранном режиме работы системы скремблирования. Согласно [5] он должен находиться в секции карты программы на уровне цикла информации о программе. Состав дескриптора скремблирования **scrambling_descriptor** приведен в таблице 1.

Таблица 1 — Дескриптор скремблирования

Синтаксис	Число битов	Тип данных
scrambling_descriptor(){		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
scrambling_mode	8	uimsbf
}		

Семантика **scrambling_descriptor**.

scrambling_mode — поле длиной 8 битов, показывающее выбранный режим алгоритма скремблирования согласно таблице 2.

Таблица 2 — Кодировка поля **scrambling_mode**

Значение поля	Описание
0x00	Зарезервировано для будущего использования
0x01	Зарезервировано для других целей [5]
0x02	Используется DVB CSA1
0x03	Используется DVB CSA3 в стандартном режиме
0x04	Зарезервировано для других целей [5]
0x05	Зарезервировано для других целей [5]
0x06 … 0x0F	Зарезервировано для будущего использования
0x10	Используется DVB CISSA версии 1
0x11 … 0x1F	Зарезервировано для будущих версий DVB CISSA
0x20 … 0x6F	Зарезервировано для будущего использования
0x70 … 0x7F	Зарезервировано для других целей [5]
0x80 … 0xFE	Определяется пользователем
0xFF	Зарезервировано для будущего использования

Примечание — Возможные способы применения дескриптора скремблирования описаны в [5] (Приложение E).

7.2 Применение дескриптора скремблирования

В контексте настоящего стандарта должны использоваться только значения 0x02, 0x03 и от 0x10 до 0x1F.

Примечание — Согласно [5] могут применяться иные скремблеры, не указанные в таблице 2 настоящего стандарта, что должно сигнализироваться дескрипторами, определяемыми пользователем (в диапазоне от 0x80 до 0xFE).

Приложение А
(справочное)

Рекомендации по применению CISSA

Программно ориентированный механизм скремблирования, описанный в настоящем стандарте, должен применяться таким образом, чтобы атаки против этого механизма были крайне неуспешны.

В качестве вероятных атак следует рассматривать:

- атаки по внешнему каналу, т.е. направленные на мониторинг параметров, являющихся внешними по отношению к системе, в которой работает алгоритм скремблирования (например, время работы, потребляемая мощность и т.п.). Такое наблюдение может раскрыть секретные данные или секретные временные значения;
- атаки, направленные на мониторинг параметров, являющихся внутренней частью системы, в которой работает алгоритм скремблирования (например, кеш-память). Такое наблюдение может раскрыть секретные данные или секретные временные значения;
- использование ошибок системы (например, искусственно вызванное переполнение буфера может раскрыть некоторые секретные данные);
- модификации кода (для программных реализаций);
- атаки методом внесения неисправностей.

Перечисленный список не является полным, после публикации настоящего стандарта могут появиться иные типы атак.

Приложение Б
(справочное)

Тестовые последовательности CISSA для скремблирования на уровне транспортного потока

В настоящем приложении приведены 4 случая адаптации к CISSA транспортного потока MPEG-2:
- случай 1: без поля адаптации, в соответствии с таблицей Б.1;
- случай 2: поле адаптации длиной 7 байтов, в соответствии с таблицей Б.2;
- случай 3: поле адаптации длиной 8 байтов, в соответствии с таблицей Б.3;
- случай 4: поле адаптации длиной 9 байтов, в соответствии с таблицей Б.4.

Все пакеты TS должны быть скремблированы с использованием следующего контрольного слова:
00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff

Примечания

1 Приведенные ниже тестовые последовательности демонстрируют воздействие скремблера на пакет TS. Оно включает как шифрование полезной нагрузки пакета, так и изменение бита transport_scrambling_control согласно [3]:

2 Нормативная часть настоящего стандарта описывает только шифрование полезной нагрузки.

В данном приложении использованы следующие условные обозначения:

XX XX XX – заголовок пакета TS;

XX XX XX – поля адаптации;

XX XX XX – байты полезной нагрузки, оставленные без изменений;

XX XX XX – скремблированные байты полезной нагрузки.

