ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57871— 2017

ТЕЛЕВИДЕНИЕ ВЕЩАТЕЛЬНОЕ ЦИФРОВОЕ. РАСШИРЕННАЯ СПЕЦИФИКАЦИЯ ОБЩЕГО ИНТЕРФЕЙСА В СИСТЕМАХ ОГРАНИЧЕНИЯ ДОСТУПА CI Plus™. СИСТЕМА УПРАВЛЕНИЯ КОНТЕНТОМ

Основные параметры

[ETSI TS 103 205 V1.1.1 (2014-03), NEQ]

Издание официальное

Москва
Стандартинформ
2020

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 31 октября 2017 г. № 1585-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений стандарта Европейского института по стандартизации в области телекоммуникаций (ETSI) ЕТСИ ТС 103 205 V1.1.1 (2014-03) «Телевидение вещательное цифровое. Расширенная спецификация общего интерфейса в системах ограничения доступа CI Plus™» [ETSI TS 103 205 V1.1.1 (2014-03) «Digital Video Broadcasting (DVB); Extensions to the CI Plus™ Specification», NEQ]

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Март 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 (www.gost.ru)

© Стандартинформ, оформление, 2017, 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, обозначения и сокращения 1
3.1 Термины и определения 1
3.2 Обозначения 2
3.3 Сокращения 2
4 Общие сведения о расширенной спецификации общего интерфейса 3
4.1 Вводная часть 3
4.2 Компоненты системы управления контентом 4
4.3 Основные принципы реализации 5
4.4 Аутентификация хоста и CICAM 6
4.5 Обмен ключами и шифрование контента 6
4.6 Улучшенный MMI 6
5 Система управления контентом 6
5.1 Схема системы управления контентом 6
5.2 Правила работы общего интерфейса 7
5.3 Иерархия ключей 9
5.4 Ввод модуля CICAM в действие 12
5.5 Введение в аннулирование хоста 14
5.6 Шифрование и дешифрование контента 14
5.7 Применение управления копированием контента 15

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТЕЛЕВИДЕНИЕ ВЕЩАТЕЛЬНОЕ ЦИФРОВОЕ. РАСШИРЕННАЯ СПЕЦИФИКАЦИЯ ОБЩЕГО ИНТЕРФЕЙСА В СИСТЕМАХ ОГРАНИЧЕНИЯ ДОСТУПА CI Plus™. СИСТЕМА УПРАВЛЕНИЯ КОНТЕНТОМ

Основные параметры

Digital video broadcasting. Extensions to the CI Plus™ specification. Content control system. Basic parameters

Дата введения — 2018—08—01

1 Область применения

Спецификация общего интерфейса CI Plus™ системы условного доступа, установленная стандартом ГОСТ Р 56950, обеспечивает защиту информации, передаваемой по каналам вещания и по каналам интернет-протокола от головного узла до дескремблера TS системы ограничения доступа. Настоящий стандарт дополняет ГОСТ Р 56950 и устанавливает основные параметры системы управления контентом, работающей в составе системы безопасной передачи информации через обратный канал общего интерфейса.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ Р 53528 Телевидение вещательное цифровое. Требования к реализации протокола высокоскоростной передачи информации DSM-CC. Основные параметры

ГОСТ Р 56950 Телевидение вещательное цифровое. Расширенная спецификация общего интерфейса в системах ограничения доступа CI Plus™. Основные параметры

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, обозначения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 52591, ГОСТ Р 53528, а также следующие термины с соответствующими определениями:

3.1.1 **аутентификация** (authentication): Процедура подтверждения, что хост или CICAM имеют подлинный сертификат и что сертификат не был отменен, а также средство подтверждения, что сообщение получено из доверяемого источника.

Издание официальное

3.1.2 **аутентифицированный** (authenticated): Подтвержденная процедура в результате применения аутентификации.

3.1.3 **вещатель** (broadcaster): Объект, который агрегирует и распространяет контент аудио/видео.

3.1.4 **высокий уровень MMI кодирования объектов текста (**high-level MMI text object coding): Уровень кодирования, обеспечивающий гарантированную доставку контента.

3.1.5 **дескриптор** (descriptor): Ключевое слово, определяющее тип передаваемых данных.

3.1.6 **интерфейс MMI высокого уровня** (high-level MMI): Интерфейс MMI, не нарушающий работы приложений, запущенных на хосте.

3.1.7 **контент** (content): Видео- и аудиофайлы, к которым пользователь хотел бы получить доступ и которые могут быть сохранены на персональном цифровом рекордере (Personal Digital Recorder; PDR).

3.1.8 **протокол Диффи-Хеллмана** (Diffie Hellman; DH): Криптографический протокол, который дает возможность двум сторонам получить общий ключ шифрования при использовании незащищенного от перехвата канала связи. Полученный ключ используется для шифрования обмена данными с помощью алгоритмов симметричного шифрования.

3.1.9 **сертификат CICAM** (CICAM certificate): Уникальный сертификат, выданный каждому CICAM. Сертификат используется для проверки подлинности CICAM. Имя параметра: CICAM_DevCert.

3.1.10 **сертификат хоста** (host certificate): Уникальный сертификат, выданный для каждого устройства хост. Сертификат используется для аутентификации хоста. Имя параметра: Host_DevCert.

3.1.11 **скремблированный контент** (scrembled content): Защищенный контент для предотвращения несанкционированного доступа.

3.1.12 **транспортный поток** (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.

3.1.13 **тюнер** (tuner): IRD, имеющий функциональную возможность доставки TS, содержащего не менее одной службы DVB.

3.1.14 **управляемый контент** (controlled content): Контент, переданный от главного узла, с набором битов индикатора режима шифрования ("EMI") со значением, не равным нулю, или с набором битов EMI со значением, равным нулю, но с набором значений RCT, равным 1.

3.1.15 **хост** (host): IRD, включающий в себя интерфейс CI Plus™, совместимый со слотом CICAM.

3.1.16 **хеширование** (**хеш-функции** или **функции свертки)** (pashing): Преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины.

3.1.17 **шифрованный контент** (encrypted content): Контент, модифицированный для предотвращения несанкционированного доступа (синоним «скремблированный контент»).

