МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

J.197
(11/2005)

СЕРИЯ J: КАБЕЛЬНЫЕ СЕТИ И ПЕРЕДАЧА СИГНАЛОВ ТЕЛЕВИЗИОННЫХ И ЗВУКОВЫХ ПРОГРАММ И ДРУГИХ МУЛЬТИМЕДИЙНЫХ СИГНАЛОВ

Кабельные модемы

Высокоуровневые требования к мосту управления цифровыми правами (DRM), соединяющему кабельную сеть доступа с домашней сетью

Рекомендация МСЭ-Т J.197

Рекомендация МСЭ-Т J.197

Высокоуровневые требования к мосту управления цифровыми правами (DRM), соединяющему кабельную сеть доступа с домашней сетью

Резюме

В настоящей Рекомендации определяются требования к мосту управления цифровыми правами, соединяющему кабельную сеть доступа с домашней сетью, в которую оператором сети может быть передан контент многих типов (например, видео, аудио и т. д.), при условии, что этот контент не используется с нарушением каких либо соглашений о предоставлении услуг или требований закона.

Источник

Рекомендация МСЭ-Т J.197 была утверждена 29 ноября 2005 года 9-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т J.197

Высокоуровневые требования к мосту управления цифровыми правами (DRM), соединяющему кабельную сеть доступа с домашней сетью

1 Сфера применения

В настоящей Рекомендации определяются требования к мосту управления цифровыми правами, соединяющему кабельную сеть доступа с домашней сетью, в которую оператором сети может быть передан контент многих типов (например, видео, аудио и т. д.), при условии, что этот контент не используется с нарушением каких либо соглашений о предоставлении услуг или требований закона.

2 Справочные документы

2.1 Нормативные справочные документы

В нижеследующих Рекомендациях МСЭ-Т и в других документах содержатся положения, которые, с помощью ссылки в настоящем тексте, составляют положения настоящей Рекомендации. На время публикации указанные здесь издания были действительными. Все Рекомендации и другие документы постоянно пересматриваются; поэтому всем пользователям данной Рекомендации настоятельно рекомендуется по возможности использовать последние издания перечисленных ниже Рекомендаций и других документов. Список действующих Рекомендаций МСЭ-Т регулярно публикуется. Ссылка в настоящей Рекомендации на какой-либо документ не придает этому отдельному документу статуса рекомендации.

– NIST FIPS 140-2 (2002), *Security requirements for cryptographic modules*.

2.2 Информативные справочные документы

– ITU-T Recommendation J.192 (2005), *A residential gateway to support the delivery of cable data services*.

– DTCP (2005), *Digital transmission content protection specification volume 1 (information version)*.

– Intel (2005), *High-bandwidth digital content protection system, revision 1.1*.

3 Термины и определения

В настоящей Рекомендации определены следующие термины:

3.1 биты аналоговой системы защиты (APS bits): Биты 3 и 2 байта CCI, определяющие состояние аналоговой защиты декодера телевизионных каналов.

3.2 правила соблюдения технических условий: Правила, которые применяются к декодерам телевизионных каналов с целью противодействия незаконному копированию контролируемого контента.

3.3 метка соглашения: Стандартная метка, разработанная для применения в DRM.

3.4 ограниченное изображение: Видимый эквивалент с размером не более 520 000 пикселов в кадре (например, изображение с разрешением 540 строк на 960 вертикальных линий для растра 16:9). Для повышения воспринимаемого качества изображения, ограниченное изображение может быть передано на выход устройства или отображено с использованием таких методов видеообработки, как дублирование строк или повышение резкости.

3.5 триггер ограничения изображения (CIT): Поле или биты, используемые для подачи на аналоговый выход высокой четкости декодера телевизионных каналов "ограниченного изображения".

3.6 защита контента: Применение технических мер защиты, которые препятствуют незаконному тиражированию и/или повторному распространению контента, доставленного по сети.

3.7 контролируемый контент: Контент, который передан из сети провайдера услуг распространения видеопрограмм с битами индикатора режима шифрования (EMI), установленными в значение, отличное от нулевого (0,0) ("копирование не ограничено").

3.8 информация управления копированием (CCI): Однобайтовое поле, содержащее информацию, которую декодер телевизионных каналов использует для управления копированием контента. Подробнее – см. Приложение A.

3.9 управление цифровыми правами (DRM): Определение, управление и контроль выполнения комплекса правил использования контента. В этих правилах использования указываются такие вещи, как право копирования, просмотра или распределения конкретных блоков контента.

3.10 защита контента при цифровой передаче (DTCP): Метод шифрования, дешифрования, передачи и возобновления ключей, который описывается в спецификации "5C защита контента при цифровой передаче 1.0".

3.11 мост DRM: Объект инфраструктуры и технологии распределительной и домашней сетей, который установлен для обеспечения защиты контента и управления цифровыми правами доставленного по сети контента, который хранится и распространяется в домашней сети.

3.12 биты индикатора режима шифрования (EMI Bits): Два бита, связанных с защищенным контентом, которые определяют какие операции копирования разрешены для соответствующего контента.

3.13 аналоговая форма или выход высокой четкости: Формат или выход, который не является цифровым и имеет разрешение выше, чем разрешение стандартного аналогового сигнала иди выхода.

3.14 широкополосная защита цифрового контента (HDCP): Метод аутентификации, шифрования, дешифрования и возобновления, который описан в спецификации "Система широкополосной защиты цифрового контента, версия 1.1".

3.15 изделие: Устройство и/или технология, которое принимает и, возможно, распределяет контент с управлением распределения и/или управлением копированием.

3.16 правила устойчивости: Правила, описанные в разделе 6, которые применяются к декодерам телевизионных каналов и противостоят попыткам изменить декодеры телевизионных каналов, имеющим цель нарушить правила соответствия техническим условиям.

3.17 услуга: Сигналы изображения, звука и данных, вне зависимости от того, являются ли они аналоговыми или цифровыми, передаваемые по сети провайдера услуг распределения видеопрограмм на (или от) декодер(а) телевизионных каналов, с целью выполнения функций приема или передачи информационного, развлекательного или иного контента.

3.18 декодер телевизионных каналов (STB): Любое устройство, принимающее контент непосредственного от провайдера услуг распространения видеопрограмм, которое содержит как устройства, которые отделены от устройств отображения, так и устройства отображения, которые обладают собственными функциями. STB служит для передачи сигнала услуги в домашнюю сеть и содержит систему условного доступа (CA) и систему управления цифровыми правами (DRM).

3.19 аналоговая форма или выход стандартной четкости: Формат или выход, который не является цифровым (например, PAL RF, NTSC RF, композитный, S-Video, YUV, Y, R-Y, B-Y или RGB) и имеет не более 483 активных строк чересстрочной или прогрессивной развертки.

3.20 система защиты видео контента (VCPS): При выполнении записи шифрованного контента на DVD+RW и DVD+R оптическая цифровая среда защищается технологией VCPS.

3.21 провайдер услуг распределения видеопрограмм (VSP): Провайдер услуг, предлагающий "услугу", определенную в настоящей Рекомендации.

4 Сокращения, акронимы и условные обозначения

В настоящей Рекомендации использованы следующие сокращения:

AES	Улучшенный стандарт шифрования
APS	Аналоговая система защиты
CCI	Информация управления копированием
CGMS-A	Аналоговая система управления числом копий
CIT	Триггер ограниченного изображения
DRM	Управление цифровыми правами
DTCP	Защита контента при цифровой передаче
DVD-RW	Универсальный цифровой диск – перезаписываемый
DVD+R	Универсальный цифровой диск – записываемый
DOCSIS	Спецификация интерфейса передачи данных по кабелю
DVI	Цифровой видеоинтерфейс
EEPROM	Электронно-стираемое программируемое ПЗУ
EMI	Индикатор режима шифрования
HDCP	Широкополосная защита цифрового контента
HDMI	Мультимедийный интерфейс высокой четкости
IP	Протокол Интернет
LSB	Младший бит
MPEG	Группа экспертов по вопросам кинотехники
NTSC RF	Национальный комитет по телевидению – радиочастоты
OOB	Внеполосный
PAL	Строки с переменной фазой
PCI	Интерфейс периферийных устройств
PCMCIA	Международная ассоциация производителей плат памяти для персональных компьютеров
QoS	Качество обслуживания
RF	Радиочастота
RGB	Красный, зеленый, синий
SRM	Системное сообщение о возобновлении
STB	Декодер телевизионных каналов
S-Video	Улучшенное видео
VCPS	Система защиты видео контента
VSP	Провайдер услуг видеопрограмм
WTSA	Всемирная ассамблея по стандартизации электросвязи

5 Обзор

Технология домашних сетей и домашнего приема развилась до такого состояния, что домашняя сеть становится притягательной развлекательной сетью, позволяющей пользователю хранить и распределять контент между различными устройствами, работающими в домашней сети. В интересах данной индустрии – эффективно использовать эту среду для расширения возможностей доставки развлекательных услуг в домашние сети. Поскольку кабельные службы часто работают с высококачественным, защищенным авторским правами контентом, то по ряду причин, определяемых бизнесом и законодательством, возникает необходимость создать механизмы защиты контента и применения соответствующих правил его использования. В настоящей Рекомендации определены требования к мосту управления цифровыми правами, соединяющему кабельную сеть доступа с домашней сетью, в которую оператором сети может быть передан контент многих типов (например, видео, аудио и т. д.), при условии, что этот контент не используется с нарушением каких либо соглашений о предоставлении услуг или требований закона.

5.1 Основные цели

Среди целей создания моста DRM можно отметить следующие:

- Достаточно устойчивый с точки зрения провайдера контента.
- Ненавязчивый с точки зрения абонента.
- Соответствующий нормативно-правовой базе.

5.2 Основные функции

Далее перечислены основные функции моста DRM:

- Аутентификация всех устройств, участвующих в передаче и/или потреблении видео контента.
- Расширение набора бизнес-правил управления цифровыми правами для защиты контента (ограничение числа копий, числа просмотров, ограничение по времени и т. д.), которые были сформулированы как часть декодера телевизионных каналов.
- Шифрование/дешифрование видеоконтента для передачи/потребления.

5.3 Основные технические особенности

Далее перечислены основные технические особенности моста DRM:

- Мост DRM распространяет основные элементы DRM на элементы домашней сети, находящиеся за пределами декодера телевизионных каналов.
- Мост DRM поддерживает передачу и хранение как контента, доставленного кабельным оператором, так и контента, доставленного не кабельным оператором.
- Контент с контролем дальнейшего распространения и копирования может покинуть декодер телевизионных каналов или элементы домашней сети только через определенные выходы.
- Контент без контроля дальнейшего распространения и копирования может использоваться и храниться в декодере телевизионных каналов или элементах домашней сети.
- Контент без контроля дальнейшего распространения и копирования может свободно покинуть декодер телевизионных каналов или элементы домашней сети.

5.4 Основные требования к мосту DRM

G-1	**удобство в использовании**: Мост DRM должен быть прозрачным для абонента, позволяя потреблять и воспроизводить обычный контент без каких либо преград для его использования.
G-2	**простая модель использования**: Мост DRM реализует простую модель использования, позволяющую использовать в домашней сети оплаченный контент, доставленный оператором сети, в соответствии с правами, назначенными этому контенту.
G-3	**защита контента**: Мост DRM должен противостоять незаконной передаче и незаконному копированию защищенного контента вне домашней сети.
G-4	**Защита от пиратов**: Мост DRM должен противостоять пиратам и защищать правила использования контента (например, противостоять краже контента в беспроводной домашней сети с компактно расположенными пользователями).
G-5	**Совместимость с другими технологиями DRM**: Мост DRM не должен препятствовать использованию других технологий защиты контента для контента, доставленного некабельным оператором.
G-6	**независимость от транспорта**: Технология, используемая для создания моста DRM, не должна зависеть от технологий домашней сети.
G-7	**совместимость назад**: Технология моста DRM не должна вредить существующим сетям распределения видеопрограмм.
G-8	**независимость от распределительной сети**: Мост DRM должен поддерживать различные технологии распределительных сетей, включая MPEG радиовещание, передачу IP потоков и FTP.
G-9	**защита в реальном времени**: Технология, используемая для создания моста DRM, должна быть применима для передач в реальном времени (например, для источников сигналов MPEG радиовещания, IP потоков).
G-10	**комплексность**: Технология и процессы моста DRM должны быть совместимы с другими соответствующими промышленными стандартами, такими как DOCSIS (Рекомендации МСЭ-Т J.112/J.122), IPCablecom (Рекомендации МСЭ-Т серий J.16x и J.17x) и IPCable2Home (Рекомен дации МСЭ-Т серий J.19x).
G-11	**открытая спецификация**: Спецификация моста DRM должна позволять взаимодействие оборудования различных производителей.
G-12	**экономическая эффективность**: Стоимость реализации, обслуживания, проверки и соблюдения технологий и процессов моста DRM должна позволять создание эффективных бизнес-моделей.
G-13	**возможность динамического управления**: должна быть предусмотрена возможность динамической конфигурации и управления информацией, используемой для защиты контента.
G-14	**возможность возобновления**: Программное обеспечение безопасности моста DRM должно иметь возможность обновления.
G-15	**работа во время неисправности**: При неисправности доступа к системе условного доступа подача в домашнюю сеть управляемого и неуправляемого контента не должна прекращаться.
G-16	**незащищенный контент**: Мост DRM не должен оказывать влияния на использование незащищенного контента.
G-17	**степень защиты контента**: Для всех видеопередач по домашней сети защита контента должна быть такой, как установлена комплексом правил DRM.
G-18	**расширение комплекса правил DRM**: В DRM представлен богатый набор правил DRM (копирование, воспроизведение, время просмотра и т. д.), и декодер телевизионных каналов должен управлять ими и распространять их на все элементы домашней сети.
G-19	**Аутентификация клиента**: Аутентификация должна поддерживаться для всех элементов домашней сети, участвующих в передаче и/или потреблении видеоконтента.
G-20	**шифрование**: Для всех видеопередач в домашней сети должно применяться шифрование контента.
G-21	**аннулирование устройства**: Должна быть предусмотрена возможность отказа в доступе к контенту конкретному устройству, даже, если это устройство было когда-то элементом сети моста DRM.

5.5 Общие сведения

Когда речь идет о доставке защищенного контента по безопасной распределительной сети, очень важно, чтобы применялась технология для защиты контента от незаконного копирования или повторного распространения. Кроме того, само устройство должно быть надежным и устойчивым к нарушению правил безопасности. В настоящей Рекомендации подробно описываются требования к технологии защиты контента, требования по устойчивости устройства и соответствия техническим условиям для устройств, работающих с защищенным контентом. Эти требования к технологии контента и устойчивости сформулированы с позиции абонентского приемного устройства

(т. е. декодера телевизионных каналов), которое принимает контент от провайдера услуг распространения видеопрограмм, являясь частью кабельной распределительной сети, которая должна защищать ценный контент. Контент шифруется в источнике и защищается в сети провайдера услуг. Целью настоящей Рекомендации является обеспечение необходимого уровня безопасности в домашней сети. Основное внимание в настоящей Рекомендации уделяется надежной и безопасной передаче потока контента в сети более низкого уровня.

Защита контента и технологии с цифровыми выходами, которые позволяют контенту провайдера услуг появиться на выходе декодера телевизионных каналов, должны гарантировать, что провайдер услуг сохраняет за собой контроль копирования и перераспределения этого контента, даже после того, как контент был передан с выхода декодера телевизионных каналов на другое устройство. Устройства домашней сети, расположенные после декодера телевизионных каналов, оборудованные цифровыми выходами, DRM, или технологией защиты контента, также должны подчиняться правилам устойчивости и соответствия техническим условиям, установленным в настоящей Рекомендации для декодера телевизионных каналов. Правила устойчивости и соответствия техническим условиям, установленные для декодера телевизионных каналов, распространяются на всю сеть более низкого уровня.

6 Требования по устойчивости

Устройства, которые принимают и, возможно, распределяют защищенный контент, должны соответствовать целому ряду требований по устойчивости, для того чтобы обеспечить достаточную защиту контента. Общепризнано, что устойчивость может меняться в зависимости от того контента, который передается на устройство, и что может потребоваться изменить устойчивость, поскольку со временем меняется и технология безопасности, и методы взлома такой технологии. В данном разделе описывается общий комплекс рекомендованных требований по устойчивости устройства.

6.1 Конструкция

6.1.1 Общие положения

Изделия должны удовлетворять правилам соответствия техническим требованиям и должны быть разработаны и произведены таким образом, чтобы эффективно противостоять попыткам изменения изделий с целью нарушения правил соответствия техническим требованиям.

6.1.2 Функции защиты

Изделия не должны содержать:

i) переключателей, кнопок, перемычек, специальных соединений, которые можно перерезать, или программных эквивалентов вышеперечисленного; или

ii) сервис-меню или функций (включая функции дистанционного управления),

в каждом случае, представляющем угрозу для технологий защиты контента, аналоговой системы защиты, дополнительной защиты, ограничений по выходным сигналам, ограничений возможности записи, для других обязательных положений правил соответствия техническим требованиям, или в каждом случае, когда контролируемый контент может стать предметом незаконного копирования. В тексте настоящей Рекомендации, термин "дополнительная защита" следует понимать как применение, при необходимости, одобренной технологии защиты контролируемого контента, принятого из распределительной сети видеопрограмм, и передаваемого на выход декодера телевизионных каналов, а также технологии защиты целостности системы и методы, при помощи которых обеспечивается работа этого приложения.

6.1.3 Сохранение тайны

Для того чтобы противостоять попыткам нарушения безопасности со стороны лиц, не имеющих соответствующих полномочий, изделия должны быть разработаны и произведены таким образом, чтобы эффективно противостоять попыткам узнать или обнародовать:

i) индивидуальный номер, имеющий определенную длину битовой посылки, присвоенный каждому декодеру телевизионных каналов, или цифры, используемые в процессе шифрования или дешифрования контролируемого контента (которые называют "Ключами"); и

ii) методы и алгоритмы шифрования, используемые для генерации Ключей.

6.2 Пути распространения контролируемого контента

Контент не должен быть доступен на выходах, отличных от тех, что указаны в правилах соответствия техническим требованиям, и контролируемый контент не должен появляться в нешифрованном, некомпрессированном виде на шинах изделия, доступных пользователю (определенных далее). Аналогично, нешифрованные Ключи, используемые для шифрования и/или дешифрования любого контента, не должны появляться на шинах, доступных пользователю. Термин "шина, доступная пользователю" следует понимать как шину данных, которая разработана так, что конечный пользователь может продолжить ее или получить к ней доступ, например PCI, который имеет разъемы (или является доступным для пользователя), SmartCard, PCMCIA или Cardbus.

6.3 Методы обеспечения устойчивости функций

В изделиях должны использоваться, как минимум, следующие методы обеспечения устойчивости функций и защиты, описанные в настоящей Рекомендации.

6.3.1 Распределенные функции

Блоки изделия, которые выполняют аутентификации и дешифрование, а также MPEG (или аналогичный) декодер должны быть разработаны и произведены так, чтобы для контролируемого контента в любой допускающей использование форме, передаваемого между этими блоками изделия, была обеспечена защита от перехвата и копирования с уровнем, описанным в § 6.3.5.

6.3.2 Программное обеспечение

Любой блок изделия, в котором программно реализуется часть технологии защиты контента, должен включать в себя все характеристики перечисленные в § 6.1 и § 6.2. В тексте настоящей Рекомендации термин "программное обеспечение" следует понимать как реализацию функций, направленных на выполнение требований, определенных в настоящей Рекомендации, при помощи любого программного кода, состоящего из команд или данных, отличных от тех команд или данных, которые реализованы аппаратно. Такие программные реализации должны:

a) Обеспечить соответствие § 6.1.3 любым разумным способом, включая (но не ограничиваясь этим) шифрование, выполнение отдельных участков программы в режиме кольца нулевого уровня или в режиме супервизора, и/или воплощение в форме защищенного физического объекта, и применением в каждом случае создания программного обеспечения эффективных методов противостояния попыткам проникновения под чужим именем или попыткам раскрытия используемых подходов.

b) Разрабатываться так, чтобы выполняли самопроверку целостности блоков своих компонентов, так чтобы незаконные модификации проявлялись как ошибка в выполнения функций аутентификации и/или дешифрования. В тексте этого положения модификация включает в себя любое изменение, искажение или нарушение функций или характеристик, или прерывание работы, в соответствии с § 6.1 и § 6.2. Данное положение требует, по меньшей мере, применения кода с циклическим контролем избыточности, который далее шифруется с секретным ключом или при помощи защищенного алгоритма перемешивания.

c) Соответствовать уровню защиты, описанному в § 6.3.5.

d) Содержать механизмы защиты от незаконных атак на программное обеспечение.

6.3.3 Аппаратура

Любой блок изделия, который аппаратно реализует требования настоящей Рекомендации, должен включать в себя все характеристики перечисленные в § 6.1 и § 6.2. В тексте настоящей Рекомендации термин "аппаратура" следует понимать как физическое устройство, содержащее компоненты, которые реализуют любые требования по защите контента, которым, согласно настоящей Рекомендации, должно отвечать данное изделие, и который:

i) не содержит команд и данных, отличных от тех команд и данных, которые постоянно встроены в это устройство или компонент; или

ii) содержит команды и данные, которые не являются постоянно встроенными в это устройство или компонент, когда такие команды или данные специально разработаны для такого изделия или компонента, и эти команды или данные не становятся доступными для конечного пользователя посредством данного изделия или компонента.

Такие реализации должны:

a) соответствовать § 6.1.3 любым разумным способом, включая (но не ограничиваясь этим): встроенные Ключи, методы генерации Ключей и алгоритмы шифрования в виде микросхем или программно-аппаратных средств, которые невозможно прочесть, или вышеописанные методы для программного обеспечения;

b) разрабатываться так, чтобы попытки перепрограммировать, удалить или заменить элементы аппаратуры способом, который мог бы нарушить безопасность или защиту контента, реализованные в рассматриваемой технологии или в декодере телевизионных каналов, представляли бы серьезный риск повреждения изделия, при котором оно теряет возможность принимать, дешифровать или декодировать контролируемый контент (компонент, которые припаивается, а не присоединяется при помощи разъема);

c) соответствовать уровню защиты, описанному в § 6.3.5.

6.3.4 Гибридное решение

Интерфейсы между аппаратными и программными блоками изделия должны быть разработаны так, чтобы они обеспечивали уровень защиты аналогичный тому, который обеспечивает отдельно аппаратура или отдельно программное обеспечение, как описано выше.

6.3.5 Уровень защиты

Основные функции шифрования (сохранение секретности Ключей, методы генерации Ключей и алгоритмы шифрования, соблюдение правил соответствия техническим условиям и предотвращение копирования и незаконного просмотра расшифрованного контролируемого контента) должны быть реализованы в соответствии с требованиями "Уровня 2" документа FIPS (Федеральный стандарт по обработке информации) 140-2 "Требования по безопасности для криптографических моделей" и, как минимум, способом, при котором они:

a) В соответствии с разумными прогнозами, не могут быть повреждены или обойдены с применением бытовых средств или оборудования, которое широко доступно и недорого, например отвертка, перемычки, кусачки или паяльник ("широко доступные инструменты"), или с применением специальных электронных устройств или специального программного обеспечения, которые широко доступны и недороги, например устройств чтения и записи EEPROM, отладчиков, декомпиляторов или аналогичных инструментов разработки программ ("специальные инструменты"), отличных от тех устройств или технологий, аппаратуры или программного обеспечения, которые специально разработаны и применяются для обхода или обмана механизмов защиты ("устройства обхода"); и

b) Могут быть с трудом нарушены или обмануты с применением профессиональных инструментов или оборудования (за исключением устройств обхода и профессиональных инструментов или оборудования, которые доступны только на условиях соглашений о неразглашении), например анализаторов логических схем, устройств дизассемблирования процессоров, внутрисистемных эмуляторов или других инструментов, оборудования, методов или способов, не включенных в вышеприведенные определения широко доступных и специальных инструментов.

7 Правила соблюдения технических требований

7.1 Введение

Для того чтобы устройство было бы одобрено для подключения к сети провайдера услуг распространения видеопрограмм с целью приема защищенного контента, оно должно соответствовать целому ряду условий.

7.2 Выходные сигналы

7.2.1 Общие положения

Изделие не должно передавать на выход контент или не должно передавать контент, полученный по сети, на любой выход, кроме тех, которые разрешены настоящей Рекомендацией. В тексте настоящей Рекомендации предполагается, что выход включает в себя (но не ограничивается этим) любые устройства передачи для любого внутреннего копирования, записи или хранения, но не включает в себя внутренние незащищенные или транзитные линии передачи, которые удовлетворяют техническим требованиям и правилам устойчивости.

7.2.2 Аналоговые выходы стандартной четкости

Изделия с любыми аналоговыми выходными сигналами стандартной четкости должны иметь на выходе контент, полученный по сети, или передавать контент, полученный по сети, только если контент должным образом защищен в соответствии с национальными или региональными стандартами по защите аналогового контента от копирования.

7.2.3 Аналоговые выходы высокой четкости

Изделия должны иметь возможность, если это установлено значением бита CIT CCI, ограничить степень разрешения контента высокой четкости, так, чтобы он мог быть передан по линии связи, способной переводить аналоговый контент высокой четкости в выходное ограниченное изображение. Изделия должны содержать один или несколько сертифицированных цифровых выходов. Все изделия должны создавать и передавать сигналы триггера CGMS-A для всех аналоговых выходов высокой четкости, но от них не требуется учитывать триггер CGMS-A, кроме тех случаев, когда это соответствует надлежащему законодательству или нормативному акту.

7.2.4 Цифровые выходы

Изделия с любыми цифровыми выходами могут иметь на выходе контент, полученный по сети, или передавать контент, полученный по сети, в соответствии с требованиями настоящей Рекомендации. Перечень технологий, которые были проверены на соответствие настоящей Рекомендации, содержится в Дополнении I.

7.2.5 Метка невмешательства

Изделия и компоненты НЕ ДОЛЖНЫ разрушать, маскировать или препятствовать дешифрации Метки Соглашения в контролируемом контенте.

7.3 Копирование, запись и хранение контролируемого контента

7.3.1 Общие положения

Изделия, содержащие все без ограничений блоки копирования, записи или хранения, не должны копировать, записывать или сохранять контролируемый контент, если это не разрешено в настоящем разделе.

7.3.2 Простой буфер для воспроизведения

Изделия могут временно хранить контролируемый контент с единственной целью обеспечить непосредственное воспроизведение контролируемого контента, при условии, что:

a) такое хранение прекращается после того, как контент был воспроизведен; и

b) данные не хранятся таким образом, который предполагает возможность копирования, записи или хранения этих данных для других целей.

7.3.3 Больше не копировать

Изделия не должны копировать, записывать или хранить контролируемый контент, который обозначен битами EMI, как скопированный, но не разрешенный к дальнейшему копированию ("больше не копировать"), кроме случаев, разрешенных в § 7.3.2 или § 7.3.5.2.

7.3.4 Никогда не копировать

Изделия, содержащие все без ограничений устройства, имеющие возможность записи, например, так называемые, "персональные устройства видеозаписи", не должны копировать контролируемый контент, который обозначен битами EMI, как контент, который никогда не должен копироваться ("никогда не копировать"), кроме случаев, разрешенных в § 7.3.2 или следующих случаев:

Такое устройство может хранить такой контент внутри, например, для реализации функции "пауза" в ходе воспроизведения, если сохраняемый контент передан на изделие, выполняющее запись, безопасным способом, при котором его нельзя оттуда переместить и этот контент не является объектом дальнейшей временной или иной записи внутри изделия до того, как он отмечается, как непригодный к использованию; при условии, что это устройство произведено в соответствии со специфицированными требованиями по устойчивости с целью предотвращения нарушения этих ограничений. При внутреннем сохранении такого контента, включая хранение для реализации функции "пауза", разрешенное в данном разделе, контент должен шифроваться и храниться в таком виде, который обеспечивает безопасность не хуже, чем обеспечивается 128-битовым улучшенным стандартом шифрования (AES).

Изделия должны быть разработаны и произведены так, чтобы они имели возможность уничтожать сохраненный контент или по прошествии определенного периода времени отмечать сохраненный контент, как непригодный к использованию (покадрово, поминутно, помегабайтно).

7.3.5 Создание одной копии

7.3.5.1 Функция копирования

Изделия могут создавать копию контролируемого контента, который отмечен битами EMI, как разрешенный к однократному копированию ("разрешено создание одной копии"), как предусмотрено в § 7.3.2 или § 7.3.4 или. При условии, что эта копия:

a) в каждом случае скремблирована, зашифрована или уникальным образом связана с этим устройством, с применением той формы защиты от копирования, которая определена в приложении к § 7.3.5, если таковая имеется; и

b) отмечена, как запрещенная к дальнейшему копированию ("более не копировать") способом, который идентичен определенному в приложении к § 7.3.5, если таковой имеется, и сможет эффективно предотвращать дальнейшее копирование контента устройствами, способными принимать передачу таких отмеченных данных на выходах, определенных в § 7.2.4. В отсутствии любого из таких дополнений к § 7.3.5, не может быть сделано ни одной копии этого контролируемого контента, отличных от тех, что разрешены в § 7.3.2 или § 7.3.4, за исключением указанных в § 7.3.5.2.

7.3.5.2 Функция перемещения

Изделие, которое делает копию контента, отмеченного в поле CCI как "разрешено создание одной копии" в соответствии с § 7.3.5, может переместить этот контент на одно съемное устройство записи, или на одно внешнее устройство записи, только когда:

a) внешнее устройство записи показывает, что ему разрешено выполнить эту функцию перемещения в соответствии с требованиями настоящего раздела и копировать этот контролируемый контент в соответствии с требованиями § 7.3.5;

b) этот контролируемый контент отмечен создавшим его устройством, для передачи с меткой "разрешено создание одной копии";

c) контролируемый контент является выходным сигналом на защищенном выходе в соответствии с § 7.2.2, § 7.2.3 или § 7.2.4;

d) до того, как будет выполнено перемещение контента, устройство, создавшее запись, отмечается как непригодное к использованию и перемещаемый контролируемый контент отмечается "как более не копировать";

e) устройство, на которое перемещается съемное устройство записи неспособно или отмечено как неспособное передать контролируемый контент на выход, за исключением тех выходов, которые разрешены правилами соблюдения технических условий; и

f) копия сохраняется:

i) с использованием протокола шифрования, одобренным в приложении к правилам соблюдения технических условий, который уникальным образом связывает эту копию с одним-единственным устройством, так, что она не может быть воспроизведена на другом устройстве или, если она сохранена на съемном носителе, так, что с него более не может быть сделано пригодных к использованию копий; или

ii) в противном случае с применением методов, описанных в § 7.3.5.1.

Современный вариант реализации ограничивает количество перемещений до одного перемещения. Дополнительные средства управления контентом находятся в стадии изучения и смогут применяться после того, как будут определены системы DRM следующего поколения.

8 Контроль за изменениями

Любые материальные или заметные изменения технологии требуют оценки с использованием описанных здесь критериев и процедуры. Материальные или заметные изменения включают в себя (но не ограничиваются этим):

1) преобразование в новые средства или среду передачи;

2) изменения в кодировании или обработке контента;

3) изменения, которые могут оказать материальное и неблагоприятное воздействие на целостность или безопасность технологии;

4) изменения в используемом методе криптографии (кроме случаев, когда алгоритм остается неизменным, и только увеличивается длина Ключа);

5) изменения в условиях повторного распределения; и

6) любые фундаментальные изменения в природе технологии.

Приложение A

Информация управления копированием

Информация управления копированием (CCI) передается от провайдера услуг распределения видеопрограмм по каналу передачи данных, для того чтобы сообщить декодеру телевизионных каналов о требуемом уровне защиты от копирования. CCI передается в виде, понятном для декодера телевизионных каналов, но целостность информации поддерживается путем аутентификации битов CCI с использованием простого протокола. Это процесс повторяется для каждого элемента домашней сети после декодера телевизионных каналов.

Однобайтовое поле CCI содержит информацию, которую декодер телевизионных каналов и дальнейшие элементы используют для управления копированием контента. Два бита EMI управляют копированием на цифровых выходах декодера телевизионных каналов, два бита APS управляют копированием на аналоговых выходах, один бит служит триггером ограниченного изображения, три бита являются резервными.

A.1 Переключение канала

Когда происходит переключение канала, декодер телевизионных каналов должен рассматривать весь CP-скремблированный контент так, как если бы биты EMI имели значение "никогда не копировать", но не должен использовать ограничения изображения, пока не будет получено новое сообщение CCI. После получения от провайдера услуг распределения видеопрограмм значений битов CCI, декодер телевизионных каналов должен сразу же начинать их использовать. Если в течение 10 секунд новое CCI сообщение не было принято, то декодер телевизионных каналов должен применить функцию ограничения изображения, как если бы бит CIT был бы равен единице. Переключение канала не должно приводить к обновлению Ключа.

A.2 Определение CCI

CCI – это однобайтовое (8-битовое) поле, передаваемое от декодера телевизионных каналов на элементы домашней сети. Пять из восьми битов уже определены. Оставшиеся три являются резервными. Резервные биты должны быть установлены в ноль, как показано в таблице A.1. Элементы, расположенные в домашней сети после декодера телевизионных каналов, должны использовать значения резервных битов, принятых от декодера телевизионных каналов, только для выполнения описанного далее аутентифицированного туннельного протокола. После этого декодер телевизионных каналов должен игнорировать резервные биты.

Таблица A.1/J.197 – Назначение битов CCI

№ битов CCI	7	6	5	4	3	2	1	0
VSP устанавливает в	0	0	0	CIT	APS1	APS0	EMI1	EMI0
STB понимает как	резерв	резерв	резерв	CIT	APS1	APS0	EMI1	EMI0

A.3 EMI – биты управления цифровым копированием

Для младших битов байта CCI – это биты EMI. Они должны управлять разрешениями цифрового копирования. Биты EMI должны подаваться на все цифровые выходные порты декодера телевизионных каналов для управления копиями, сделанными на этих выходах. Биты EMI определяются в таблице A.2.

Таблица A.2/J.197 – Значение EMI и контент

Значение EMI	Разрешение цифрового копирования	Тип контента
00	Копирование не ограничено	не "ценный"
01	Дальнейшее копирование не разрешено	ценный
10	Разрешено сделать одну копию	ценный
11	Копирование запрещено	ценный

A.4 APS – аналоговая система защиты

Биты 3 и 2 в поле CCI, как показано в таблице A.1, являются битами аналоговой системы защиты (APS). Декодер телевизионных каналов должен использовать биты APS для кодирования сигналов управления защиты от копирования аналоговых композитных выходных сигналов, как показано в таблице A.3.

Таблица A.3/J.197 – Определение значений битов APS

APS	Описание
00	Отключен код защиты от копирования
01	Включена обработка AGC, разделение отключено
10	Включена обработка AGC, 2-строчное разделение включено
11	Включена обработка AGC, 4-строчное разделение включено

A.5 CIT – триггер ограниченного изображения

Бит 4 байта CCI, как показано в таблице A.4, это бит CIT. Декодер телевизионных каналов должен использовать бит CIT для управления ограничением изображения аналоговых компонентных выходных сигналов высокой четкости.

Таблица A.4/J.197 – Значения и применение CIT

Значение CIT	Применение ограничения изображения
0	Никаких ограничений изображения не накладывается
1	Требуется ограничение изображения

A.6 Аутентифицированный туннельный протокол

Декодер телевизионных каналов рассчитывает значение CCI_auth, используя принятое значение CCI, сравнивает его со значением CCI_auth, принятым от провайдера услуг распределения видеопрограмм. Отсутствие равенства этих значений означает появление ошибки, и декодер телевизионных каналов устанавливает EMI = 11 и применяет ограничение изображения, так, если бы это значение было бы = 1.

Приложение B

Перечень вопросов по проверке устойчивости

До выпуска любого изделия, разработчик технологии должен провести испытания и анализ с целью убедиться в устойчивости реализации. Приведенный ниже перечень вопросов по проверке устойчивости может использоваться, как руководство для разработчика по проведению испытаний, охватывающих определенные важные аспекты устойчивости. Поскольку перечень вопросов по проверке устойчивости не учитывает всех элементов, необходимых для производства изделия, отвечающего всем требованиям, разработчику настоятельно рекомендуется в своих испытательных процедурах тщательно оценить соответствие его изделия техническим требованиям.

Общие вопросы реализации

1) Было ли изделие разработано и произведено так, что в нем нет никаких переключателей, кнопок, перемычек или программных эквивалентов перечисленного или специальных соединений, которые можно перерезать, при помощи которых могут быть нарушены технологии защиты контента, аналоговые системы защиты, ограничения по выходным сигналам, ограничения возможностей записи, или другие обязательные положения правил соответствия техническим требованиям или при помощи которых контролируемый контент может оказаться незащищенным от незаконного копирования?

2) Было ли изделие разработано и произведено так, что в нем нет никаких сервис-меню и никаких функций (таких, как функции дистанционного управления, коммутаторы, переключатели и другие средства), которые могут перехватить поток контролируемого контента или подвергнуть его незаконному копированию?

3) Было ли изделие разработано и произведено так, что в нем нет никаких сервис-меню и никаких функций (таких как функции дистанционного управления, коммутаторы, переключатели и другие средства), которые могут отключить любые аналоговые системы защиты, ограничения по выходным сигналам, ограничения возможностей записи, или другие обязательные положения правил соответствия техническим требованиям?

4) Имеет ли изделие сервис-меню, сервисные функции или сервисные возможности, которые могут изменить или раскрыть поток контролируемого контента внутри устройства?

   Если "Да", пожалуйста, опишите эти сервис-меню, сервисные функции или сервисные возможности, а также меры, которые были предприняты для обеспечения того, чтобы эти сервисные инструменты не использовались для раскрытия или неверной маршрутизации контролируемого контента.

5) Имеет ли изделие сервис-меню, сервисные функции или сервисные возможности, которые могут отключить любые аналоговые системы защиты, ограничения по выходным сигналам, ограничения возможностей записи, или другие обязательные положения правил соответствия техническим требованиям?

   Если "Да", пожалуйста, опишите эти сервис-меню, сервисные функции или сервисные возможности, а также меры, которые были предприняты для обеспечения того, чтобы эти сервисные инструменты не использовались для противодействия процессам шифрования изделия (включая выполнение правил соответствия техническим требованиям).

6) Имеет ли изделие какие-либо доступные для пользователя шины (определенные в § 6.2 правил устойчивости)?

   Если да, то передается ли по этой шине контролируемый контент?

   Если да, то:

   Назовите и опишите шину, и укажите, является ли контролируемый контент компрессированным или не компрессированным. Если эти данные компрессированы, подробно опишите, как и какими средствами эти данные дешифруются, как того требует § 6.2 правил устойчивости.

7) Подробно объясните, как изделие обеспечивает секретность всех Ключей.

8) Подробно объясните, как изделие обеспечивает секретность конфиденциальных алгоритмов шифрования, используемых в изделии.

9) Если изделие передает контролируемый контент от одного блока изделия на другой, либо между модулями программного обеспечения, интегральными схемами или между ними в любой комбинации, объясните, как были разработаны, связаны и объединены друг с другом блоки, выполняющие аутентификацию и дешифрование, а также MPEG (или аналогичный) декодер, так, чтобы контролируемый контент оставался защищенным от перехвата и копирования как того требует § 6.3.1 правил устойчивости.

10) Реализуются ли в аппаратуре какие-либо функции защиты контента?

Если да, ответьте на вопросы о реализации аппаратуры.

11) Реализуются ли в программном обеспечении какие-либо функции защиты контента?

Если да, ответьте на вопросы о реализации программного обеспечения.

Вопросы по реализации программного обеспечения

12) Для данного изделия опишите метод, при помощи которого все Ключи хранятся в защищенном виде.

13) Способны ли вы, используя утилиту grep или эквивалентную ей, раскрыть какие-либо Ключи в виде бинарных изображений любого устройства с перехватом памяти?

14) Для данного изделия опишите метод, используемый для скрытия секретных алгоритмов шифрования и программно реализованных Ключей.

15) Для данного изделия опишите метод, при помощи которого создаются и хранятся в защищенном виде промежуточные криптографические значения (например, полученные в ходе процесса аутентификации между модулями или устройствами в составе изделия).

16) Опишите метод, используемый для предотвращения применения широкодоступных инструментов отладки и декомпиляции (например, Softice) для пошагового запуска, декомпиляции или анализа работы функций защиты, реализованных в программном обеспечении.

17) Опишите метод, при помощи которого изделие выполняет такую самопроверку блоков компонентов, что любые изменения будут приводить к отказу в авторизации или дешифровании, как описано в § 6.3.2b правил устойчивости. Опишите, что случится, если целостность нарушается.

18) Для гарантии того, что самопроверка выполняется, проведите испытание, которое подтвердило бы, что выполнение программы прекращается, как только начинает использоваться редактор битов для изменения случайного байта исполнимого модуля, содержащего функции защиты контента, а также опишите метод и результаты такой проверки.

Вопросы по реализации аппаратуры

19) Для данного изделия опишите метод, при помощи которого все Ключи хранятся в защищенном виде и укажите, как поддерживается их секретность.

20) Способны ли вы, используя утилиту grep или эквивалентную ей, раскрыть какие-либо Ключи в виде бинарных изображений любого устройства с перехватом памяти?

21) Для данного изделия опишите, как схемно или программно-аппаратно реализованы конфиденциальные алгоритмы шифрования так, что их невозможно прочесть.

22) Для данного изделия опишите метод, при помощи которого создаются и хранятся в защищенном виде промежуточные криптографические значения (например, полученные в ходе аутентификации между модулями или устройствами в составе изделия).

23) Опишите средства, используемые для предотвращения попыток заменить, удалить, или исказить элементы или модули аппаратуры, используемые для выполнения функций защиты?

24) Приведет ли удаление или замена аппаратных элементов данного изделия, ставящие под угрозу возможности изделия по защите контента (включая правила соответствия техническим условиям и правила устойчивости), к повреждению изделия, при котором оно будет неспособно принимать, дешифровать или декодировать контролируемый контент?

Дополнение I

Цифровые выходы

Нам потребуется протестировать цифровые выходы на соответствие требованиям, установленным в настоящей Рекомендации. Далее для сведения приведен перечень цифровых выходов, которые были протестированы на соответствие настоящей Рекомендации. Ожидается, что в будущем все дополнительные выходы будут отвечать требованиям настоящей Рекомендации.

I.1 Лаборатория кабельного телевидения протестировала следующий выход и подтвердила его соответствие настоящей Рекомендации:

- **1394 с DTCP**: Изделие может принимать контролируемый контент и передавать контролируемый контент на выход в цифровом виде через интерфейсы IEEE 1394, когда этот выход защищен при помощи DTCP. Изделие должно поддерживать режим DTCP "полная аутентификация" и может дополнительно поддерживать режим DTCP "ограниченная аутентификация". Если требуется применяемой для DTCP лицензией, контент, который *не является* контролируемым контентом, должен подаваться на выход IEEE 1394 без защиты DTCP.

I.2 Лаборатория кабельного телевидения протестировала следующий выход и подтвердила его соответствие настоящей Рекомендации:

- **DVI/HDMI с HDCP**: Изделие может получать контент, принятый от сети и передавать полученный контент на выход, в цифровом виде через интерфейсы DVI, включая интерфейсы HDMI и на выходе которого всегда стоит HDCP, который всегда включен. Изделие должно передавать законно принятые биты HDCP SRM на функцию HDCP.

Дополнение II

Критерии проверки

В зависимости от конкретного выхода и применяемой технологии, критерии для оценки должны включать в себя следующие позиции:

II.1 Транспортировка видеосигнала

Используются ли стандартизованные методы для передачи и доставки CCI от декодера телевизионных каналов в предлагаемые условия работы или профиль устройства?

i) *Компрессированные цифровые выходы*

- Используется ли на интерфейсе исходный компрессированный цифровой сигнал системы, или сигнал де-компрессирован?
- Если сигнал де-компрессирован, то какие требуются система, профиль, разрешение и скорости передачи данных?
- Если сохраняется исходная компрессия, то передается ли через интерфейс полный мультиплексированный транспортный поток, или интерфейс ограничен передачей отдельных программных потоков после демультиплексирования?
- Если на выход передается полный транспортный поток, как передается системная информация (например, внеполосные данные)?
- Какие методы используются для обеспечения передачи через этот интерфейс непрерывного потока программ, вне зависимости от остального трафика, который может быть представлен на интерфейсе (QoS)?
- Какова минимальная гарантированная пропускная способность интерфейса?
- Какие методы используются для доставки, декодирования или воспроизведения аналоговых и цифровых данных субтитров, справочных рейтинговых данных контента и внутриполосных сообщений оповещение об аварийной ситуации?
- Как на этом интерфейсе сохраняется "бесшовная" передача аналоговых программ?

ii) *Некомпрессированные цифровые выходы*

- Какова минимальная гарантированная пропускная способность интерфейса?
- Как на этом интерфейсе сохраняется "бесшовная" передача аналоговых программ?
- Какие методы используются для доставки, декодирования или воспроизведения аналоговых и цифровых данных субтитров, справочных рейтинговых данных контента и внутриполосных сообщений об аварийной ситуации?

II.2 Интерфейсы безопасности

- Как используется система безопасности при транспортировке видеосигнала, и как транспортировка связана с профилями защиты контента, методами аутентификации и профилями защиты контента?
- Какие используются методы для генерации, защиты и передачи ключей?
- Известны ли участки, на которых контент находится в незащищенном состоянии?

II.3 Точки атаки и слабые стороны системы

- Может ли технология быть обойдена на каком-то участке?
- Где расположены самые слабые преграды атаке?
- Где хакер будет атаковать и какие ресурсы требуются?
- Каковы возможные слабые стороны/угрозы и каков компромисс между безопасностью и затратами?

II.4 Эффективность предлагаемой технологии

- В достаточной ли мере технология защищает контент, передаваемый через цифровой выход и записываемый или хранимый в защищенном виде для дальнейшего воспроизведения?
- Какова область дальнейшего распределения контента? Эффективно ли защищают контент цифровой выход или технология DRM от незаконного распространения за счет применения управления местонахождением, других ограничений по географической зоне или пользователям?

II.5 Обеспечение безопасности

- Защищены ли ключи и секреты от прочтения и записи в ходе криптографических вычислений?
- Защищены ли системным дизайном биты CCI, ограничения изображения и другие механизмы управления?

II.6 Аннулирование и возобновление ключей

- Имеет ли изделие возможность аннулирования ключа?
- Имеет ли изделие возможность возобновления ключа?
- Какие критерии и процессы используются для аннулирования и возобновления? Кто участвует в процессе?
- Каков минимальный размер системного сообщения о возобновлении (SRM) и в каком формате оно доставляется?
- Каким образом обычно доставляется SRM? Какое влияние оказывает решение по аннулированию/возобновлению на работу и инфраструктуру сети провайдера услуг распространения видеопрограмм (включая обновление производственного оборудования или сети, которые могут потребоваться)? Что должен сделать провайдер услуг распространения видеопрограмм, для того чтобы реализовать предлагаемые решения аннулирования и возобновления?

II.7 Новые алгоритмы

- Какова относительная сила алгоритма?
- Какова относительная сила аутентификации по отношению к другим технологиям?

II.8 Сохранение целостности услуги

- Мешают ли предлагаемые выходы/технология работе устройства декодера телевизионных каналов, отвечающего другим требованиям лицензирования или тестирования? Требуется ли для предлагаемого цифрового выхода переключение аналогового источника или ретранслятор высокой четкости?
- Обеспечивает ли выход возможность сохранить пользовательские навигационные и сервисные приложения провайдера услуг?
- Мешают ли предлагаемые выходы/технология работе других коммерчески доступных устройств и интерфейсов?
- Возникают ли проблемы взаимодействия предлагаемых выходов/технологии с другими коммерчески доступными устройствами и интерфейсами?
- Способен ли предлагаемый интерфейс взаимодействовать с изделиями других производителей или он представляет собой патентованное или, другими словами, эксклюзивное решение?
- Определен ли порядок взаимодействия промышленными стандартами (какими?) или лицензией, или обоими?
- Требуется ли для гарантии взаимодействия выполнения испытаний на соответствие технологии техническим условиям?

II.9 Условия лицензирования

- Условия лицензирования должна соответствовать положениям МСЭ и национальным требованиям.

II.10 Общее воздействие на сеть распределения видеопрограмм

- Какое влияние оказывает предлагаемая технология на работу и инфраструктуру распределительной сети видеопрограмм (включая обновление производственного оборудования или сети, которые могут потребоваться)?
- Что должен сделать провайдер услуг распространения видеопрограмм для реализации предлагаемого технологического решения?

Дополнение III

Элементы проверки представленных технологий

Технологии, охватываемые этим рекомендованным процессом оценки, включают в себя защищенные цифровые интерфейсы, безопасные запись, хранение и воспроизведение контента, а также управление цифровыми правами. Конкретные меры безопасности, используемые этими технологиями, могут меняться. Кроме того, различные технологии выходов могут использовать механизмы и протоколы транспортировки, которые требуют определенных ограничений, накладываемых на их работу или реализацию. В данном Дополнении определяется несколько ключевых элементов, которые должны быть общими для всех рассматриваемых технологий-кандидатов, но не приводится исчерпывающий перечень, не позволяющий применять другие типы информации, которые могут быть необходимы, для того чтобы полностью оценить конкретную технологию. Представляемые технологии не должны исключать или неправильно истолковывать спецификации материалов, факты или другие подробности, необходимые для выполнения тщательной и точной проверки технологии.

Рассматриваемые технологии могут содержать смесь технологических элементов защищенных цифровые интерфейсов, безопасных записи, хранения и воспроизведения контента, а также управления цифровыми правами. В последующих параграфах описываются рекомендованные элементы, которые должны быть представлены для тщательной проверки технологий-кандидатов.

III.1 Условия лицензирования

Условия лицензирования должна соответствовать положениям МСЭ и национальным требованиям.

Замечание по Устойчивости и Правилам соблюдения технических требований. – Устройства, расположенные в домашней сети после декодера телевизионных каналов, которые содержат любые цифровые выходы, DRM, или технологию защиты контента, также должны соответствовать правилам устойчивости и правилам соблюдения технических требований, установленным в настоящей Рекомендации для декодера телевизионных каналов. Правила устойчивости и правила соблюдения технических требований, установленные для декодера телевизионных каналов, относятся ко всей остальной системе домашней сети после декодера. В результате, правила устойчивости и правила соблюдения технических требований, указанные в лицензии производителя любой технологии, не должны противоречить правилам устойчивости и правилам соблюдения технических требований условий, подробно описанным в настоящей Рекомендации.

III.2 Обзор безопасности

Спецификация и документация по безопасности должны содержать введение и обзор безопасности, в котором должна быть приведена следующая информация:

1) Описание архитектуры безопасности, ее компонентов (например, сервер упаковки, сервер обмена лицензиями, клиент и т. д.), их функций и ключевых интерфейсов; требования к соединительным линиям для выхода/безопасности.
2) Подробную блок-схему архитектуры безопасности, на которой указаны ключевые компоненты и интерфейсы, необходимые для реализации сквозного решения, включая приемник и другие элементы среды передачи (компьютеры, память, дисплей и т. д.).
3) В этом обзоре также должно быть четко указаны возможности по транспортировке видеосигнала, для которых имеются альтернативные варианты реализации. Например, алгоритмы кодировки транспортируемого видеосигнала (AES, 3-DES и т. д.) и алгоритмы обмена ключами (Diffie-Hellman, RSA и т. д.).
4) Подробное описание соответствия правил и лицензий по защите контента на декодере телевизионных каналов, предлагаемой технологии защиты контента, которая должна быть реализована в устройствах домашней сети после декодера, в частности, рассмотрение проблемы обеспечения общей безопасности и защиты контента в распределительной абонентской сети.

III.3 Транспортировка видеосигнала

Спецификация безопасности должна содержать подробное описание метода транспортировки видеосигнала и сведения о том, как информация управления копированием (CCI), представленная декодером телевизионных каналов, транслируется в предлагаемые условия/профиль. Эта

спецификация должна также подробно описывать, как связана транспортировка видеосигнала с любыми профилями защиты контента и методами аутентификации и безопасными профилями защиты контента.

Кроме того, должны быть представлены спецификации или другие технические описания, которые бы полностью объясняли, как предлагаемый цифровой выход поддерживает один или несколько протоколов транспортировки, позволяющих доставлять все определенные[1] аудиовизуальные услуги, связанные с декодером телевизионных каналов, без прерывания, задержки или искажения доставки таких услуг на оконечное устройство отображения. Такие услуги также включают в себя (но не ограничиваются этим) доставку, декодирование или отображение аналоговых и цифровых данных субтитров, справочных рейтинговых данных контента и сообщений об аварийной ситуации.

Проверка технологии должна быть выполнена для каждого механизма и протокола транспортировки, охватываемого технологий защиты контента. Такие проверки должны выполняться для каждого варианта транспортировки и для каждой среды передачи. Если определенная технология полностью соответствует приведенным критериям, то не следует считать, что такая технология получила "глобальное одобрение" для любого варианта и протокола транспортировки.

III.4 Профили защиты контента

Спецификация безопасности должна содержать подробное описание формата и правил использования всех профилей защиты контента с цифровой подписью, применяемых в системе. Спецификация безопасности должна также определять структуру и возможности, которые реализованы в данной системе, а также все сообщения и сигнализацию, необходимые для данной реализации.

III.5 Алгоритмы обмена ключами

Спецификация безопасности должна содержать подробное описание аутентификации приемных устройств, устройств хранения и всех устройств, соединенных с ними. Спецификация безопасности должна также перечислять методы аутентификации сервера лицензий, сервера упаковки и клиента. Для полной проверки должны быть определены все передаваемые в ходе сеанса связи ключи и используемые криптографические протоколы. Могут быть реализованы также и варианты без шифрования, они также должны быть подробно объяснены.

III.6 Интерфейсы безопасности

Спецификация должна содержать подробности, которые полностью определяют интерфейсы безопасности всей системы, а также создание и защиту симметричных и асимметричных ключей. Для полной проверки интерфейсов безопасности должно быть приведено подробное описание аппаратно и программно реализованных компонентов обеспечения безопасности.

III.7 Обеспечение безопасности

Спецификация должна содержать подробности, которые показывают, как ключи и секреты защищены от прочтения и записи в ходе криптографических вычислений и как защищены в системе биты CCI, ограничения изображения и другие параметры.

III.8 Управление сертификатами

Спецификация должна содержать подробности, которые полностью определяют использование сертификатов, методы защиты секретных ключей, методы аннулирования ключей. А также как сертификаты связаны с контентом и серверами упаковки/лицензий. В спецификацию должны быть также включены подробные данные об установке, подписании, обращение к главному администратору, а также об общей структуре, подтверждении безопасности и защите сертификатов от фальсификации.

---

[1] См., например, ANSI/SCTE40-2004; Раздел 8.1.

III.9 Аннулирование/возобновление ключа

Спецификация должна содержать подробные данные о том, как системы выполняет аннулирование и возобновление ключа.

III.10 Точки атаки/возможные слабые места

Спецификация должна содержать описание и анализ возможных угроз для проверки возможных слабых мест/угроз и нахождения компромисса с возможной стоимостью. Кроме того, должна быть выполнена независимая проверка безопасности. При необходимости, для засекречивания результатов такой проверки могут быть наложены ограничения по неразглашению.

III.11 Коммерческое использование

Представленные данные должны содержать описание всех известных вариантов коммерческого использования предлагаемых выхода и технологии, а также все известные способы влияния на качество работы устройств и проблемы взаимодействия. Заявитель должен представить список пользователей (разработчиков) и сторонников (владельцев, разработчиков контента и т. д.) и указать любые коммерческие взаимоотношения между разработчиком технологии и владельцами контента.

III.12 Контактная информация

Представленные данные должны содержать имена и контактную информацию для специалистов в области безопасности и других физических лиц, с кем можно связаться по вопросам, касающимся представленного материала.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	**Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов**
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2006 г.