Таблица Б.1 — Случай 1: без поля адаптации

Вид пакета	Данные
Пакет без изменений	47 60 80 11 54 68 69 73 20 69 73 20 74 68 65 20 70 61 79 6c 6f 61 64 20 75 73 65 64 20 66 6f 72 20 63 72 65 61 74 69 6e 67 20 74 68 65 20 74 65 73 74 20 76 65 63 74 6f 72 73 20 66 6f 72 20 74 68 65 20 44 56 42 20 49 50 54 56 20 73 63 72 61 6d 62 6c 65 72 2f 64 65 73 63 72 61 6d 62 6c 65 72 2e 20 54 68 69 73 20 69 73 20 74 68 65 20 70 61 79 6c 6f 61 64 20 75 73 65 64 20 66 6f 72 20 63 72 65 61 74 69 6e 67 20 74 68 65 20 74 65 73 74 20 76 65 63 74 6f 72 73 20 66 6f 72 20 74 68 65 20 44 56 42 20 49 50 54 56 20 73 63 72 61 6d 62 6c 65 72 2f 64 65 73 63 72 61 6d 62 6c 65 72
Скремблированный пакет	47 60 80 91 15 ce 67 e0 cb 01 b5 3c e7 60 54 e5 7a 4a d1 20 a0 df a4 ea aa e9 32 c6 78 3f 51 ae 19 fa ee 10 8b db 78 f3 11 3e c2 b5 72 cc 20 85 00 a5 2c ec a1 14 12 6c 58 24 4d f5 63 e7 a9 b4 e0 41 cb c3 fb ff fb d8 3c 8f bf fb 10 e8 3e a3 82 04 ba d7 02 fb 01 a2 7b 62 2c 4f 85 aa b6 aa 75 55 97 20 d6 5a b8 44 ce a2 8c f2 e1 fe 5e 7a c1 9d 44 81 89 19 c2 32 49 f1 40 75 7b 5d 16 c0 af 45 b2 5f 50 9b 9d a0 61 97 12 c5 9f 0b 39 b0 6f 1f be 90 12 3f 21 29 83 93 6a 95 31 7f cb 62 f4 34 6a 1b 1e 16 48 40 30 3a ff 83 8a 01 9b f8 10 a8 e0 b2 2f 64 65 73 63 72 61 6d

Таблица Б.2 — Случай 2: поле адаптации длиной 7 байтов

Вид пакета	Данные
Пакет без изменений	47 60 80 31 06 00 FF FF FF FF FF 54 68 69 73 20 69 73 20 74 68 65 20 70 61 79 6c 6f 61 64 20 75 73 65 64 20 66 6f 72 20 63 72 65 61 74 69 6e 67 20 74 68 65 20 74 65 73 74 20 76 65 63 74 6f 72 73 20 66 6f 72 20 74 68 65 20 44 56 42 20 49 50 54 56 20 73 63 72 61 6d 62 6c 65 72 2f 64 65 73 63 72 61 6d 62 6c 65 72 2e 20 54 68 69 73 20 69 73 20 74 68 65 20 70 61 79 6c 6f 61 64 20 75 73 65 64 20 66 6f 72 20 63 72 65 61 74 69 6e 67 20 74 68 65 20 74 65 73 74 20 76 65 63 74 6f 72 73 20 66 6f 72 20 74 68 65 20 44 56 42 20 49 50 54 56 20 73 63 72 61 6d 62 6c 65 72 2f
Скремблированный пакет	47 60 80 b1 06 00 FF FF FF FF FF 15 ce 67 e0 cb 01 b5 3c e7 60 54 e5 7a 4a d1 20 a0 df a4 ea aa e9 32 c6 78 3f 51 ae 19 fa ee 10 8b db 78 f3 11 3e c2 b5 72 cc 20 85 00 a5 2c ec a1 14 12 6c 58 24 4d f5 63 e7 a9 b4 e0 41 cb c3 fb ff fb d8 3c 8f bf fb 10 e8 3e a3 82 04 ba d7 02 fb 01 a2 7b 62 2c 4f 85 aa b6 aa 75 55 97 20 d6 5a b8 44 ce a2 8c f2 e1 fe 5e 7a c1 9d 44 81 89 19 c2 32 49 f1 40 75 7b 5d 16 c0 af 45 b2 5f 50 9b 9d a0 61 97 12 c5 9f 0b 39 b0 6f 1f be 90 12 3f 21 29 83 93 6a 95 31 7f cb 62 f4 34 6a 1b 1e 16 48 40 30 3a ff 83 8a 01 9b f8 10 a8 e0 b2 2f

Таблица Б.3 — Случай 3: поле адаптации длиной 8 байтов

Вид пакета	Данные
Пакет без изменений	47 60 80 31 07 00 FF FF FF FF FF FF 54 68 69 73 20 69 73 20 74 68 65 20 70 61 79 6c 6f 61 64 20 75 73 65 64 20 66 6f 72 20 63 72 65 61 74 69 6e 67 20 74 68 65 20 74 65 73 74 20 76 65 63 74 6f 72 73 20 66 6f 72 20 74 68 65 20 44 56 42 20 49 50 54 56 20 73 63 72 61 6d 62 6c 65 72 2f 64 65 73 63 72 61 6d 62 6c 65 72 2e 20 54 68 69 73 20 69 73 20 74 68 65 20 70 61 79 6c 6f 61 64 20 75 73 65 64 20 66 6f 72 20 63 72 65 61 74 69 6e 67 20 74 68 65 20 74 65 73 74 20 76 65 63 74 6f 72 73 20 66 6f 72 20 74 68 65 20 44 56 42 20 49 50 54 56 20 73 63 72 61 6d 62 6c 65 72
Скремблированный пакет	47 60 80 b1 07 00 FF FF FF FF FF FF 15 ce 67 e0 cb 01 b5 3c e7 60 54 e5 7a 4a d1 20 a0 df a4 ea aa e9 32 c6 78 3f 51 ae 19 fa ee 10 8b db 78 f3 11 3e c2 b5 72 cc 20 85 00 a5 2c ec a1 14 12 6c 58 24 4d f5 63 e7 a9 b4 e0 41 cb c3 fb ff fb d8 3c 8f bf fb 10 e8 3e a3 82 04 ba d7 02 fb 01 a2 7b 62 2c 4f 85 aa b6 aa 75 55 97 20 d6 5a b8 44 ce a2 8c f2 e1 fe 5e 7a c1 9d 44 81 89 19 c2 32 49 f1 40 75 7b 5d 16 c0 af 45 b2 5f 50 9b 9d a0 61 97 12 c5 9f 0b 39 b0 6f 1f be 90 12 3f 21 29 83 93 6a 95 31 7f cb 62 f4 34 6a 1b 1e 16 48 40 30 3a ff 83 8a 01 9b f8 10 a8 e0 b2