3.1.18 **Nonce:** Одноразовый код, выбранный псевдослучайным образом.

3.2 Обозначения

В настоящем стандарте применены следующие обозначения:

E{K}(M) — шифрование сообщения 'M' с помощью ключа 'K' (Encryption of message 'M' using key 'K');

D{K}(M) — дешифрование сообщения 'M' с помощью ключа 'K' (Decryption of message 'M' using key 'K');

P — открытый ключ (Public Key);

Q — закрытый ключ (Private Key);

DQ — закрытый ключ устройства (Device Private Key),

DP — открытый ключ устройства (Device Public Key);

A{K}(M) — аутентификация сообщения 'M' ключом 'K' (Authentication of message 'M' with key 'K');

V{K}(M) 0 — проверка сообщения 'M' ключом 'K' (Verification of message 'M' with key 'K');

0x… префикс шестнадцатеричного числа;

0b… префикс двоичного числа.

3.3 Сокращения

В настоящем стандарте применены следующие сокращения:

AES — расширенный стандарт шифрования;

AKH — ключ аутентификации хоста;

AKM — ключ аутентификации модуля;

APDU — модуль данных протокола приложения;

APS — система защиты аналогового выхода хоста;

AV — аудио-видео;

BSM — режим основной службы;
CA — условный доступ;
CAS — система условного доступа;
CASD — дескриптор CAS;
CC — управление контентом;
CCK — ключ управления контентом;
CI — общий интерфейс;
CI Plus™ — общий интерфейс с расширенной спецификацией;
CICAM — модуль CI CA;
CIV — вектор инициализации управления контентом;
CRL — список отозванных (аннулированных) сертификатов,
CWL — список белых сертификатов;
DES — стандарт шифрования данных;
DH — протокол Диффи-Хеллмана;
DHPH — открытый ключ Диффи-Хеллмана хоста;
DHSK — секретный ключ Диффи-Хеллмана;
DTV — цифровое телевидение;
DVB — цифровое телевизионное вещание;
EMI — индикатор режима шифрования;
ECM — сообщение управления доступом;
EMM — сообщение разрешения доступа;
ID — идентификатор;
IRD — интегрированный приемник-декодер;
MDQ — устройство закрытого ключа;
MMI — интерфейс «человек — машина»;
PRNG — генератор псевдослучайных чисел;
RCT — маркер управления перераспределением;
RSM — режим зарегистрированной службы;
SAC — канал безопасной аутентификации;
SAK — ключ аутентификации SAC;
SEK — ключ шифрования SAC;
SHA — алгоритм безопасного хеширования;
SHA-256 — алгоритм безопасного хеширования, версия 256;
SIV — вектор инициализации SAC;
TS — транспортный поток;
TSC — управление скремблированием транспортного потока;
URI — информация по правилам использования.

4 Общие сведения о расширенной спецификации общего интерфейса

4.1 Вводная часть

Общий интерфейс DVB является составной частью системы ограниченного доступа, определенной ГОСТ Р 56950.

Спецификации общего интерфейса DVB, определенные ГОСТ Р 56950, устанавливают требования к общему интерфейсу CI Plus™.

Настоящий стандарт устанавливает основные параметры системы управления контентом, работающей в составе системы безопасной передачи информации через обратный канал общего интерфейса CI Plus™. Повышение безопасности передачи контента через обратный канал общего интерфейса от дескремблера системы CA к декодеру приемника DTV пользователя абонента достигается дополнительным шифрованием контента на стороне дескремблера и дешифрованием на стороне декодера приемника DTV. Схема системы условного доступа представлена на рисунке 1.

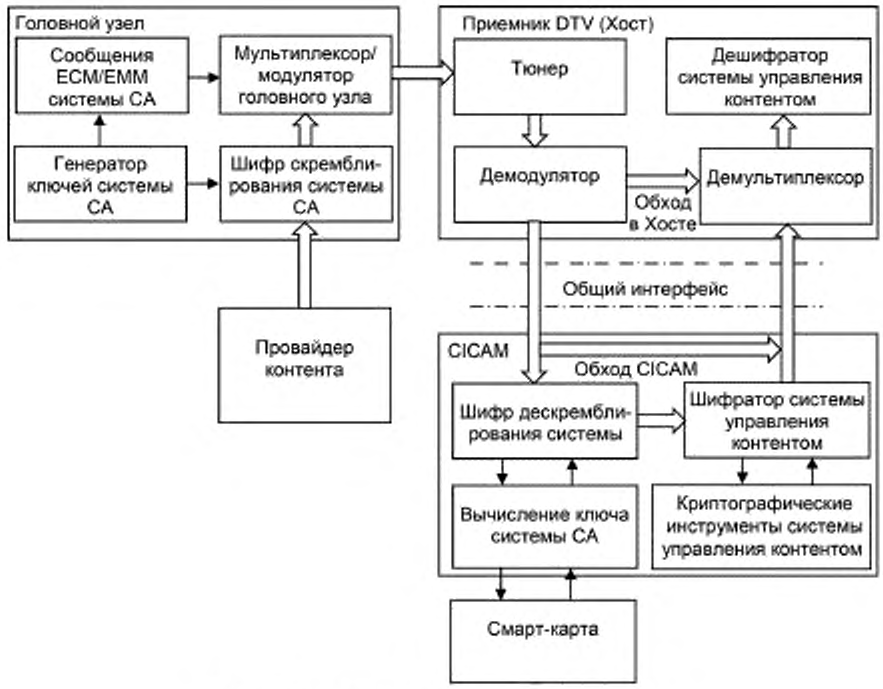

Рисунок 1 — Схема системы условного доступа

На головном узле системы CA защита контента от несанкционированного доступа выполняется системным скремблированием транспортного потока. Приемник DTV пользователя (хост) выполняет демодуляцию сигнала DTV и передает скремблированный транспортный поток на модуль CICAM системы CA. После системного дескремблирования модулем CICAM контент становится не защищенным от несанкционированного копирования при его перемещении через обратный канал общего интерфейса. Защита контента от копирования при передаче от дескремблера CA до декодера приемника DTV является задачей системы управления контентом, определенной в настоящем стандарте.

Настоящий стандарт не нормирует параметры управления копированием контентом, детализированные параметры механизмов аутентификации, вычисления ключей, управления открытыми ключами.

4.2 Компоненты системы управления контентом

Как показано на рисунке 1, система управления контентом включает в себя три устройства:

- головной узел,
- приемник DTV (хост),
- модуль CICAM.

В настоящем стандарте не рассматриваются вопросы защиты контента скремблированием, передаваемого по каналам DTV.

4.2.1 Головной узел

На головном узле система CA скремблирует контент, используя системный шифр CA. Головной узел вводит в поток информацию, которая позволяет модулю общего интерфейса системы условного доступа дескремблировать контент и управлять абонентским доступом и правами.

4.2.2 Хост

В контексте настоящего стандарта хост является устройством бытовой электроники, которое используется для приема цифровых данных каналов вещания. Это устройство должно включать один или более слотов общего интерфейса, через которые CICAM соединяется с хостом. Как правило, хост содержит тюнер, демодулятор, демультиплексор и декодеры. Хост передает демультиплексированный транспортный поток на CICAM. Состав хоста иллюстрируется на рисунке 1.

В соответствии с ГОСТ Р 56950 CICAM, работающий в составе системы СА, выполняет дескремблирование транспортного потока, поступающего от демультиплексора хоста, и возвращает его на хост через общий интерфейс для декодирования. Контент в дескремблированном TS передается хосту, не защищенным от копирования.

Хосты, совместимые с настоящим стандартом, могут взаимодействовать с CICAM, обеспечивая функционирование системы управления контентом, защищающей контент, который был дескремблирован системой СА.

Хост может определить соответствие CICAM, вставленного в слот, требованиям ГОСТ Р 56950 или соответствие требованиям настоящего стандарта. Хост должен работать как с модулями CICAM, соответствующими CI Plus™, так и с модулями CICAM, соответствующими ГОСТ Р 56950. Взаимосвязь режимов работы хоста и CICAM показана в таблице 1.

Таблица 1 — Взаимосвязь режимов работы хоста и CICAM

Режим работы		Хоста	
		CI	CI Plus™
CICAM	CI	По умолчанию, поведение CI соответствует ГОСТ Р 56950	Режим игнорирования хоста может защитить управляемый контент (опционально), если применение этой функции сигнализировано в потоке вещания. Режим CI по умолчанию соответствует ГОСТ Р 56950, если режим игнорирования хоста не активизирован вещателем. Контент дешифруется CICAM CI и не перекодируется в общем интерфейсе
	CI Plus™	Часть управляемого контента дескремблируется и под управлением системы общего интерфейса передается на хост. Контент, дескремблированный CICAM, повторно не шифруется на общем интерфейсе	Управляемый контент не будет отображаться, если CICAM и хост не аутентифицированы и хост поддерживает алгоритмы шифрования, предписанные CI Plus™ и повторно затребованные CICAM. Управляемый контент дескремблируется CICAM, повторно шифруется на общем интерфейсе со значением EMI в соответствии с URI

Хост включает в себя набор криптографических инструментов и функций, которые дают ему возможность оценить аутентичность и надежность сопряженного с ним модуля CICAM.

4.2.3 Модуль общего интерфейса системы условного доступа

В системе ограниченного доступа по ГОСТ Р 56950 CICAM является ее функциональным окончанием. CICAM содержит шифр дескремблирования СА, считыватель смарт-карт (опционально) и интерфейс программного обеспечения, дающий возможность вычисления ключей дешифрования при использовании данных из принятого потока.

Для версии общего интерфейса, не совместимого с CI Plus™, контент передается на хост в открытом виде через соединение CI, допускающее возможность перехвата и копирования. Настоящий стандарт обеспечивает шифрование контента в CICAM на местном уровне перед передачей контента хосту.

В дополнение к элементам системы защиты СА CICAM содержит криптографические инструменты и функции, которые позволяют ему аутентифицировать хост, в который был вставлен. Если CICAM аутентифицирован хостом, он может дескремблировать службу вещания и шифровать контент средствами системы управления контентом.

4.3 Основные принципы реализации

Система управления контентом CICAM включает следующие функциональные элементы:

- аутентификация хоста, основанная на обмене сертификатами CICAM и хоста. CICAM и хост проверяют сертификаты друг друга, используя методы проверки подписи. Идентификатор хоста CICAM проверяет (в режиме основной службы) по списку аннулированных (скомпрометированных) устройств и

отмененных мер против скомпрометированных устройств. Опционально служба оператора может проводить специальные проверки на головном узле (режим зарегистрированной службы);

- управление контентом. Система управления контентом зашифровывает в CICAM инструменты и функции для защиты передачи от CICAM к хосту;
- безопасность контента. Безопасное распространение содержания URI от головного узла системы CA к хосту.

CICAM дескремблирует TS контента, скремблированного системой условного доступа, а затем, перед доставкой на хост, повторно шифрует транспортный поток открытого контента с помощью ключа управления контентом. На хосте система управления контентом дешифрует транспортный поток контента.

4.4 Аутентификация хоста и CICAM

Система управления контентом требует выполнения аутентификации хоста и CICAM до начала процесса дескремблирования модулем CICAM контента, скремблированного системой CA. CICAM запрашивает сертификат хоста, и хост предоставляет его. Хост запрашивает сертификат CICAM, и CICAM предоставляет его.

Аутентификация выполняется при следующих процедурах:

- проверка CICAM подписи сертификата, содержащей ID хоста;
- проверка хостом подписи сертификата, содержащей ID CICAM;
- проверка наличия у CICAM и хоста закрытых ключей, каждый из которых соединен с открытыми ключами, встроенными в сертификаты, и передача закрытых ключей другим устройствам (хосту или CICAM соответственно) для проверки подписи;
- CICAM и хост подтверждают, что они могут получить ключ аутентификации.

4.5 Обмен ключами и шифрование контента

Механизм управления контентом состоит из четырех этапов:

- настройка режимов работы;
- вычисление ключа;
- шифрование контента;
- шифрование контента в соответствии со значениями URI, которые безопасно передаются механизмом управления контентом.

CICAM и хост содержат алгоритмы согласования ключей Диффи-Хеллмана (DH), алгоритм хэширования SHA-256, DES и AES. CICAM и хост содержат также закрытые ключи и соответствующие открытые ключи.

4.6 Улучшенный MMI

Параметры улучшенного интерфейса MMI должны соответствовать ГОСТ Р 56950.

5 Система управления контентом

Принятый контент дескремблируется модулем CICAM в системе CA согласно ГОСТ Р 56950, в незащищенном от копирования виде и через общий интерфейс возвращается на хост. В разделе 5 определены требования к защите контента. Защита контента выполняется путем шифрования при выполнении следующих операций:

- взаимная аутентификация CICAM и хоста;
- верификация (проверка полномочий) хоста и CICAM;
- расчет ключа шифрования;
- использование связи по безопасному аутентифицированному каналу.

5.1 Схема системы управления контентом

Система управления контентом включает в себя головной узел, хост и CICAM. Все устройства, расположенные по тракту выше головного узла, и любые соединения между хостом и другими устройствами настоящим стандартом не нормируются. Настоящий стандарт определяет правила, которые хост должен использовать при формировании сигналов массовой информации, доступной на любом совместимом внешнем интерфейсе.

На рисунке 2 показана совокупность схем защиты контента, включающая систему защиты CA и систему управления контентом.

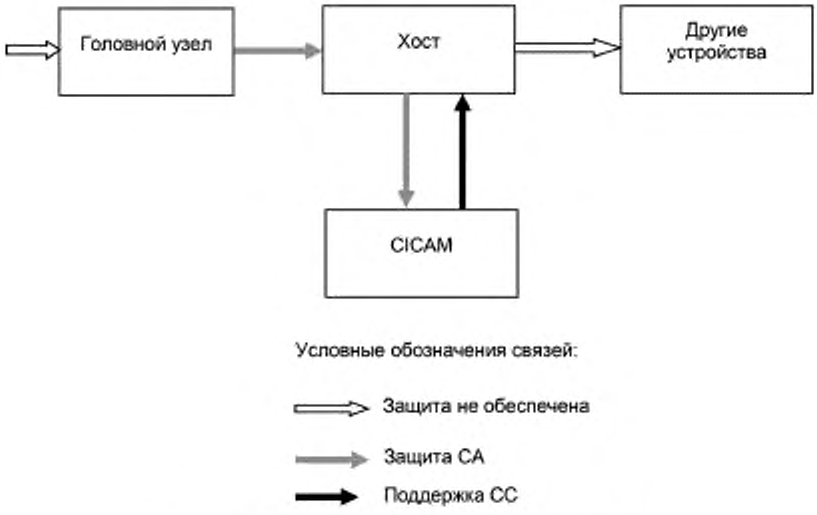

Рисунок 2 — Совокупность схем защиты контента

Настоящий стандарт устанавливает общие параметры системы управления контентом (CC), обеспечивающей безопасность обратного канала интерфейса между CICAM и хостом. CICAM работает, используя средства системы CA и набор криптографических средств для обеспечения защиты информации, проходящей к хосту. Хост, используя аналогичный набор криптографических средств, снимает защиту и делает контент доступным для декодера хоста.

5.2 Правила работы общего интерфейса

Процессы запуска интерфейса при включении питания описываются в ГОСТ Р 56950. Ресурс системы управления контентом, определенный в настоящем стандарте, используется для защиты контента при следующих условиях:

а) контент передается от CICAM к хосту;

б) контент становится доступным на внешнем интерфейсе хоста.

Процесс защиты контента состоит из нескольких этапов. Компоненты системы используют ресурс системы CC для выполнения процесса взаимной аутентификации. После того как CICAM и хост подтвердили, что они общаются с нормализованными компонентами CI Plus™, инициализируется безопасный канал аутентификации (SAC). SAC используется для передачи сообщений, аутентификации и шифрования. Компоненты системы устанавливают общий ключ шифрования/дешифрования CC, обмениваются URI и лицензиями (опционально).

Диаграмма этапов процесса защиты контента иллюстрируется на рисунке 3. Описание этапов процесса защиты контента представлено в таблице 2.

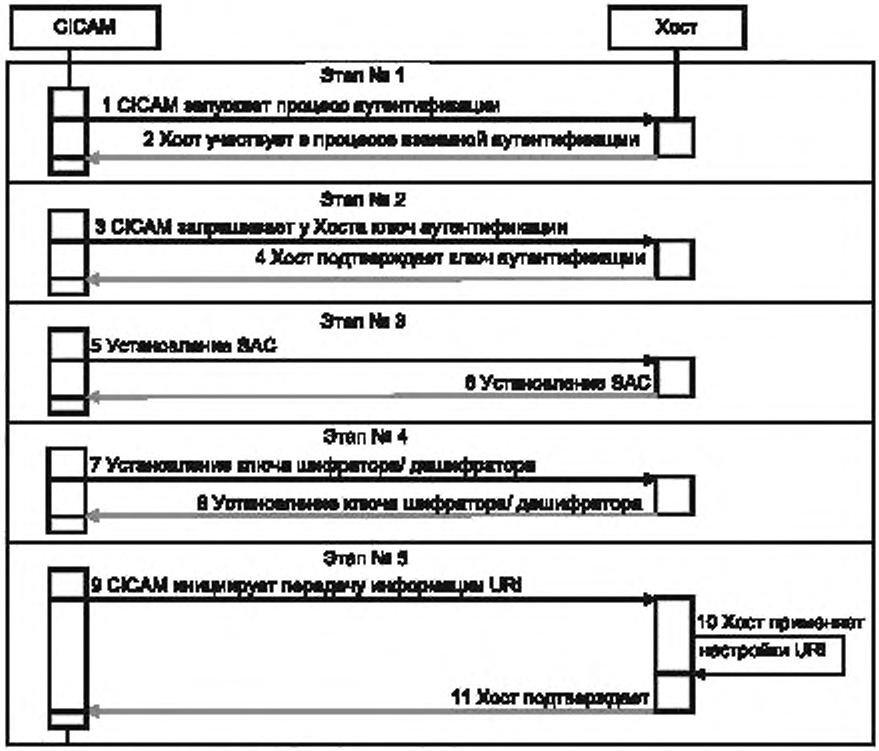

Рисунок 3 — Диаграмма этапов процесса защиты контента

Таблица 2 — Описания этапов процесса защиты контента

Порядковый номер	Описание
Этап № 1	Начало аутентификации — проверка сертификатов и обмен ключами DH
1	CICAM запускает процесс аутентификации. CICAM инициирует процесс аутентификации, если отсутствует ключ аутентификации, сохранившийся от предыдущего сеанса успешного взаимодействия CICAM и хоста
2	Хост участвует в процессе взаимной аутентификации. Хост проверяет данные в полученном протоколе для определения соответствия CICAM норме и участвует во взаимном процессе аутентификации
Этап № 2	Начало аутентификации — подтверждение подлинности ключа
3	CICAM запрашивает ключ аутентификации (АКН) у хоста для проверки. CICAM запрашивает ключ аутентификации (АКН) от хоста для проверки идентичности ключей, рассчитанных CICAM и хостом. Хост отвечает на этот запрос, пересылая свой вычисленный ключ аутентификации
4	Хост подтверждает ключ аутентификации
Этап № 3	Установление безопасного канала аутентификации SAC
5, 6	Установление SAC. После успешной аутентификации CICAM и хост начинают обмениваться данными и вычислять материал ключей (SEK) для шифрования ключей и аутентификации SAC, которые должны быть переданы по SAC. После создания ключей SAK и SEK CICAM должен синхронизироваться с хостом и начать использовать новые ключи в рамках установленного интервала времени. Инициализация SAC выполняется при использовании материала ключей

Окончание таблицы 2

Порядковый номер	Описание
Этап № 4 7, 8	Установление ключа СС. После успешной аутентификации CICAM может начать вычисление ключа управления контентом (ключ СС). После успешной инициализации SAC CICAM может сообщить хосту о вычислении ключа СС. После установления ключа СС CICAM должен синхронизироваться с хостом, чтобы начать использовать новый ключ СС на интервале определенного времени ожидания. Шифратор/дешифратор инициализируется, используя этот ключ СС Примечание — Этот этап может выполняться неоднократно на интервале максимального времени жизни ключа.
Этап № 5	Передача информации URI и управление копированием контента
9	CICAM инициирует передачу информации URI и (опционально) лицензии. CICAM передает URI и лицензию (опционально), которая сопоставляет текущие ограничения управления копированием выбранной службы на хосте. Этот этап может быть выполнен несколько раз на интервале события программы, используя фактическое значение URI
10 11	Хост применяет настройки URI. Хост применяет параметры URI в соответствии с записанной лицензией. Хост подтверждает. После получения информации URI хост должен ответить CICAM в течение заданного интервала времени, а затем применить ограничения управления копированием на внешних интерфейсах

5.3 Иерархия ключей

Ключи, используемые для защиты контента и управления копированием контента, относятся к следующим уровням иерархии:

- уровень проверки полномочий;
- уровень аутентификации;
- уровень канала безопасной аутентификации;
- уровень управления контентом.

5.3.1 Ключи уровня проверки полномочий

На уровне проверки полномочий предусмотрены открытый и закрытый ключи, предназначенные для CICAM и для хоста. CICAM имеет устройство закрытого ключа (MDQ) и соответствующее устройство открытого ключа (MDP), которые встроены в сертификат устройства CICAM. Хост по аналогии с CICAM имеет устройства закрытого (HDQ) и открытого (HDP) ключей.

Данные уровня проверки полномочий (ключи, начальные числа, сертификаты и константы), представленные в таблице 3, участвуют в операциях на уровне аутентификации. Уровень проверки полномочий содержит параметры, которые не подлежат замене.

Таблица 3 — Данные уровня проверки полномочий

Имя ключа	Описание	Сохраненный или временный	Замененный или сохраненный местный
Root cert	Корневой сертификат	Сохраненный (постоянная лицензия)	Сохраненный местный (не подлежит замене)
Brand cert	Сертификат марки	Сохраненный (постоянная лицензия)	Сохраненный местный (не подлежит замене)
Device cert	Сертификат устройства	Сохраненный (постоянная лицензия)	Сохраненный местный (не подлежит замене)
prng_seed	Начальное число для PRNG устанавливается изготовителем	Сохраненный (постоянная лицензия)	Сохраненный местный (не подлежит замене)

Окончание таблицы 3

Имя ключа	Описание	Сохраненный или временный	Замененный или сохраненный местный
DH_p	Основной модуль Диффи-Хеллмана	Сохраненный (постоянная лицензия)	Сохраненный местный
DH_g	Модуль генератора Диффи-Хеллмана	Сохраненный (постоянная лицензия)	Сохраненный местный
DH_q	Константа Диффи-Хеллмана	Сохраненный (постоянная лицензия)	Сохраненный местный
MDQ	Закрытый ключ устройства модуля CICAM	Сохраненный (постоянная лицензия)	Сохраненный местный (не подлежит замене)
MDP	Открытый ключ устройства модуля CICAM	Сохраненный	Замененный
HDQ	Закрытый ключ хоста	Сохраненный (постоянная лицензия)	Замененный или сохраненный местный (не подлежит замене)
HDP	Открытый ключ хоста	Сохраненный	Замененный
DHX	Nonce Диффи-Хеллмана (e^x)	Временный	Сохраненный местный
DHY	Nonce Диффи-Хеллмана (e^y)	Временный	Сохраненный местный
DHPM	Открытый ключ Диффи-Хеллмана модуля CICAM	Временный	Сохраненный местный
DHPH	Открытый ключ Диффи-Хеллмана хоста	Временный	Замененный
DHSK	Закрытый ключ Диффи-Хеллмана	Сохраненный	Сохраненный местный
AKM	Ключ аутентификации модуля	Сохраненный (на модуле)	Сохраненный местный
AKH	Ключ аутентификации хоста	Сохраненный (на хосте)	Замененный (защищенный)
Ns_Module	Nonce SAC модуля CICAM	Временный	Замененный
Ns_Host	Nonce SAC хоста	Временный	Замененный
SEK	Ключ шифрования SAC	Временный	Сохраненный местный
SAK	Ключ аутентификации SAC	Временный	Сохраненный местный
SIV	Вектор инициализации SAC	Сохраненный (постоянная лицензия)	Сохраненный местный
Kp	Прекурсор ключа	Временный	Замененный (защищенный)
CCK	Ключ управления контентом	Временный	Сохраненный местный
CIV	Вектор инициализации CC	Временный	Сохраненный местный

Настоящий стандарт не определяет точные механизмы, используемые для защиты данных уровня полномочий.

5.3.2 Ключи уровня аутентификации

Ключами уровня аутентификации являются: открытый ключ из сертификата хоста или CICAM и закрытый ключ. Эти ключи участвуют в двух операциях:

1) защита обмена параметрами при аутентификации. Аутентификация основана на протоколе Диффи-Хеллмана, который хост использует для обмена параметрами, которые должны быть защищены от вредоносных источников помех;

2) проверка цепочки сертификатов. Цепочка сертификатов содержит информацию, которая используется в последующих шагах в иерархии ключей. Полученные сертификаты должны быть взаимно проверены.

Результирующими ключами для уровня аутентификации являются секретный ключ Диффи-Хеллмана (DHSK) и ключи аутентификации (AKM для CICAM и AKH для хоста). CICAM запрашивает ключ аутентификации, используемый хостом. AKM и AKH защищены и управляются на уровне аутентификации. Уровень аутентификации передает запрошенные ключи, но уровень, который использует эти ключи, не должен поддерживать или хранить их.

5.3.3 Ключи уровня канала безопасной аутентификации

На уровне SAC используются ключи для аутентификации и шифрования сообщения перед передачей. Приемная часть использует одинаковые расчетные ключи для расшифровки и проверки сообщения.

Ключ аутентификации SAC (SAK) используется для аутентификации и проверки сообщений SAC. Подобным же образом ключ шифрования SAC (SEK) используется для шифрования и дешифрования полезной нагрузки сообщений SAC. Ключи SAK и SEK рассчитываются на CICAM и хосте независимо друг от друга. Ключи SAK и SEK являются временными краткосрочными секретами. На рисунке 4 представлена схема процесса формирования ключей SAC.

5.3.4 Ключи уровня управления контентом

Уровень управления контентом использует ключи для шифрования контента AV перед его передачей от CICAM к хосту. Ключ управления контентом (CCK) (и при необходимости CIV) используется для шифрования AV. На принимающей стороне хост использует идентичные вычисленные ключи для дешифрования контента AV. CCK (и при необходимости CIV) рассчитываются независимо друг от друга на CICAM и хосте. CCK (и при необходимости CIV) являются временными, краткосрочными секретами. На рисунке 5 представлена схема процесса формирования ключей уровня управления контентом.

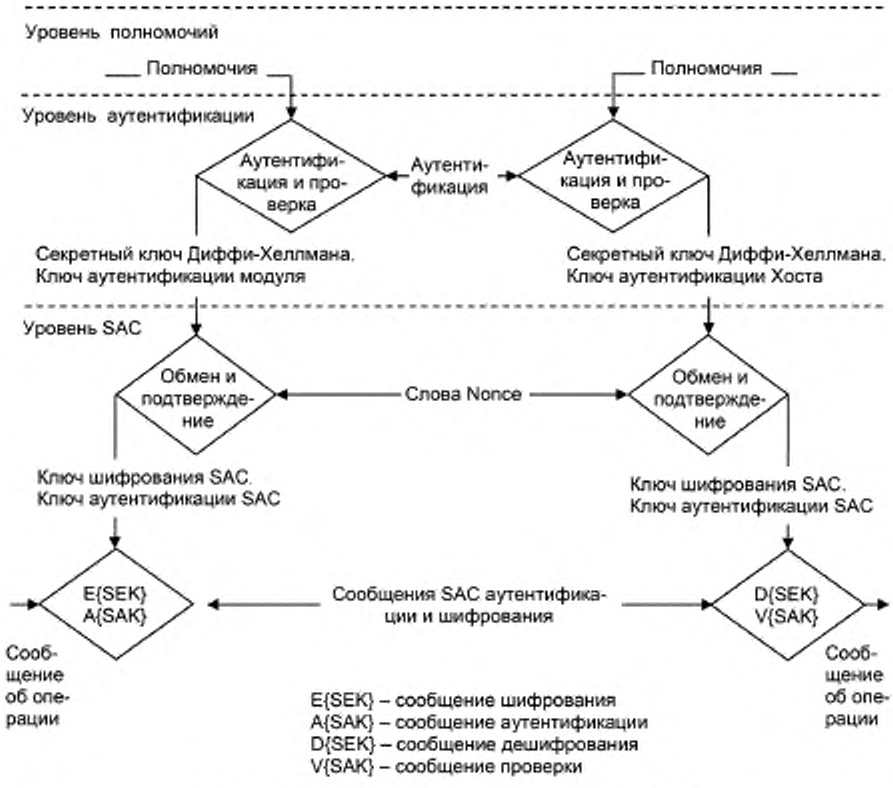

Рисунок 4 — Схема процесса формирования ключей SAC

5.4 Ввод модуля CICAM в действие

CICAM может быть введен в действие в режиме:

- основной службы (BSM);
- зарегистрированной службы (RSM).

Режим основной службы является обязательным, режим зарегистрированной службы — опциональным. Ввод в режим BSM выполняется в два этапа:

1) проверка сертификата и обмен ключами DH;

2) проверка ключа аутентификации.

Режим RSM поддерживает третий этап: отчет головной станции.



Рисунок 5 — Схема процесса формирования ключей уровня управления контентом

Каждый из режимов BSM и RSM CICAM может работать в двух субрежимах:

- ограниченный оперативный субрежим совместим с ГОСТ Р 56950 для служб, не требующих защиты CI Plus™, которые были дескремблированы системой CA;
- полностью оперативный субрежим совместим с CI Plus™ — для всех служб, повторно защищенных CI Plus™.

5.4.1 Ввод в действие CICAM в режиме основной службы

Режим основной службы определяет работу CICAM в среде вещания. CICAM не вступит в режим функционирования сразу в момент сопряжения с хостом и включения питания.

На рисунке 6 приведена схема процесса аутентификации в режиме BSM.

При включении питания CICAM определяет совместимость хоста с нормами CI Plus™. Хост, совместимый с CI Plus™, объявляет ресурс CC в протоколе диспетчера ресурсов при запуске в соответствии с ГОСТ Р 56950. Если хост не совместим с нормами CI Plus™, то выдается описание ошибки с помощью приложения MMI высокого уровня (3), и CICAM устанавливается в ограниченный оперативный режим в соответствии с ГОСТ Р 56950. Если хост совместим с нормами CI Plus™, то он проверяет возможность повторной аутентификации. Повторная аутентификация включением питания возможна, если CICAM ранее был успешно связан с хостом. В этом случае при успешной привязке могут быть пропущены операции проверки сертификатов, обмена ключами DH (5), проверки ключей аутентификации (6), и CICAM может запустить процесс создания SAC (7). После создания SAC следуют операции создания ключей CC (8) и установления CICAM в режим основной службы (9).

SAC используется для передачи информации правил использования (URI) в безопасном режиме. URI ассоциирована со службой/событием, которые защищены системой CA, и передает информацию управления (защиты) копированием для аналоговых (APS) и цифровых (EMI) выходов хоста. Хост по умолчанию применяет правила использования (в основном ограничительные) до тех пор, пока протокол доставки URI не будет успешно завершен.

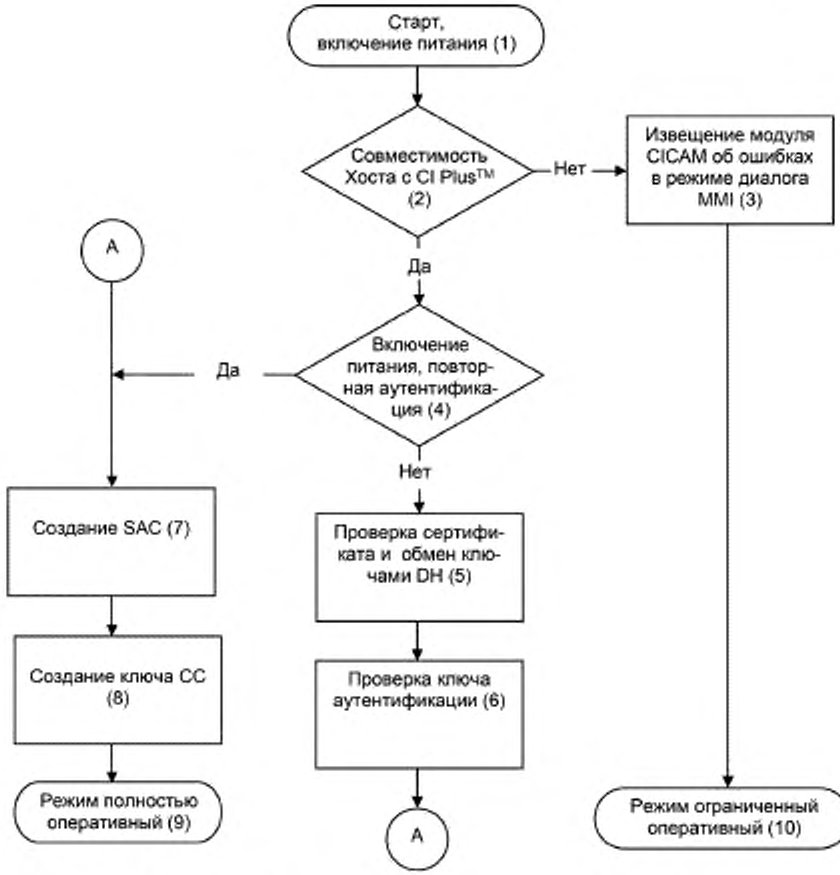

Рисунок 6 — Схема процесса аутентификации в режиме BSM

Ключи CC используются CICAM для шифрования защищаемых служб и для дешифрования хостом защищенных служб. Хост выводит (рассчитывает) ключ CC как результат обмена ключами DH, ключи CC не передаются с CICAM на хост. SAC и процесс установления ключей CC выполняются при необходимости замены ключей. Если по каким-либо причинам SAC или ключ CC не могут быть восстановлены, то CICAM возвращается в ограниченный оперативный субрежим (8). Если SAC и ключ CC могут быть возобновлены, то субрежим CICAM становится полностью оперативным.

Режим основной службы поддерживает аннулирование хоста при использовании списка аннулирования сертификата (CRL), который передан главным узлом к CICAM при использовании карусели данных DSM-CC. В случае аннулирования хоста CICAM сообщает пользователю, что его хост помещен в «черный» список. Для этого используется универсальная функция сообщения об ошибке.

В дополнение к CRL режим основной службы поддерживает «белый» список сертификата (CWL), который позволяет оператору службы отменять предыдущее аннулирование отдельного хоста. Механизм аннулирования настоящим стандартом не определяется.

5.4.2 Ввод в действие CICAM в режим зарегистрированной службы

Режим зарегистрированной службы является расширением режима основной службы и предназначен для сетей, которые содержат двунаправленный канал передачи от CICAM до сетевой абонентской системы управления. Чтобы реализовать режим зарегистрированной службы, CICAM может использовать высокий уровень MMI или приложение MMI к инструкциям и регистрационным данным пользователя для обеспечения обратной связи с сетевой абонентской системой управления. Оперативное поведение режима зарегистрированной службы определяется оператором службы и не нормируется настоящим стандартом.

5.4.3 Общие отчеты об ошибках

Сообщение об обнаружении ошибки формирует CICAM или хост. При обнаружении ошибки CICAM использует высокий уровень MMI или приложение MMI, чтобы отобразить код ошибки. Если хост обнаруживает ошибку, то он использует специфический метод отображения кода ошибки. Код ошибки может сопровождаться описательным текстом и должен быть подтвержден пользователем. Настоящим стандартом не определяются условия возникновения ошибок и соответствующие им коды.

В случаях, когда CICAM поддерживает режим зарегистрированной службы, поставщик CA или оператор службы, оценивая коды ошибок, определяет необходимые действия для устранения причин возникновения ошибок. Настоящий стандарт не нормирует правила необходимых действий по оценкам кодов ошибки.

5.5 Введение в аннулирование хоста

Настоящий стандарт использует аннулирование как метод работы с хостами, безопасность которых поставлена под угрозу. Настоящий стандарт различает три механизма аннулирования:

1) службы игнорирования хостом;

2) аннулирование CAS;

3) аннулирование хоста.

Служба игнорирования хостом — согласно ГОСТ Р 56950.

Механизмы аннулирования CAS и хоста определяются конкретной CAS и в настоящем стандарте не рассматриваются.

5.6 Шифрование и дешифрование контента

5.6.1 Уровень шифрования транспортного потока

Для защиты контента провайдер служб применяет шифрование элементарных потоков контента службы. Приемное устройство использует дешифратор для дешифрирования элементарных потоков. Дешифратор определяет правила дешифрирования, опрашивая биты управления шифрованием транспорта (TSC) в пакете TS в соответствии с таблицей 4.

Таблица 4 — Определения битов управления шифрованием транспорта

Бит управления шифрованием транспорта	Описание	Комментарии
00	Шифрование не применяется	Необходима поддержка
01	Шифрование контента ключом, заданным по умолчанию	Не поддерживается хостом и CICAM
10	Шифрование контента четным ключом	Необходима поддержка
11	Шифрование контента нечетным ключом	Необходима поддержка

Двухключевые дескремблеры используют два регистра для хранения ключей: первый регистр хранит ключ, который в настоящий момент использует дескремблер. В этот период второй регистр может обновляться данными нового ключа для следующего периода дешифрирования. Регистры идентифицированы как четный и нечетный. Биты TSC в пакете TS (как показано в таблице 4) указывают на ключ, который дескремблер использует в нечетном или четном регистре для дескремблирования пакета TS и при необходимости обращения к соответствующему регистру.

Для определения окончания процесса вычисления хостом ключа CC и загрузки его в требуемый регистр (четный или нечетный) CICAM и хост синхронизируются друг с другом. Для этого CICAM инициирует синхронизирующий APDU запроса, который подтверждает хост. Если время обновления ключей, определяемое по таймеру, истечет, то CICAM начинает использовать новый ключ CC (CCK) и меняет биты TSC заголовка пакета TS. Непосредственно после того, как CICAM изменит значение TSC, хост обнаруживает это изменение и переключается на альтернативный регистр ключа. Протокол URI передает значение URI хосту. URI указывает на ограничения контента.

5.6.1.1 Уровень шифрования PES

В случае, если провайдер служб использует уровень шифрования PES элементарных потоков, то есть биты PES_scrambling_control пакета PES_packet не равны нулю, любое повторное шифрование в CICAM должно быть применено на уровне транспортного потока, и в поле PES_scrambling_control должно быть установлено «Not Scrambled» (не шифровать).

5.6.2 Определение типов шифратора/дешифратора

5.6.2.1 Правила шифрования

Эта спецификация определяет два типа шифратора транспортного потока DES и AES. В таблице 5 описаны параметры шифрования хоста и CICAM.

Таблица 5 — Обязательные параметры шифрования хоста и CICAM

Шифратор	CICAM	Хост
DES-56-ECB	Обязательный	Обязательный для хоста SD и хоста HD
AES-128-CBC	Опциональный	Обязательный

Определения SD хостов и HD хостов настоящий стандарт не устанавливает.

Хост и CICAM согласовывают возможности шифратора во время обмена сертификатами, и каждый из них определяет возможность шифратора/дешифратора своего устройства-партнера. Правила выбора шифра шифрования приведены в таблице 6.

Таблица 6 — Правила выбора шифра шифрования

CICAM	Хост	Решение	Комментарий
Ни один из шифров	Ни один из шифров	Управление контентом остановлено и на выходе транспортного потока формируется «чистый» контент	Ни один из шифров для любого хоста или CICAM
DES	DES	Выход транспортного потока использует дешифрование DES	—
DES	AES	Выход транспортного потока использует дешифрование DES	—
AES	DES	Выход транспортного потока использует дешифрование DES	Примечание 3
AES	AES	Выход транспортного потока использует дешифрование AES	—

Примечания

1 Владелец контента может согласиться на использование DES или AES, а это означает, что провайдер может сделать выбор технологии для использования DES или AES.

2 Выход транспортного потока соответствует ГОСТ Р 56950.

3 Система CA может принять решение о том, что DES не подходит и предпочтет не расшифровывать контент.

5.7 Применение управления копированием контента

5.7.1 Определение URI

Провайдер контента и дистрибьютор контента определяют значения URI для каждой программы (службы или события). Система CA предоставляет URI безопасно от главного узла до CICAM. CICAM передает URI к хосту, используя протокол SAC. Хост использует URI для управления созданием копии, кодированием управления копированием аналогового выхода, ограничением инициирования изображения и установлением параметров управления копированием на выходах хоста.

5.7.2 Ассоциирование URI с контентом

Система CA должна безопасно связывать URI с контентом, определенным службой/событием MPEG-2. URI связана с выбранной службой через 16-разрядное число в формате MPEG-2. Все PID, принадлежащие службе (в соответствии с PMT), связаны только с одним URI.

Примечание — Контент (то есть события MPEG-2), рассматриваемый в настоящем стандарте, не должен использовать 16-разрядное число со значением 0 (ноль).

5.7.3 Передача URI от главного узла к CICAM

URI может передаваться от главного узла DVB к CICAM нераскрытыми способами. Так, например, должны переноситься необходимая информация о URI и информация о номере программы в сообщениях EMM или ECM, защищенных системой CA. Точный механизм передачи данных URI от главного узла до CICAM настоящий стандарт не устанавливает.

УДК 621.397:681.327.8:006.354 ОКС 31.170

Ключевые слова: DVB, общий интерфейс, контент, аутентификация, протокол Диффи-Хеллмана, общий интерфейс, шифратор, дешифратор

Редактор переиздания *Н.Е. Рагузина*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 02.03.2020. Подписано в печать 18.05.2020. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10.
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