Таблица Б.4 — Случай 4: поле адаптации длиной 9 байтов

Вид пакета	Данные
Пакет без изменений	47 60 80 31 | 08 00 FF FF FF FF FF FF FF 54 | 68 69 73 20 69 73 20 74 68 65 20 70 61 79 6c 6f 61 64 20 75 73 65 64 20 66 6f 72 20 63 72 65 61 74 69 6e 67 20 74 68 65 20 74 65 73 74 20 76 65 63 74 6f 72 73 20 66 6f 72 20 74 68 65 20 44 56 42 20 49 50 54 56 20 73 63 72 61 6d 62 6c 65 72 2f 64 65 73 63 72 61 6d 62 6c 65 72 2e 20 54 68 69 73 20 69 73 20 74 68 65 20 70 61 79 6c 6f 61 64 20 75 73 65 64 20 66 6f 72 20 63 72 65 61 74 69 6e 67 20 74 68 65 20 74 65 73 74 20 76 65 63 74 6f 72 73 20 66 6f 72 20 74 68 65 20 44 56 42 20 49 50 54 56 20 73 63 72 61 6d 62 6c 65
Скремблированный пакет	47 60 80 b1 | 08 00 FF FF FF FF FF FF FF 15 | ce 67 e0 cb 01 b5 3c e7 60 54 e5 7a 4a d1 20 a0 df a4 ea aa e9 32 c6 78 3f 51 ae 19 fa ee 10 8b db 78 f3 11 3e c2 b5 72 cc 20 85 00 a5 2c ec a1 14 12 6c 58 24 4d f5 63 e7 a9 b4 e0 41 cb c3 fb ff fb d8 3c 8f bf fb 10 e8 3e a3 82 04 ba d7 02 fb 01 a2 7b 62 2c 4f 85 aa b6 aa 75 55 97 20 d6 5a b8 44 ce a2 8c f2 e1 fe 5e 7a c1 9d 44 81 89 19 c2 32 49 f1 40 75 7b 5d 16 c0 af 45 b2 5f 50 9b 9d a0 61 97 12 c5 9f 0b 39 b0 6f 1f be 90 12 3f 21 29 83 93 6a 95 31 7f cb 62 f4 34 6a 1b 42 20 49 50 54 56 20 73 63 72 61 6d 62 6c 65

Библиография

[1] NIST FIPS Publication 197 (2001) Публикация 197 (2001) «Улучшенный стандарт шифрования». Национальный институт стандартов и технологии, 2001
(«Advanced Encryption Standard», National Institute of Standards and Technology, 2001)

[2] Патентная заявка США, публикация № 2004/0247117
(U.S. Patent Application Pub. No. 2004/0247117)

[3] ETSI TS 100 289 (2011) «Телевидение вещательное цифровое (DVB); Алгоритм скремблирования версии 3 в цифровых вещательных системах»
(«Digital Video Broadcasting (DVB); Support for use of the DVB Scrambling Algorithm version 3 within digital broadcasting systems»)

[4] NIST Special Publication 800-38A «Рекомендации по режимам работы блочного шифра — методы и приемы»
(«Recommendation for Block Cipher Modes of Operation — Methods and Techniques»)

[5] ETSI EN 300 468 V1.11.1 (2010-04) «Телевидение вещательное цифровое (DVB); Спецификация для служебной информации (СИ) в DVB системах»
(«Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems»)

УДК 621.397.132.129:006.354 ОКС 33.170

Ключевые слова: телевидение вещательное цифровое, алгоритмы скремблирования, скремблирование контента, DVB-IPTV

Редактор *Ю.А. Расторгуева*
Технический редактор *В.Н. Прусакова*
Корректор *Р.А. Ментова*
Компьютерная верстка *Е.Е. Кругова*

Сдано в набор 18.02.2020. Подписано в печать 17.06.2020. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 1,86.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru