



МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1191

(02/2009)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасные приложения и услуги – Безопасность IPTV

**Функциональные требования и архитектура
аспектов безопасности IPTV**

Рекомендация МСЭ-Т X.1191

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X
СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1191

Функциональные требования и архитектура аспектов безопасности IPTV

Резюме

В Рекомендации МСЭ-Т X.1191 рассматриваются функциональные требования, архитектура и механизмы, связанные с аспектами безопасности контента, услуг, сетей, оконечных устройств и абонентов (конечных пользователей) IPTV.

Источник

Рекомендация МСЭ-Т X.1191 была утверждена 20 февраля 2009 года 17-й Исследовательской комиссией МСЭ-Т (2009–2012 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

Ключевые слова

Аутентификация, санкционирование, шифрование, IPTV, защита неприкосновенности частной жизни, безопасность, архитектура безопасности, скремблирование, защита услуг и контента.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). 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 осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: <http://www.itu.int/ITU-T/ipr/>.

© ITU 2009

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

	Стр.
1 Сфера применения	1
2 Справочные документы	1
3 Термины и определения	1
3.1 Термины, определенные в других документах	1
3.2 Термины, определенные в настоящей Рекомендации	2
4 Сокращения и акронимы	4
5 Условные обозначения	5
6 Требования безопасности	6
6.1 Общие требования безопасности	6
6.2 Требования безопасности контента	6
6.3 Требования к защите услуг	8
6.4 Требования к безопасности сети	10
6.5 Требования к безопасности оконечного устройства	11
6.6 Требования к безопасности абонентов	12
7 Архитектура безопасности	12
7.1 Общая архитектура безопасности	13
7.2 Архитектура защиты контента	14
7.3 Архитектура защиты услуг	17
7.4 Описание функций и функциональных блоков архитектуры безопасности IPTV	19
8 Механизмы безопасности	21
8.1 Механизмы безопасности, обеспечивающие защиту контента	21
8.2 Механизмы безопасности, обеспечивающие защиту услуг	223
8.3 Механизмы безопасности, обеспечивающие защиту сети	23
8.4 Механизмы безопасности, обеспечивающие защиту оконечных устройств	23
8.5 Механизмы безопасности, связанные с абонентами или конечными пользователями	24
Приложение А – Защита безопасности абонентов	25
А.1 Защита конфиденциальности пользователей	25
А.2 Родительский контроль, защита юридически несовершеннолетних, управление доступом	26
Дополнение I – Угрозы безопасности	27
I.1 Модель угроз безопасности	27
Дополнение II – Взаимодействие SCP	30
II.1 Обзор взаимодействия SCP	30
II.2 Сценарии взаимодействия SCP	30
II.3 Технические области функциональной совместимости SCP	31
II.4 Архитектуры взаимодействия SCP	32
II.5 Сценарии, при которых SCP-B или SCP-IX размещены в оконечном устройстве	33

	Стр.
Дополнение III – Пример процесса защиты контента IPTV	35
Дополнение IV – Управление защитой и копированием контента DVB	36
IV.1 Введение	36
IV.2 Определения	36
IV.3 Сокращения	37
IV.4 Архитектура CPCM	38
IV.5 Эталонная модель CPCM и функциональные составляющие	39
IV.6 Санкционированная область CPCM	39
IV.7 Правила использования контента CPCM	40
IV.8 Метаданные информации о состоянии использования	40
IV.9 Контент CPCM	40
IV.10 Устройство CPCM	40
IV.11 Правило использования и информация о состоянии использования	40
Дополнение V – Схема безопасного транскодирования	41
V.1 Обзор схемы безопасного транскодирования	41
Библиография	42

Введение

Услуги IPTV, контент, доставляемый при помощи таких услуг, оконечные устройства, используемые для его обработки, а также предоставление таких услуг – все это требует учета многих аспектов безопасности. В настоящей Рекомендации содержатся требования, архитектурные модели, функциональные объекты, интерфейсы, механизмы и дополнительные информативные справочные материалы, в которых описываются и рассматриваются указанные аспекты безопасности.

Рекомендация МСЭ-Т Х.1191

Функциональные требования и архитектура аспектов безопасности IPTV

1 Сфера применения

В данной Рекомендации рассматриваются функциональные требования, архитектура и механизмы, связанные с аспектами безопасности и защиты контента, услуг, сетей, оконечных устройств и абонентов IPTV. Предполагается, что требования и соответствующие функции, определенные в настоящей Рекомендации, могут применяться в соответствии с услугами и бизнес-моделями IPTV, для которых могут требоваться различные уровни функций безопасности.

2 Справочные документы

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники являются предметом пересмотра, поэтому всем пользователям данной Рекомендации предлагается рассмотреть возможность применения последнего издания Рекомендаций и других ссылок, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т публикуется регулярно. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус рекомендации.

[ITU-T X.509] Рекомендация МСЭ-Т Х.509 (2008 г.) / ИСО/МЭК 9594-8:2008, *Информационные технологии – Взаимосвязь открытых систем – Справочник: Структуры сертификатов открытых ключей и атрибутов.*

[ITU-T Y.1910] Recommendation ITU-T Y.1910 (2008), *IPTV functional architecture.*

3 Термины и определения

3.1 Термины, определенные в других документах

В данной Рекомендации используются следующие термины, определенные в других документах.

3.1.1 управление доступом (access control) [b-ITU-T X.800]: Предотвращение несанкционированного использования ресурса, включая предотвращение использования ресурса несанкционированным образом.

3.1.2 приложение (application) [b-ITU-T Y.101]: Структурированный набор возможностей, которые обеспечивают выполнение приносящих дополнительный доход функций, поддерживаемых в одной или нескольких услугах.

3.1.3 аутентификация (authentication) [b-ITU-T X.800]: См. определение терминов "аутентификация источника данных" и "аутентификация одноранговых объектов".

3.1.4 санкционирование (authorization) [b-ITU-T X.800]: Предоставление прав, включая предоставление доступа на основе прав доступа.

3.1.5 готовность (availability) [b-ITU-T X.800]: Способность быть доступным и годным к использованию по запросу санкционированного объекта.

3.1.6 конфиденциальность (confidentiality) [b-ITU-T X.800]: Свойство, в соответствии с которым информация не доступна и не раскрывается несанкционированным лицам, организациям или процессам.

3.1.7 аутентификация источника данных (data origin authentication) [b-ITU-T X.800]: Подтверждение того, что источником принятых данных является именно тот, кто заявлен.

3.1.8 отказ в обслуживании (denial of service – DoS) [b-ITU-T X.800]: Предотвращение санкционированного доступа к ресурсам или затягивание критических по времени операций.

3.1.9 цифровая подпись (digital signature) [b-ITU-T X.800]: Добавленные данные к блоку данных или криптографическое преобразование (см. криптография) блока данных, позволяющее получателю этого блока данных убедиться в источнике и целостности блока данных, а также защищающее от подделки, например, со стороны получателя.

3.1.10 элементарный поток (elementary stream) [b-ITU-T H.222.0]: Общий термин для кодированного видеосигнала, кодированного аудиосигнала или других двоичных потоков, кодированных в виде PES пакетов.

ПРИМЕЧАНИЕ. – PES означает пакетированный элементарный поток.

3.1.11 функциональная архитектура (functional architecture) [b-ITU-T Y.2012]: Набор функциональных объектов и эталонных точек между ними, используемый для описания структуры сети последующих поколений (СПП). Эти функциональные объекты разделяются эталонными точками, и, таким образом, они определяют распределение функций.

3.1.12 функциональный объект (functional entity) [b-ITU-T Y.2012]: Объект, который включает в себя набор определенных функций. Функциональные объекты являются логическими концепциями, в то время как группирование функциональных объектов используется для описания практических, физических реализаций.

3.1.13 целостность (integrity) [b-ITU-T X.800]: Свойство, в соответствии с которым данные не могут быть изменены или уничтожены несанкционированным образом.

3.1.14 ключ (key) [b-ITU-T X.800]: Последовательность символов, которая управляет операциями шифровки и дешифровки

3.1.15 управление ключами (key management) [b-ITU-T X.800]: Создание, хранение, распределение, удаление, архивирование и применение ключей в соответствии с политикой безопасности.

3.1.16 маскировка (masquerade) [b-ITU-T X.800]: Обман, при котором один объект выдает себя за другой объект.

3.1.17 поставщик сети (network provider) [b-ITU-T Q.1290]: Организация, которая поддерживает и эксплуатирует сетевые компоненты, необходимые для работы IPTV.

ПРИМЕЧАНИЕ 1. – Поставщик сети может в отдельных случаях также выступать в качестве поставщика услуг.

ПРИМЕЧАНИЕ 2. – Хотя поставщик услуг и поставщик сети рассматриваются как два отдельных объекта в отдельных случаях, это может быть один организационный объект.

3.1.18 аутентификация однорангового объекта (peer-entity authentication) [b-ITU-T X.800]: Подтверждение того, что данный одноранговый объект является тем, за кого он себя выдает.

3.1.19 неприкосновенность частной жизни (privacy) [b-ITU-T X.800]: Право отдельных лиц управлять тем или влиять на то, как может собираться и храниться относящаяся к ним информация, а также кем и кому эта информация может быть раскрыта.

3.1.20 отказ (repudiation) [b-ITU-T X.800]: Отрицание одним из субъектов, участвующих в соединении, своего участия во всем соединении или его части.

3.1.21 метка безопасности (security label) [b-ITU-T X.800]: Маркировка ресурса, который может быть блоком данных, называющая или назначающая атрибуты безопасности этого ресурса.

ПРИМЕЧАНИЕ. – Маркировка и/или соединение может быть явным или неявным.

3.1.22 политика безопасности (security policy) [b-ITU-T X.800]: Набор критериев для предоставления услуг безопасности.

3.1.23 поставщик услуг (service provider) [b-ITU-T M.1400]: Общее определение оператора, предоставляющего услуги связи потребителям и другим пользователям на тарифной или на договорной основе. Поставщик услуг может управлять сетью. Поставщик услуг может быть потребителем другого поставщика услуг.

3.1.24 угрозы (threat) [b-ITU-T X.800]: Возможные нарушения безопасности.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 получение (acquisition): Процесс приобретения контента конечным пользователем.

3.2.2 экспорт контента (content export): Процесс безопасного экспорта контента IPTV из терминала IPTV в другой терминал, принадлежащий пользователю, которому предоставлено право его использовать.

3.2.3 защита контента (content protection): Обеспечение того, что конечный пользователь может использовать только тот контент, который он/она уже получил в соответствии с правами, предоставленными ему владельцем прав. Защита контента включает в себя защиту контента от незаконного копирования и распространения, перехвата, злонамеренных манипуляций, несанкционированного использования и т. д.

3.2.4 отслеживание контента (content tracing): Процесс, позволяющий идентифицировать (произвольный) источник контента и/или ответственную сторону, например, конечного пользователя, с целью содействия последующему расследованию в случае несанкционированного использования контента, например, копирования или перераспределения контента.

ПРИМЕЧАНИЕ. – Информация для отслеживания контента может быть присоединена к нему в качестве метаданных или соответствующей метки.

3.2.5 предоставленные права (entitlements): Обозначения уровня (уровней) санкционирования, в том числе информация условного доступа, которая может использоваться абонентом для доступа к определенным услугам IPTV в своем окончательном устройстве (TD) IPTV.

3.2.6 защита окончательного устройства (TD) IPTV (IPTV terminal device (TD) protection): Обеспечение того, что TD, используемое конечным пользователем для получения услуг, может использовать контент надежно и безопасно, в то время как обеспечение прав использования, предоставляемого для такого контента, физически и электронное защищает целостность TD и конфиденциальность контента, а также критические параметры безопасности, например, сохраненные ключи, которые не защищены.

3.2.7 линейное ТВ (linear TV): Телевизионная вещательная услуга по аналогии с классической формой телевизионных услуг, предоставляемых операторами кабельного, наземного и непосредственного спутникового вещания. Здесь программный контент, передаваемый в соответствии с определенным графиком для потребления конечным пользователем в режиме реального времени.

3.2.8 метаданные для упрощения введения меток (metadata for watermarking facilitation): Метаданные, созданные для упрощения дальнейшего введения меток в устройствах нисходящего потока.

3.2.9 фишинг (phishing): Действия для получения персональной или личной информации, такой как имя пользователя, дата рождения или параметры кредитной карты под маской доверенного объекта.

3.2.10 права (rights): Обозначают возможности для выполнения заранее определенного набора функций использования элементов контента; эти функции включают в себя разрешения (например, для просмотра/прослушивания, копирования, изменения, записи, цитирования, выборки, сохранения в течение определенного времени, распространения), ограничения (например, на воспроизведение/просмотр/прослушивание некоторое число раз, на проигрывание/просмотр/прослушивание в течение определенное количество часов) и обязательства (например, плата, отслеживание контента), которые распространяются на контент и обеспечивают свободу использования, гарантируемую конечному пользователю.

3.2.11 выражение прав (rights expression): Синтаксическое выражение прав в конкретном, формальном виде.

3.2.12 сквозная SCP (SCP end-to-end): Режим защиты услуг и контента, при котором контент доступен для окончательных устройств или передается окончательными устройствами в соответствии с предоставленными им правами, используя единую систему защиты услуг и контента.

3.2.13 мостовое соединение SCP (SCP bridging): Режим работы системы защиты услуг и контента, при котором несколько систем защиты услуг и контента работают на одном устройстве, выступающем в роли моста между этими системами защиты услуг и контента. Контент, полученный через одну систему защиты услуг и контента, может быть доступен на другой системе защиты услуг и контента через мост в соответствии с предоставленными правами.

3.2.14 обмен SCP (SCP interchange): Более общий режим работы системы защиты услуг и контента, при котором каждое устройство имеет одну или несколько систем защиты услуг и контента. Контент, полученный через одну систему защиты услуг и контента, может быть доступен на другой системе защиты услуг и контента через мост в соответствии с предоставленными правами.

3.2.15 скремблирование (scrambling): Процесс, предназначенный для защиты мультимедийного контента. Как правило, при скремблировании для защиты контента используется технология шифрования.

3.2.16 алгоритм скремблирования (scrambling algorithm): Алгоритм, используемый в процессе скремблирования или дескремблирования.

3.2.17 схема безопасного транскодирования (secure transcodable scheme): Вид схемы безопасности, позволяющей промежуточным сетевым узлам выполнять транскодирование без расшифровки при сохранении сквозной безопасности. Эта схема может быть выполнена в результате объединения масштабируемого кодирования, прогрессивного шифрования и пакетирования. Схема безопасного транскодирования может обеспечивать как конфиденциальность, так и целостность сообщений/аутентификации.

3.2.18 защита услуг (service protection): Обеспечение того, чтобы конечный пользователь мог получить услугу и содержащийся в ней контент, только в соответствии с имеющимися у него/ее правами на получение. Защита услуг включает в себя защиту услуг от несанкционированного доступа, так как IPTV контент проходит через подключения IPTV услуг.

3.2.19 защита услуг и контента (service and content protection): Комбинация защиты услуг и защиты контента или их внедрение.

3.2.20 спуфинг (spoofing): Деятельность, при которой поддельный (ложный) источник, например, человек или компьютерная программа, успешно маскируется под законный источник путем фальсификации данных и с целью получения информации и/или маскировки истинного источника с тем, чтобы поддельный источник мог выполнять несанкционированные действия, такие как распространение злонамеренных программ, например вирусов, и т. д.

3.2.21 устойчивый к злонамеренным манипуляциям (tamper-resistant): Устойчивость к злонамеренным манипуляциям какой-либо продукцией, корпусом или системой с использованием физического или программного доступа к ним, осуществляемых либо индивидуальными пользователями, либо злоумышленниками.

3.2.22 транскодирование (transcoding): Процесс преобразования мультимедийного содержания, (картинки, текст, звук и видео) из первоначального формата в другой формат или качество.

3.2.23 защита неприкосновенности частной жизни пользователя (user privacy protection): Обеспечение того, чтобы информация конечного пользователя, полагаемая частной (или конфиденциальной) остается конфиденциальной, а остальные подлежат обязательному раскрытию в связи с юридическими процессами.

3.2.24 видеоподпись (video signature): Метаданные (или визуальные характеристики) для идентификации видеоконтента; в отличие от меток, введенных посредством изменения исходного видеоконтента, видеоподпись выделяется из видеоконтента без риска ухудшения качества.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения:

AAA	Authentication, Authorization and Accounting	Аутентификация, санкционирование и учет
AD	Authorized Domain	Санкционированная область
CBC	Cipher Block Chaining	Сцепление блоков шифротекста
CDN	Content Delivery Network	Сеть доставки контента
DNG	Delivery Network Gateway	Шлюз сети доставки
DNGF	Delivery Network Gateway Function	Функции шлюза сети доставки
DoS	Denial of Service	Отказ в обслуживании
ECB	Electric Code Book	Электронная кодовая книга
ECM	Entitlement Control Message	Сообщение для управления доступом на основе предоставленных прав
EMM	Entitlement Management Message	Сообщение для управления предоставлением прав
EPG	Electronic Program Guide	Электронная программа передач

HN	Home Network	Домашняя сеть
HN TD	Home Network Terminal Device	Оконечное устройство домашней сети
ID	Identifier	Идентификатор
IPTV	Internet Protocol Television	Телевидение по протоколу Интернет
MIKEY	Multimedia Internet KEYing	Использование мультимедийных ключей для интернета
NAT	Network Address Translation	Трансляция сетевых адресов
OFB	Output FeedBack	Режим обратной связи по выходу
P2P	peer to peer	Одноранговое взаимодействие
PDA	Personal Digital Assistant	Персональный цифровой ассистент
PIN	Personal Identification Number	Персональный идентификационный номер
PKI	Public Key Infrastructure	Инфраструктура открытого ключа
PVR	Personal Video Recorder	Персональный видеомаягнитофон
QoE	Quality of Experience	Оценка пользователем качества услуги
QoS	Quality of Service	Качество обслуживания
REL	Rights Expression Language	Язык выражения прав
SCP	Service and Content Protection	Защита услуг и контента
SCP-B	SCP Bridge	Мостовое подключение SCP
SCP-EE	SCP End-to-End	Сквозная SCP
SCP-IX	SCP Interchange	Обмен SCP
STS	Secure Transcodable Scheme	Схема безопасного транскодирования
TD	IPTV-compliant Terminal Device	IPTV-совместимое оконечное устройство
USB	Universal Serial Bus	Универсальная последовательная шина
VoD	Video on Demand	Видео по запросу

5 Условные обозначения

В данной Рекомендации:

Ключевые слова "**требуется, чтобы**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии этой Рекомендации.

Ключевые слова "**рекомендуется, чтобы**" означают требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, для заявления о соответствии это требование не является обязательным.

Ключевые слова "**запрещается**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии этой Рекомендации.

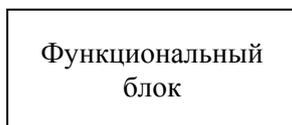
Ключевые слова "**может быть дополнительно**" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Этот термин не означает, что вариант реализации поставщика должен обеспечивать выполнение этой функции и функция может быть активирована по желанию оператора сети/поставщика услуг. Это означает лишь, что поставщик может дополнительно предоставить эту функцию и по-прежнему заявлять о соответствии спецификации.

В контексте архитектуры безопасности IPTV в этой Рекомендации:

"Функции" определяются как набор функциональных возможностей. Они обозначаются следующим символом:



"Функциональный блок" определяется как группа функциональных возможностей, которые далее не делятся на уровни, подробно описанные в этой Рекомендации. Он обозначается символом:



6 Требования безопасности

6.1 Общие требования безопасности

- Рекомендуется, чтобы при внедрении безопасности архитектура IPTV учитывала ее влияние/воздействие на показатели работы, качество обслуживания, удобство использования, масштабируемость и ограничение по стоимости.
- Архитектура IPTV может дополнительно поддерживать защиту контента конечных пользователей в режиме совместного использования контента.

6.2 Требования безопасности контента

В этом пункте определены требования, которые по отдельности или все вместе относятся к контенту или защите контента.

Требования к архитектуре

- Требуется, чтобы архитектура IPTV поддерживала защиту контента как определено в пункте 3.
- Требуется, чтобы архитектура IPTV поддерживала обеспечение соответствия контента с защитой и метаданными управления контентом.
- Требуется, чтобы архитектура IPTV поддерживала безопасную доставку защиты контента и метаданных управления контентом, включая метаданные прав использования.
- Требуется, чтобы архитектура IPTV поддерживала метаданные прав использования контента, которые обеспечивают различие между правами использования, включая рендеринг (просмотр), хранение, перераспределение, а также их комбинации.
- Требуется, чтобы архитектура IPTV поддерживала защиту контента распространяемого для очень большого числа абонентов одновременно (масштабируемость).
- Требуется, чтобы архитектура IPTV поддерживала защиту потокового контента многоадресной и/или одноадресной передачи.
- Требуется, чтобы архитектура IPTV поддерживала защищенность хранимого контента в соответствии с предоставленным правом использования.
- Если используется отслеживание контента, то требуется, чтобы архитектура IPTV поддерживала отслеживание контента в автономном (не в режиме реального времени) режиме (например, контент VoD).
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению передачи информации отслеживания контента (например, упрощение маркировки метаданных).
- Запрещается, чтобы архитектура IPTV препятствовала поддержке применения технологии отслеживания контента на выходе конечного устройства (TD) в целях однозначной идентификации сеанса связи (например, канал, время/дата), TD и/или оператора сети. Одним из вариантов примера таких технологий отслеживания контента может быть видимая и невидимая информация.

- Запрещается, чтобы архитектура IPTV препятствовала восстановлению информации отслеживания контента из контента.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению функциональной совместимости систем защиты услуг и контента, когда контент IPTV разрешено использовать только санкционированному пользователю (пользователям) или устройству (устройствам), даже после его (их) перехода в другую систему безопасности.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению функциональной совместимости систем защиты услуг и контента, с целью сохранения идентификационной информации таким образом, чтобы контент IPTV мог быть последовательно определен, независимо от того, какая схема идентификации используется и в какую систему безопасности передается контент.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению функциональной совместимости систем защиты услуг и контента, с тем чтобы не допустить снижения уровня безопасности при передаче контента в другую систему безопасности.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению функциональной совместимости систем защиты услуг и контента, при котором права предоставляются только доверенным устройствам.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению функциональной совместимости систем защиты услуг и контента таким образом, чтобы обеспечивалась безопасная среда обмена функционально совместимыми данными систем защиты услуг и контента (например, информация аутентификации, метаданные информация о ключах и т. д.).
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению функциональной совместимости систем защиты услуг и контента, так чтобы указанная функциональная совместимость не зависела от особенностей программного или аппаратного обеспечения.
- Запрещается, чтобы архитектура IPTV требовала открытого указания механизма защиты услуг и контента, используемого в функционально совместимых системах SCP на любой из двух сторон.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению гибкой и расширяемой функциональной совместимости систем защиты услуг и контента для поддержки различных бизнес-моделей.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению функциональной совместимости систем защиты услуг и контента в рамках различных систем безопасности, использующих разные механизмы безопасности, в целях поддержки услуг со сдвигом во времени (абонент может сохранить контент и получить его позже) и услуг со сменой места (абонент может просматривать контент в любом месте), даже с разными механизмами безопасности.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению функциональной совместимости систем защиты услуг и контента с целью обеспечения прозрачности для пользователей.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению нескольких механизмов защиты контента и услуг независимо от конкретных аппаратных или программных требований.

Рекомендации по архитектуре

- Если контент IPTV использует технологию отслеживания контента, рекомендуется, чтобы технология отслеживания была незаметной.
- Рекомендуется, чтобы архитектура IPTV обеспечивала устойчивое отслеживание контента в режиме реального времени (например, радиовещательный контент).
- Рекомендуется, чтобы архитектура IPTV обеспечивала возможность аутентификации и авторизации конечных пользователей в случае совместного использования контента, например экспорт контента и перераспределения контента, если поддерживается совместное использование контента.

- Если реализация архитектуры IPTV использует технологию отслеживания контента на основе метаданных, то для упрощения маркировки рекомендуется внести соответствующие метаданные в контент элементарных потоков, используя положения для "данных пользователя", подобные тем, что предусмотрены в конкретной схеме кодирования.
- В случае если одно оконечное устройство или HN-TD в рамках архитектуры IPTV поддерживает несколько механизмов защиты контента и услуг, рекомендуется использовать одну стандартную функцию трансляции, которая дает возможность сочетания нескольких систем SCP и осуществления согласованной трансляции между ними, а также обеспечивает функциональную совместимость любого присоединенного оконечного устройства или HN-TD, задействованного в таком механизме трансляции.

Дополнительные возможности архитектуры

- Архитектура IPTV может дополнительно поддерживать введение информации отслеживания контента. Данная информация отслеживания контента дополнительно может содержать ID-оператора, ID-собственника контента, ID-оконечного устройства (TD) и другую информацию.

Требования к алгоритмам скремблирования

- Требуется, чтобы алгоритмы скремблирования потоков вещательной передачи обеспечивали периодическое обновление необходимых криптографических ключей.
- Требуется, чтобы алгоритмы скремблирования IPTV создавались с использованием общедоступных и стандартизованных алгоритмов шифрования.

Рекомендации для алгоритмов скремблирования

- Рекомендуется, чтобы алгоритмы скремблирования для IPTV имели достаточно большую энтропию ключа для эффективной защиты контента от криптоанализа.
- Не запрещается, чтобы архитектура IPTV препятствовала обеспечению широко используемых алгоритмов скремблирования.
- Рекомендуется, чтобы архитектура IPTV не препятствовала обеспечению нескольких систем скремблирования.
- Рекомендуется, чтобы алгоритмы скремблирования для IPTV эффективно внедрялись в аппаратные средства и/или программное обеспечение.
- Рекомендуется, чтобы алгоритмы скремблирования для IPTV были масштабируемыми и могли выдержать проверку временем, т. е. параметры шифрования (например, длина ключа, периоды шифрования и т. д.) или способ шифрования (например, CBC, OFB, ECB и т. д.).

Дополнительные возможности алгоритмов скремблирования

- В алгоритмах скремблирования для IPTV могут дополнительно применяться алгоритмы шифрования различной интенсивности к различным типам контента.

6.3 Требования безопасности услуг

В этом пункте определены требования, по отдельности или все вместе касающиеся услуг и защиты услуг.

Требования к архитектуре

- Требуется, чтобы архитектура IPTV обеспечивала возможность защиты услуг согласно определению в пункте 3.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению обновления SCP или возобновления действия SCP в оконечном устройстве, осуществляемого со стороны сервера.
- Требуется, чтобы архитектура IPTV обеспечивала возможность санкционирования и аутентификации конечного пользователя (абонента).
- Требуется, чтобы архитектура IPTV поддерживала механизм для передачи оконечному устройству указания использовать определенный алгоритм скремблирования, основанный на стандартной схеме.

- Требуется, чтобы архитектура IPTV имела возможность использовать стандартные системы управления ключом (например, MIKEY, EMM/ECM), как требуется для обеспечения совместимости.
- Требуется, чтобы архитектура IPTV обеспечивала возможность обновления и запроса систем SCP относительно алгоритмов скремблирования для IPTV и любого другого алгоритма скремблирования, выбираемого оператором, на стороне сервера с помощью интерфейсов SCP.
- Требуется, чтобы архитектура IPTV поддерживала механизмы SCP, не зависящие от конкретных форматов контента.
- Требуется, чтобы архитектура IPTV поддерживала механизм защиты целостности и аутентификации источника данных для важных метаданных.
- Требуется, чтобы архитектура IPTV поддерживала механизм безопасности доставки прав и информации управления доступом оконечных устройств к контенту.
- Требуется, чтобы архитектура IPTV обеспечивала контроль использования контента, например, воспроизведения.
- Требуется, чтобы архитектура IPTV поддерживала различные режимы воспроизведения, например, ограничение на количество воспроизведений, ограничение по времени воспроизведения, ограничение ускоренной перемотки вперед или назад.
- Требуется, чтобы архитектура IPTV поддерживала механизм сохранения конфиденциальности сообщений сигнализации между сервером SCP и клиентом SCP.
- Требуется, чтобы архитектура IPTV поддерживала механизм сохранения достоверности сообщений сигнализации между сервером SCP и клиентом SCP.
- Требуется, чтобы архитектура IPTV поддерживала механизм сохранения целостности сообщений сигнализации между сервером SCP и клиентом SCP.
- Требуется, чтобы архитектура IPTV поддерживала механизм безопасного получения параметров SCP, например, конфигурация, статус, с TD.
- Требуется, чтобы архитектура IPTV поддерживала механизм безопасного обновления параметров SCP, например, конфигурации, от TD.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению возможности включения и выключения функции отслеживания контента в программируемой форме, например, на основе времени, события, контента или канала.
- При использовании систем управления ключами, требуется, чтобы такие системы проектировались с учетом масштабируемости, надежности и совместимости.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению возможности установки и эксплуатации решений по защите мультисервисных услуг без замены аппаратного обеспечения, за исключением съемных устройств, таких как USB-ключи защиты и SIM-карты.
- Запрещается, чтобы архитектура IPTV препятствовала поддержке механизма идентификации для доступных решений защиты услуг, которые способны удовлетворить требования, определенные для соответствующей защиты контента.
- Запрещается, чтобы архитектура IPTV препятствовала поддержке механизма системы SCP обнаружения механизма таким образом, чтобы она могла поддерживать метод обнаружения и адаптироваться к нему, когда определенный контент требует определенной системы защиты услуг.
- Запрещается, чтобы архитектура IPTV препятствовала поддержке механизма выбора системы SCP из имеющихся систем SCP без замены аппаратных средств, за исключением съемных устройств.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению безопасности загрузки для системы SCP. Загружаемая система SCP может дополнительно зависеть от конкретных требований защиты услуг.
- Если используется загружаемая система SCP, то требуется, чтобы архитектура IPTV обеспечивала для загруженной системы SCP защиту целостности и аутентификацию исходных данных.

- При обеспечении безопасности загрузки программы приложения для TD, требуется, чтобы архитектура IPTV обеспечивала защиту целостности и аутентификацию исходных данных для загруженных приложений.

Рекомендации по архитектуре

- Рекомендуется, чтобы архитектура IPTV обеспечивала конфиденциальность контента.
- Рекомендуется, чтобы архитектура IPTV поддерживала несколько алгоритмов скремблирования.
- Рекомендуется, чтобы архитектура IPTV обеспечивала возможность аутентификации и санкционирования конечных пользователей для услуг с совместно используемым контентом, например экспорта контента и перераспределения контента.
- Если архитектура IPTV использует систему управления ключами с иерархической схемой управления ключами, то рекомендуется поддерживать масштабируемость.
- Если архитектура IPTV использует систему управления ключами, в которой применяется групповой протокол управления ключом, с иерархической схемой управления ключами и альтернативным алгоритмом управления ключами, то рекомендуется поддерживать масштабируемость.
- Если архитектура IPTV использует систему управления ключами, в которой применяются ключи кратковременного действия, рекомендуется, чтобы передача по среде происходила таким образом, чтобы трансляция NAT и ограничения полосы пропускания не ограничивали бы обмен ключами.
- Рекомендуется, чтобы архитектура IPTV поддерживала, как минимум, ту же степень защиты (для целей контроля несанкционированного доступа) информации отслеживания контента, которая применялась к соответствующему отслеженному контенту.
- Рекомендуется, чтобы архитектура IPTV поддерживала совместную передачу контента и информации отслеживания контента, сохраняя при этом синхронизацию контента и информации отслеживания контента в процессе передачи.
- В случае если архитектура IPTV использует PKI для определения TD или поставщика контента, то, учитывая многоуровневую иерархию PKI, рекомендуется, чтобы обеспечивались масштабируемость, надежность и совместимость.
- В случае если архитектура IPTV использует PKI для услуг IPTV общего пользования, рекомендуется использовать установленный формат сертификата, список отозванных сертификатов или протокол оперативного определения статуса сертификата.
- Рекомендуется, чтобы архитектура IPTV поддерживала безопасность загрузки на TD прикладных программ.
- Рекомендуется, чтобы архитектура IPTV поддерживала механизм ограничения прав просмотра основных программ для основных групп абонентов, например, блокировку просмотра для жителей конкретного района, это, например, может быть полезной функцией для спортивных мероприятий.

Дополнительные возможности архитектуры

- Для того чтобы обеспечить масштабируемость IPTV услуг для принадлежащих пользователям оконечным устройствам, разрешающая способность которых отличается от оконечных устройств IPTV, архитектура может дополнительно поддерживать безопасные схемы транскодирования, как определено в пункте 3.

6.4 Требования к безопасности сети

В этом пункте определены требования, по отдельности или все вместе касающиеся сетей и их защиты.

Требования к архитектуре

- Требуется, чтобы архитектура IPTV поддерживала возможность смягчения DoS атаки.
- Требуется, чтобы архитектура IPTV поддерживала меры безопасности по блокировке нелегального или нежелательного трафика.

- Требуется, чтобы архитектура IPTV была устойчива к атакам на функции многоадресной передачи.
- Рекомендуется, чтобы архитектура многоадресной передачи обеспечивала возможность одноранговой аутентификации в общей или расположенной на слой выше (одноранговой) среде многоадресной передачи.
- Требуется, чтобы канал связи между оконечными устройствами в пределах домашней сети был защищен для безопасности передачи оплаченного контента, например оплаченного потребителем контента, который не защищен.
- Требуется, чтобы архитектура IPTV поддерживала аутентификацию DNG при помощи функции управления IPTV.
- Требуется, чтобы архитектура IPTV поддерживала аутентификацию функции управления IPTV при помощи DNG.

Рекомендации по архитектуре

- Для того чтобы защитить домашнюю сеть от злонамеренного или несанкционированного доступа, рекомендуется, чтобы архитектура IPTV поддерживала функцию шлюза сети (DNGF), для того чтобы создавать брандмауэры, которые настраиваются дистанционно и имеют несколько уровней безопасности, а также соответствующие шлюзы на уровне приложений.
- Рекомендуется, чтобы архитектура IPTV обеспечивала возможность управления IPTV для дистанционной настройки NAT и введения функции защиты DNG.
- Рекомендуется, чтобы архитектура IPTV обеспечивала возможность дистанционной настройки NAT и внедрения функции защиты DNG при помощи функции удаленного управления IPTV.
- Рекомендуется, чтобы архитектура IPTV обеспечивала удаленное управление TD в том случае, когда поддерживается удаленное управление.
- Рекомендуется, чтобы архитектура IPTV обеспечивала возможность использования информации меток контента для управления доставкой контента.

6.5 Требования к безопасности оконечного устройства

В этом пункте определены требования, по отдельности или все вместе касающиеся оконечных устройств (TD) и их защиты.

Требования к архитектуре

- Требуется, чтобы архитектура IPTV поддерживала защиту TD, как определено в пункте 3.
- Требуется, чтобы архитектура IPTV поддерживала аутентификацию TD.
- Требуется, чтобы архитектура IPTV поддерживала устойчивость TD к злонамеренным физическим манипуляциям.
- Требуется, чтобы архитектура IPTV поддерживала средства обнаружения злонамеренных физических манипуляций с TD.
- Если используется загружаемая SCP, то требуется, чтобы архитектура IPTV обеспечивала безопасность загрузки и установки на TD рабочего кода SCP.
- Требуется, чтобы архитектура IPTV поддерживала средства безопасности выполнения в TD критичных для безопасности процессов, таких как управление ключами и последовательное представление среды передачи, для того чтобы прервать воспроизведение контента в случае неисправности системы безопасности, обнаружения злонамеренных манипуляций или других свидетельств ненадлежащего использования.
- Требуется, чтобы архитектура IPTV обеспечивала физическую защиту важнейших процессов обеспечения безопасности и компонентов, участвующих в процессе передачи и хранения ценного контента в TD в отсутствие логической защиты (такой, как шифрование или последовательное представление меток). Эти процессы включают дескремблирование и последовательное представление среды.

- Требуется, чтобы архитектура IPTV определяла необходимость физической защиты (против зондирования или злонамеренных манипуляций в отношении системы функций SCP в TD) важных процессов обеспечения безопасности в TD, в том числе дескремблирование и последовательное представление среды (отслеживание контента) и критических данных, поддерживающих эти процессы, а также для всех компонентов, участвующих в обработке, передаче и хранении любого ценного контента в отсутствие логических средств защиты, таких как шифрование или метки отслеживания контента.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению обмена контентом между TD и другими физическими или логическими устройствами при условии, что использование такого контента предусматривает такой обмен.
- Требуется, чтобы архитектура IPTV поддерживала механизм, позволяющий TD аутентифицировать серверы SCP.
- Запрещается, чтобы архитектура IPTV препятствовала обеспечению возобновления действия SCP в TD.
- Требуется, чтобы архитектура IPTV поддерживала цифровой или аналоговый выход, который должен быть защищен согласно требованию клиента SCP на внешнем устройстве хранения, в случае если TD обладает цифровым или аналоговым видео/аудио выходом.

Рекомендации по архитектуре

- Рекомендуется, чтобы архитектура IPTV обеспечивала экспорт контента в TD с использованием IPTV контента, который необходимо безопасно передать от терминала IPTV на другой терминал, принадлежащий пользователю, имеющему право на его использование.

6.6 Требования к безопасности абонентов

В этом пункте определены требования, по отдельности или все вместе касающиеся абонентов и конечных пользователей или их защиты.

Требования к архитектуре

- Требуется, чтобы архитектура IPTV обеспечивала защиту неприкосновенности частной жизни пользователя, как определено в пункте 3.
- Требуется, чтобы архитектура IPTV позволяла абоненту устанавливать механизм управления доступом, например, с использованием пароля, для того чтобы ограничить доступ к контенту и/или услугам.
- Требуется, чтобы архитектура IPTV была способна указать причину отказа пользователю в доступе к контенту.
- Требуется, чтобы архитектура IPTV поддерживала механизм, позволяющий абоненту запрашивать расширения прав пользования, связанных с определенными элементами контента, например, больше воспроизведений, больше времени воспроизведения.

Рекомендации по архитектуре

- Рекомендуется, чтобы архитектура IPTV позволяла конечным пользователям, в соответствии с определенными правами изменять, т. е. заменять TD, без соответствующего влияния на его права потребления контента.
- Рекомендуется, чтобы архитектура IPTV поддерживала механизм определения рейтинга программы в соответствии с контентом.

ПРИМЕЧАНИЕ. – Информация о рейтинге может быть использована для управления доступом, например, контроля со стороны родителей.

7 Архитектура безопасности

В этом пункте определена архитектура безопасности IPTV с точки зрения общей архитектуры безопасности и архитектуры защиты услуг, а также функциональных модулей безопасности для выполнения требований, описанных в предыдущих пунктах.

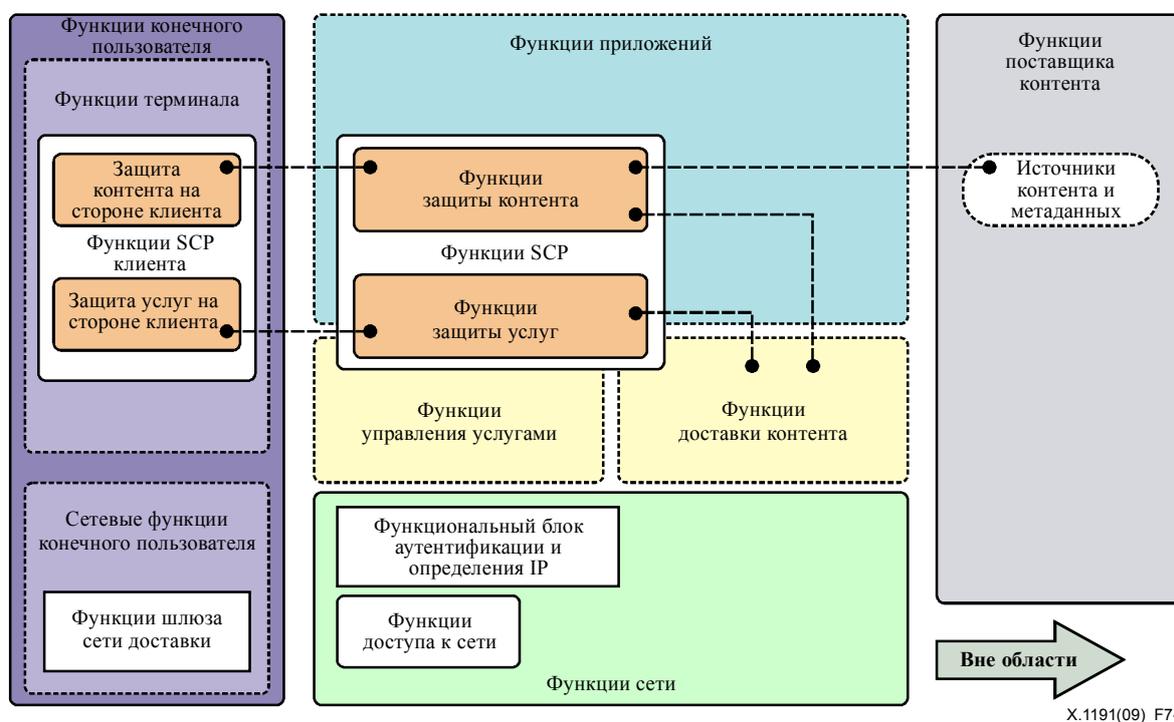
Предполагается, что описанная ниже архитектура безопасности IPTV предназначена для использования в контексте функциональных доменов IPTV и структуры функциональной архитектуры, определенных в пунктах 6 и 8 [ITU-T Y.1910], соответственно.

7.1 Общая архитектура безопасности

Общая архитектура безопасности для IPTV изображена на рисунке 7-1, ниже. Эта общая архитектура подразделяется на две основные области. Одна из них, как считается, находится в сфере применения этой Рекомендации, а другая считается выходящей за ее рамки. Первая область включает в себя области конечного пользователя, поставщика сети и поставщика услуг, тогда как вторая область охватывает область поставщика контента.

Во второй области все аспекты безопасности в пределах области поставщика контента и взаимосвязей между поставщиками контента и поставщиками услуг подчиняются частным соглашениям между заинтересованными сторонами, действующими в этих областях. Таким образом, считается, что они выходят за рамки этой Рекомендации.

Несмотря на то, что области поставщика контента и взаимосвязи между областями поставщиков контента и поставщиков услуг считаются выходящими за рамки настоящего контекста, для полноты картины область поставщика контента включена в нижеследующие рисунки и описания. Таким образом, любое сделанное здесь заявление относительно этих областей следует считать приведенным только для информации и пояснений.



ПРИМЕЧАНИЕ 1. – Функции защиты контента и функции защиты услуг на этом рисунке являются наиболее важными элементами архитектуры безопасности IPTV. Подробное описание этих функций можно найти на рисунке 7-2 (*Архитектура защиты контента*) и рисунке 7-3 (*Архитектура защиты услуг*).

ПРИМЕЧАНИЕ 2. – Для простоты на данном рисунке не показаны некоторые функции и функциональные блоки архитектуры IPTV, не относящиеся напрямую к IPTV безопасности.

Рисунок 7-1 – Общая архитектура безопасности IPTV

Общая архитектура безопасности приблизительно делится на четыре функциональные области следующим образом:

- Функции поставщика контента (технически выходят за рамки данной Рекомендации). Предполагается, что поставщик(и) контента предоставляет(ют) доступ к контенту поставщикам сети, установившим отношение(я) с поставщиком(ами) контента. В некоторых случаях поставщик контента может сам выступать в качестве поставщика услуг, в таком случае такие взаимоотношения считаются внутренними.

При предоставлении поставщикам услуг доступа к контенту, для управления и обеспечения доступа к контенту поставщик контента может использовать стандартные или частные механизмы; отметим, однако, что такие механизмы считаются выходящими за рамки данной Рекомендации и подчиняются только частным соглашениям между заинтересованными сторонами.

- Функции защиты контента и услуг (SCP) (пересекаются с некоторыми частями функций приложений, функций управления услугами и функций доставки контента).

Функции SCP играют ключевую роль в архитектуре общей безопасности IPTV, особенно в области поставщика услуг. В частности, к ней относятся функции защиты услуг, которые включают защиту инфраструктуры услуг, а также управление доступом к услугам и контенту. С другой стороны, функции защиты контента позволяют контролировать использование услуг и контента в соответствии с лицензионными требованиями. Конкретные функции и функциональные блоки SCP распределены в трех подструктурах: функции приложений, функции управления услугами и функции доставки контента.

Поставщик услуг обязан по лицензии(ям), полученным у поставщиков контента, сделать контент доступным только при определенных условиях его использования, например одноразовый просмотр без записи, одноразовая запись с несколькими просмотрами, одноразовая запись с передачей прав записи и т. д. Основная цель защиты контента функциями SCP заключается в том, чтобы позволить поставщику услуг выполнять подобные обязательства способом, поддающимся объективно контролю.

Основной целью функций SCP в аспекте защиты услуг является предотвращение несанкционированного доступа к ресурсам услуг и информации, считающейся конфиденциальной, со стороны объектов, находящихся в различных областях: обслуживание, сети, оконечные устройства и конечные пользователи.

Вторая цель функций SCP в аспекте защиты услуг заключается в том, чтобы защитить инфраструктуру услуг от ущерба, причиняемого в результате умышленного и/или случайного ненадлежащего использования ресурсов.

Подробная информация о функциональных блоках функций защиты контента и функций защиты услуг показаны на рисунке 7-2 (*Архитектура защиты контента*) и рисунке 7-3 (*Архитектура защиты услуг*), соответственно.

- Функции сети.

Функции безопасности, касающиеся сетевой области, сосредоточены на аутентификации объектов и санкционировании доступа к сети(ям), по которым доставляются или будут доставляться услуги IPTV. Второй функцией является защита целостности самой сети физически, электронно и эксплуатационно, например, путем выявления и пресечения в сетях доступа или магистральных сетях атак типа "отказ в обслуживании".

- Функции конечного пользователя.

Аспекты безопасности, применяемые к конечному пользователю (абоненту), включают защиту целостности оконечных устройств (TD), действующих на территории абонента, а также защиту неприкосновенности частной жизни конечного пользователя.

При определенных обстоятельствах DNG между TD и сетевой областью можно рассматривать в рамках области (домена) конечного пользователя и применять меры безопасности конечного пользователя.

Наконец, рекомендуется, чтобы механизмы защиты целостности применялись для обеспечения целостности контента полученного TD и перераспределенного впоследствии на другие устройства в пределах или за пределами домашней сети. (Это приводит к перекрытию между аспектами безопасности конечных пользователей и аспектами защиты контента.)

Более подробное описание функций и функциональных блоков рисунка 7-1 приводится в пункте 7.4.1.

7.2 Архитектура защиты контента

Архитектура защиты контента для IPTV изображена на рисунке 7-2, ниже.

Основная функция архитектуры защиты контента состоит в том, чтобы определить поток и обработать информацию о правах пользования контентом и информацию, необходимую для управления данными правами и их реализации.

В конечном счете, права на использование контента создает(ют) поставщик(и) контента; отметим, однако, что такие права могут быть изменены (например, сужены или даже расширены) до поставщика(ов) услуг в соответствии с его (их) соглашениями с поставщиком(ами) контента и политикой работы и бизнеса.

Показанная выше архитектура защиты контента состоит из функций, находящихся, в основном, в двух функциональных областях:

- Функции защиты контента и услуг (пересекаются с функциями приложений и функциями доставки контента).

Контент и связанные с ним права собираются от поставщиков контента, агрегируются и обрабатываются для доставки к конечному пользователю, при этом весь процесс управляется несколькими функциями, такими как функции подготовки контента, с использованием данных, описывающих права конечного пользователя и соответствующие условия.

Информация контента, прав и ключей, используемая для предоставления доступа к контенту и возможности его использования, преобразуется в форму, подходящую для конкретного применения, например просмотра линейного ТВ. Информация прав и ключей доставляется функциональным блоком управления правами и ключами в клиентский Функциональный блок защиты контента оконечного устройства в виде сообщения о предоставляемых правах, например, сообщения EMM. Содержимое дополнительно обрабатывается для вставки метаданных отслеживания контента, например, меток, а затем перед доставкой зашифровывается функциями подготовки контента. В некоторых случаях, например, для IP-услуг в режиме реального времени, контент также может быть зашифрован функциями доставки контента.

В контексте архитектуры защиты контента IPTV (в отличие от архитектуры защиты услуг IPTV, которая будет описана ниже), акцент делается, прежде всего, на управление, обработку и доставку прав и ключей в отличие от шифрования этой информации или контента в соответствии с этими правами.

- Функции конечного пользователя.

Функции терминалов, работающих в области конечных пользователей, несут ответственность за соблюдение прав использования контента в соответствии с информацией о правах, известной также как метаданные защиты контента. Этот функциональный объект интерпретирует права и ключи контента, полученные от функционального блока управления ключами и правами, а затем использует результаты интерпретации для управления обработкой и воспроизведением контента конечному пользователю с помощью устройств комплексного представления, например дисплея или аудиовизуальной системы, или с помощью физических взаимосвязей с внешними устройствами.

В тех случаях, когда TD передает защищаемый контент на внешнее устройство, например на вход дисплея, права контента могут быть переведены в другие формы; контент, к которому применимо такое использование, может быть дополнительно обработан для вставки информации отслеживания контента на стороне клиента, например меток или повторного шифрования контента для обеспечения управления доступом в нисходящем потоке.

Более подробно архитектурные блоки, показанные на рисунке 7-2, описаны в пункте 7.4.

Показанный на рисунке 7-2 интерфейс экспорта контента является логическим интерфейсом, соединяющим IPTV TD и HN TD. HN-TD могут сами потреблять контент или экспортировать его на другие HN-TD. Клиентские функции доставки контента могут настроить соответствующую метку безопасности для подтверждения того, что потреблять и экспортировать контент может только авторизованная система HN-TD.

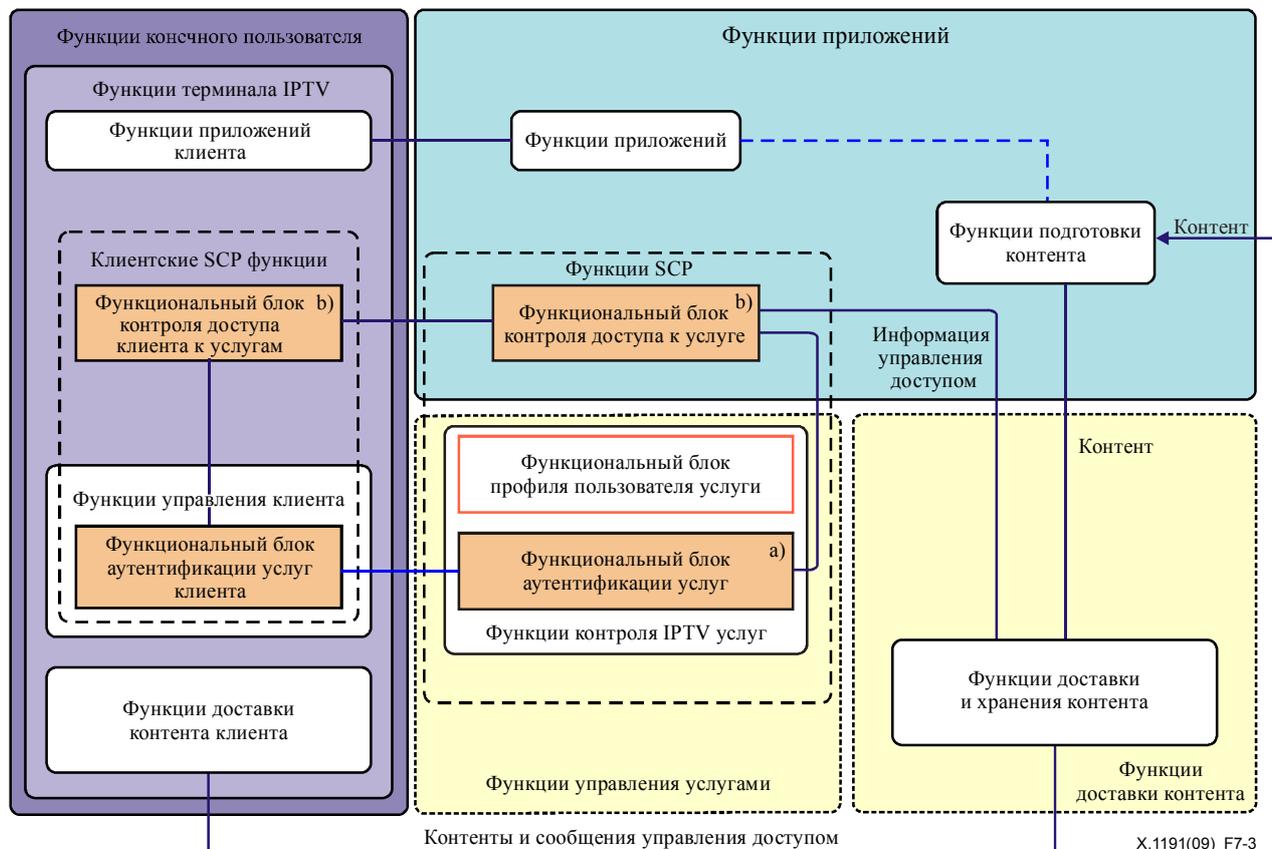
7.3 Архитектура защиты услуг

Для управляемых услуг, связанных с защитой контента, типичен случай, когда для получения доступа к услуге(ам) и размещенному в ней (них) контенту конечный пользователь (абонент) и TD должны быть аутентифицированы и санкционированы.

В зависимости от обстоятельств, функции аутентификации и санкционирования могут выполняться отдельно от TD и конечного пользователя(ей). В других случаях для получения доступа к услуге может потребоваться аутентификация дополнительных устройств на стороне пользователя, таких как сетевой шлюз доставки и другие устройства конечного пользователя.

Сочетание аутентификации и санкционирования может быть использовано для управления доступом как к услугам IPTV, так и к оконечным устройствам (TD) для целей приобретения услуг и контента до использования.

Архитектура защиты услуг для IPTV изображена ниже на рисунке 7-3.



а) Аутентификация: определяет имя абонента и ID с присвоенными приоритетами.

б) Контроль доступа к услуге: для защиты услуги от незаконного неавторизованного доступа.

ПРИМЕЧАНИЕ. – Функциональный блок защиты услуги на этом рисунке состоит из Функций защиты услуги и Функций защиты услуги Клиента.

Рисунок 7-3 – Архитектура защиты услуг IPTV

Основные функции архитектуры защиты услуг включают в себя:

- Аутентификация абонента и TD:
 - Эта функция отвечает за аутентификацию абонентов и TD.
 - Аутентификация абонента: обработка аутентичности пользователя;
 - Аутентификация TD: обработка аутентичности TD.
 - В случае использования сертификатов на основе X.509 в качестве полномочий для аутентификации, требуется отменить эту функцию.
- Аутентификация сервера:
 - В TD, функция аутентификации сервера для взаимной аутентификации.
- Управление доступом к услуге:
 - Функция для ограничения получения и предоставления санкционированными пользователями доступа к услугам, с использованием механизмов безопасности, таких как скремблирование и шифрование.

Более подробные описания архитектурных блоков, показанных на рисунке 7-3, приведены в пункте 7.4.

7.4 Описание функций и функциональных блоков архитектуры безопасности IPTV

В этом пункте содержится более подробное описание функций и функциональных блоков, изображенных выше в моделях архитектуры в п. 7.1 (*Общая архитектура безопасности*), п. 7.2 (*Архитектура защиты контента*) и п. 7.3 (*Архитектура защиты услуг*). Эти функции и функциональные блоки определены лишь общими описательными терминами и разделены на три части, соответствующие каждому из этих трех пунктов.

7.4.1 Функции и функциональные блоки общей архитектуры

Функции доступа к сети: Обеспечивают сбор и агрегирование данных управления и трафика, создаваемого в сети(ях); позволяют выполнять функции QoS/QoE, включая управление буфером, создание очередей и расписаний, фильтрацию пакетов, классификацию трафика, маркировку, определение политики и формирование трафика.

ПРИМЕЧАНИЕ 1. – С точки зрения услуг IPTV и защиты контента эти функции не зависят от функций защиты услуг и контента.

Функции приложений: Разделены между стороной сервера (поставщик услуг) и стороной клиента (территория конечного пользователя); состоят из функциональных компонентов, которые готовят, производят, принимают и обрабатывают приложения IPTV уровня обслуживания, например линейное TV, VoD и относящийся к ним контент, например информацию о доступности интерактивные приложения и т. д.

Функциональный блок аутентификации и распределения по протоколу IP: Содержит функции для аутентификации подлинности функционального блока шлюза сетевой доставки, подключенного к функциям сети, а также распределение IP-адресов для функций оконечного устройства IPTV.

Функции защиты контента: Обеспечивают механизмы, которые позволяют выполнять правила использования контента, включая агрегирование, распределение и управление правами и ключами, дополнительное создание и введение информации отслеживания контента, например меток и шифрования контента (под управлением функций защиты услуг).

ПРИМЕЧАНИЕ 2. – Конкретные функциональные блоки, составляющие функции защиты контента, описаны далее в пунктах 7.2 и 7.4.2.

Функции защиты контента клиента: Взаимодействуя со стороной сервера, функции защиты контента служат для обеспечения выполнения правил использования контента.

Функции поставщиков контента: Доставляют поставщикам услуг контент, права в отношении контента и метаданные ключей.

Функции сетевого шлюза доставки: Обеспечивают возможность установления соединений между оконечным устройством и сетью доставки; управляют возможностью установления местных (на территории конечного пользователя) IP-соединений, получают IP-адреса (адресов), а также IP-конфигурацию оконечного устройства.

ПРИМЕЧАНИЕ 3. – В том, что касается защиты услуг и контента IPTV, данные функции независимы от функций защиты услуг и контента.

Функции защиты услуг: Обеспечивают механизмы для аутентификации и санкционирования и управления доступом для услуг IPTV и содержащегося в них контента, в том числе управление и непосредственное введение сигнала управления и передача зашифрованных данных либо самостоятельно, либо в сочетании с функциями защиты контента.

ПРИМЕЧАНИЕ 4. – В том, что касается защиты услуг и контента IPTV, данные функции независимы от функций защиты услуг и контента.

ПРИМЕЧАНИЕ 5. – Конкретные функциональные блоки, составляющие функции защиты услуг, описаны далее в пунктах 7.3 и 7.4.3.

Функции защиты услуг клиента: Взаимодействуют с функциями защиты услуг на стороне сервера для управления доступом к услугам и выполнения других функций защиты.

Функции Терминала: Обеспечивают клиентов защиты услуг и защиты контента для дешифрования и повышение безопасности использования услуг и контента в соответствии с метаданными прав; выполняют шифрование на уровне линии передачи и трансляцию (изменение) SCP, требуемые для дальнейшего получения контента в нисходящем потоке или для перераспределения и внутреннего (или внешнего) хранения контента, включая поддержку безопасной (устойчивой к злонамеренным манипуляциям) обработки среды передачи, местного, защищенного, например ключом, хранения, обновляемости программ обеспечения безопасности, аутентификации и проверки загруженных программ, а также защиты локально хранимых и передаваемых объектов данных, регулируемых принципами неприкосновенности частной жизни конечного пользователя.

7.4.2 Функции и функциональные блоки архитектуры защиты контента

Функции приложений клиента: Первичная точка координации и управления взаимодействием между конечным пользователем и услугой(ами), обеспечиваемая функциями приложений IPTV; для стандартных приложений, таких как просмотра линейного ТВ, она предоставляет собой первичный интерфейс пользователя и принцип функционирования, с помощью которого конечный пользователь получает услугу.

- **Функциональный блок определения приложения и выбора клиента:** Позволяет конечному пользователю и/или оконечному устройству обнаружить имеющиеся в наличии и выбрать приложения и услуги приложений, предоставляемые поставщиком(ами) услуг.

Функции приложений IPTV: Логические объекты, которые образуют пункт происхождения некоторых услуг IPTV, таких как линейное TV, VoD и т. д., и которые способны гармонично сочетать все возможности поставщика услуг для оперативного предоставления некоторых услуг.

- **Функциональный блок определения и выбора приложения:** Взаимодействует с функциональным блоком определения приложения и выбора клиента, описанным выше, чтобы дать возможность конечному пользователю и/или оконечному устройству определить имеющиеся в наличии и приложения и услуги и сделать нужный выбор.

Функциональный блок профиля приложений: Хранит и управляет информацией о конфигурации приложений и услуг, как глобальных по своей природе, так и присущих конечному пользователю (абоненту); как правило, используется для разрешения сервера (серверам) приложений модифицировать услуги и контент под задачи конечного пользователя, этот блок будет часто взаимодействовать с различными системами учета или реализовывать такие системы на внутреннем уровне.

Функции подготовки контента: Выполняет предварительную обработку контента различных типов до его доставки абоненту; такой обработкой может быть анализ отслеживания контента, например введение меток и создание метаданных, мультиплексирование контента и метаданных контента, а также шифрование контента.

- **Функциональный блок обработки контента и меток:** Дополнительная стадия(и) обработки, анализирующая(ие) контент с целью создания метаданных отслеживания контента, например меток, для использования в последующей обработке нисходящего потока, в частности, в процессе индивидуализации таких метаданных идентифицируемых информацией из соответствующих источников.
- **Функциональный блок обработки метаданных:** Управляет и обрабатывает программно связанные метаданные и права использование информации, доставленной поставщиком контента.
- **Функциональный блок шифрования контента:** Выполняет шифрование (скремблирование) защищенного контента с целью осуществления управления доступом и конфиденциальности этого контента в процессе доставки; контент может быть зашифрован в режиме реального времени или зашифрован предварительно в автономном режиме, шифрование контента может поддерживать безопасное транскодирования без дешифрования.

ПРИМЕЧАНИЕ 1. – Шифрование контента может быть реализовано в функциях подготовки контента на прикладном уровне. В некоторых случаях оно может также дополнительно осуществляться в функциях доставки контента.

Функциональный блок управления правами и ключами: Соотносит права и ключи с контентом и управляет их распределением в пределах функционального блока защиты контента клиента в оконечном устройстве.

Функциональный блок клиента по защите контента: Получает или принимает права и ключи, используя эту информацию для управления расшифровкой контента, и обеспечивает выполнение правил пользования; необходимо, данный функциональный блок должен быть устойчивым к злонамеренным манипуляциям.

Функции доставки контента: Выполнение функций кэширования и хранения, а также доставки контента в соответствии с запросом от функций конечного пользователя; функции доставки контента могут выполнять дополнительную обработку, например кодирование или шифрование контента.

Функции клиента по доставке контента: Отвечают за прием контента в функциях оконечного устройства IPTV; выполняют дешифрование среды передачи контента, демультимплексирование, декодирование и последующую обработку, воспроизведение и хранение контента (эти функции также должны быть устойчивыми к злонамеренным манипуляциям).

- **Функциональный блок обнаружения меток:** Если этот блок имеется, то он определяет использование метки (меток) в контенте, полученном от поставщика(ов) услуг с целью проверки или введения желаемых правил использования контента в оконечное устройство или с оконечного устройства в интерфейсы нисходящих потоков.
- **Функциональный блок введения меток:** Если этот блок имеется, то он выполняет индивидуализацию экземпляров контента с целью их представления и последующего хранения или перераспределения.

Источники прав: Создание метаданных контента, связанных с правами использования контента.

Источники контента: Создание контента, который должен быть собран, обработан, а затем доставлен конечным пользователям с помощью услуг приложений, например линейное TV, VoD и т. д.

Функциональный блок внешних устройств хранения: Механизмы хранения контента после его получения, которые являются внешними по отношению к оконечному устройству (TD) и в которых хранение и использование контента не управляется оконечным устройством.

ПРИМЕЧАНИЕ 2. – Если существует внешнее хранение и его применение все время находится под управлением оконечным устройством, то оно может считаться внутренним устройством хранения, присоединенным через санкционированный, защищенный интерфейс, в зависимости от соответствия применяемого оконечного устройства и правил обеспечения устойчивости.

7.4.3 Функции и функциональные блоки архитектуры защиты услуг

Функциональный блок управления доступом к услугам: Отвечает, главным образом, за управление доступом к услугам; использует механизмы безопасности, например скремблирование и шифрование, которые используются этим функциональным блоком для предотвращения доступа или получения услуг пользователями без разрешения.

Функциональный блок клиента по управлению доступом к услугам: Выполняет задачи, обеспечивающие защиту на стороне клиента услуг, определенных в функциональном блоке управления доступом к услугам на стороне сервера.

Функциональный блок аутентификации услуг: Выполняет аутентификацию для проверки подлинности пользователя и/или оконечного устройства (TD), он также поддерживает запросы аутентификации, поступающие из TD для проверки сервера.

Функциональный блок клиента по аутентификации услуг: Кроме выполнения задач, связанных с аутентификацией абонента на стороне клиента, он также включает в себя функцию аутентификации на стороне сервера защиты услуг для взаимной аутентификации.

8 Механизмы безопасности

В данной Рекомендации не содержится четкого определения механизмов или решений безопасности, вместо этого, он в общих чертах описывает определенные механизмы безопасности, которые могут быть рассмотрены для целей определения и реализации механизмов, обеспечивающих выполнение требований в области безопасности, функциональные объекты архитектуры безопасности, а также угрозы безопасности.

Набор механизмов безопасности, описанных ниже, не является исчерпывающим решением для требований безопасности изложенных выше.

8.1 Механизмы безопасности, обеспечивающие защиту контента

Механизмы безопасности контента включают набор функций, действующих между источниками контента и оконечными устройствами, для гарантии безопасного распределения или передачи контента в сети, а также безопасного приобретения использования, экспорта, хранения и распределения или перераспределения конечным пользователем.

Механизмы безопасности контента могут быть применены к распределению контента, приобретению контента, потреблению контента, хранению контента, экспорту контента и перераспределению контента. Для удовлетворения требований по защите услуг и контента IPTV могут быть использованы следующие механизмы (все они не являются обязательными).

8.1.1 Шифрование контента

Во многих случаях контент может быть зашифрован для предотвращения незаконного использования во время доставки.

8.1.2 Отслеживание и идентификация контента

Отслеживание контента служит для идентификации и отслеживания происхождения (источника) контента и/или отвечающего за него участника, например конечного пользователя, с целью облегчения последующего расследования в случае несанкционированного доступа к контенту и его использования.

Информация отслеживания контента может быть присоединена к контенту в виде метаданных или в виде метки. Метки отслеживания контента, как правило, предназначены для надежной и незаметной защиты от умышленного или случайного удаления.

Для упрощения содержания идентификации контента рекомендуется использовать технологии видео-подписи.

8.1.3 Создание меток

Созданием меток называется процесс добавления информации к контенту посредством изменения некоторых характерных функций контента. Это область исследования известна как *стеганография*.

Создание меток является предпочтительным для многих приложений из-за трудностей, связанных с удалением из контента этой информации. Для услуг IPTV созданием меток может называться включение скрытой информации непосредственно в видео- или аудиопоток мультиплексированного контента. В идеале, метки являются невидимыми и/или неслышимыми для человека, но они будут успешно преодолевать преобразование форматов среды передачи.

8.1.4 Маркировка контента

Маркировка контента представляет собой процесс введения в контент или связывания с контентом метаданных, описывающих характер контента, а также аспекты контента и его особенности. Контент, маркированный такими метаданными, гораздо проще сортировать, фильтровать, либо классифицировать на промежуточных устройствах в цепи доставки контента.

Для некоторых регионов, администраций или конкретных вариантов реализации IPTV могут потребоваться определенные типы маркеров контента, например скорость передачи информации, позволяющая определенному количеству конечных пользователей (абонентов) управлять доступом к контенту, который считается нежелательным или вредным.

8.1.5 Безопасная схема транскодирования

Безопасная схема транскодирования (STS) относится к виду схем, позволяющих промежуточным сетевым узлам выполнить транскодирование сигнала без его дешифрования при сохранении сквозной безопасности. Эта схема может быть получена путем объединения масштабируемого кодирования, прогрессивного шифрования и пакетирования.

Для STS существуют три объекта: отправитель, промежуточный узел сети и пользователь с оконечного устройства IPTV. Отправитель выполняет функцию безопасного транскодирования, для того чтобы создать масштабируемые зашифрованные пакеты видеосигнала, и добавляет к передаваемой информации незашифрованный заголовок; промежуточный узел сети читает незашифрованный заголовок и использует эту информацию для выделения или удаления соответствующих пакетов в зависимости от желаемой операции транскодирования, оконечное устройство IPTV расшифровывает зашифрованные пакеты и декодирует обычные текстовые пакеты, получая в результате видеосигнал. Подробное описание приведено в Дополнении V к настоящей Рекомендации.

ПРИМЕЧАНИЕ. – Данный пункт не имеет цели определить или описать дополнительные механизмы для STS. Эта тема требует дальнейшего обсуждения в других Рекомендациях.

8.2 Механизмы безопасности, обеспечивающие защиту услуг

Механизмы безопасности услуг включают аутентификацию и санкционирование. Также возможна реализация конкретных механизмов управления доступом, таких как системы шифрования и дешифрования.

8.2.1 Аутентификация услуг

В случае управляемых услуг, в которых конечный пользователь (абонент) имеет прямую связь с определенным поставщиком услуг, поставщик услуг, как правило, требует, чтобы окончательные устройства и/или конечный потребитель (абонент) перед получением услуги были бы аутентифицированы безопасным образом. В таком случае аутентификация включает в себя создание и представление безопасным образом полномочий/информации, которые могут быть соотнесены с базой данных абонентов поставщика услуг с целью проверки аутентификации окончательного устройства и/или конечного пользователя в целях доставки услуг.

8.2.2 Санкционирование услуг

После аутентификации конечного пользователя (абонента) и/или окончательного устройства в целях предоставления услуг используется механизм санкционирования услуг, задачей которого является разрешение доступа и предоставление доступа к определенным услугам и размещенному в них контенту в соответствии с услугами и обслуживанием абонентов.

8.2.3 Управление доступом к услугам

В большинстве, если не во всех случаях система защиты услуг будет содержать механизмы, которые могут выполнять или выполняют шифрование (скремблирование) и дешифрование (дескремблирование), как трафика сигнализации управления услугами, так и трафика контента. Как правило, двусторонний трафик защиты услуг будет зашифрован в обоих направлениях: как от сервера к клиенту, так и от клиента к серверу. С другой стороны, потоки контента, как правило, будут зашифрованы только в направлении от сервера (поставщика услуг) к клиенту (оконечному устройству). Тем не менее, существуют такие сценарии использования, в которых поток контента может быть загружен клиентом на сервер и в этом случае такой контент для выполнения загрузки может быть зашифрован в окончательном устройстве, например, для того чтобы доступ к загруженному контенту мог получить только аутентифицированный и санкционированный поставщик услуг.

8.3 Механизмы безопасности, обеспечивающие защиту сети

В данной Рекомендации не содержится определения или описания механизма, обеспечивающего безопасность сети. В целом, ожидается, что реализация базовой сети, сети доступа, транспортной сети и сети доставки позволит введение любых механизмов, необходимых для защиты эксплуатационной целостности сети, включая, к примеру, обнаружение и предупреждение атаки типа Отказ в обслуживании (DoS). Как правило, механизмы обеспечения безопасности, задействованные поставщиками услуг IPTV и окончательными устройствами (TD), будут прозрачны для этих сетей, при условии, что эти механизмы безопасности действуют на том же уровне или уровне выше объектов данных нагрузки, обеспечиваемых уровнями сети.

8.4 Механизмы безопасности, обеспечивающие защиту окончательных устройств

Механизмы безопасности окончательных устройств включают в себя широкий спектр функциональных возможностей, в частности, безопасные, устойчивые к злонамеренным манипуляциям секретные хранилища данных, аутентификацию услуг, санкционирование услуг, шифрование и дешифрование сигналов управления, дешифрование контента, декодирование метаданных прав использования контента, выполнение правил использования контента, обнаружение и введение меток, программное управление и аутентификацию контента, обмен и межсетевое взаимодействие защиты контента, цифровой выходной порт (интерфейс) шифрования, устойчивость к злонамеренным манипуляциям на трассе передачи в среде передачи, подключаемые и возобновляемые процессоры и компоненты безопасности на основе аппаратных средств и программного обеспечения.

8.5 Механизмы безопасности, связанные с абонентами или конечными пользователями

Механизмы обеспечения безопасности абонентов или конечных пользователей, в первую очередь, связаны со сбором, хранением и передачей информации, которая может регулироваться принципами неприкосновенности частной жизни или конфиденциальности конечного пользователя. Поэтому эти механизмы могут быть распределены между точкой сбора, конечным устройством и поставщиком услуг, которые, возможно, собирают, сохраняют и повторно используют эту информацию. Таким образом, описания и определения этих механизмов, как ожидается, будут включены в пункты, описывающие услуги и безопасность конечных устройств.

В настоящее время в этой Рекомендации не определяются механизмы безопасности абонента или конечного пользователя. В дальнейшей работе над этой Рекомендацией, как ожидается, будут затронуты эти вопросы.

Дополнительная информация о безопасности абонентов приводится в Приложении А.

Приложение А

Защита безопасности абонентов

(Это Приложение является неотъемлемой частью настоящей Рекомендации)

А.1 Защита данных пользователей

При реализации услуг IPTV для главной категории пользователей важно уделять достаточное внимание безопасности и защите абонентских данных.

Абонентские данные могут также включать такую информацию отслеживания, как номер канала до и после изменения канала, время изменения, а также информацию пользователя для службы EPG, идентификацию пакета, время воспроизведения и т. д. Указанные данные являются по своей сути личными и конфиденциальными. Для защиты всех этих абонентских данных от злоупотребления требуется, чтобы поставщик услуг IPTV учитывал вопросы защиты неприкосновенности частной жизни пользователей.

- Услуга IPTV может дополнительно обрабатывать минимальный объем личных данных абонента, необходимый для предоставления услуг IPTV.
- Услуга IPTV до сбора информации, необходимой для доставки услуг IPTV может разъяснить использование личных данных абонента и получить согласие от абонента.
- Услуга IPTV может удалить личные данные абонента, ставшие ненужными для продолжения предоставления услуг IPTV.
- Если личными данными абонента управляет поставщик услуг, то услуга IPTV может дополнительно хранить собранные данные в режиме строгой секретности.

Существует множество способов, с помощью которых возможна утечка информации личных данных абонента: утечки из компании, предоставляющей услугу, утечки из сети, а также утечки из дома, например, через оконечные устройства. Здесь мы опишем методы защиты личных данных абонента для каждого из указанных вариантов утечки.

Для предотвращения утечки абонентских данных, поставщику IPTV услуг рекомендуется уделять особое внимание следующему.

- Необходимо разделить персональные данные абонента на те, которые требуют контроля и те данные, которые контроля не требуют.
- Необходимо обеспечить безопасное администрирование персональными данными абонента, требующими контроля.
- Необходимо обеспечить, чтобы личные данные абонента, требующие контроля, не использовались для иных целей, отличных от необходимых.

Рекомендуется, чтобы провайдеры услуг IPTV уделяли особое внимание изложенным ниже пунктам, касающимся услуг и транзакций, связанных с обработкой личных данных абонента.

- Необходимо разделить персональные данные абонента на те, которые требуют контроля и те данные, которые контроля не требуют.
- Для передачи персональных данных абонента, требующих контроля необходимо использовать зашифрованные каналы связи.

Поставщики услуг IPTV иногда хранят личные данные абонента в оконечном устройстве в целях повышения эффективности обслуживания. В таких случаях рекомендуется обратить особое внимание на изложенные ниже вопросы. Кроме того, рекомендуется, чтобы при обмене оконечных устройств учитывались аспекты безопасности.

- Требуется обеспечить, чтобы никакая третья сторона не могла легко прочитать личные данные абонента, хранящиеся внутри TD.
- Поставщики услуг IPTV могут по желанию контролировать доступ к личным данным абонента, хранящиеся в TD.

- Требуется обеспечить, чтобы личные данные абонента, хранящиеся в TD, могли быть полностью удалены абонентом или поставщиком услуг.
- В идеале, требуется, чтобы в ближайшем будущем оконечные устройства были защищены от атак вредоносных программ, например вирусов и программ-шпионов.

А.2 Родительский контроль, защита юридически несовершеннолетних, управление доступом

На платформе IPTV может быть использован механизм защиты юридически несовершеннолетних с целью ограничения доступа к IPTV контенту, который не должен быть доступен юридически несовершеннолетним лицам. В типичной ситуации оконечное устройство IPTV услуг используется в доме несколькими людьми совместно, в том числе юридически несовершеннолетними лицами. Рекомендуется, чтобы в оконечных устройствах поставщик услуг IPTV:

- Обеспечил, чтобы при необходимости на контент могли быть установлены права родительского контроля.
- Обеспечил, чтобы оконечные устройства могли эксплуатироваться в соответствии с правами родительского контроля.
- Обеспечил, чтобы в оконечных устройствах можно было изменить настройки родительского контроля.
- Обеспечил, чтобы с помощью оконечных устройств можно было осуществлять контроль на основе пароля, таким образом чтобы только юридические опекуны несовершеннолетних могли изменить настройки родительского контроля.
- Обеспечил, чтобы показатели контента можно было настроить для разных возрастных групп.
- Обеспечил, чтобы привилегии абонента могли быть разными для разных возрастных групп.
- Обеспечил, чтобы в оконечном устройстве была возможна авторизация юридически несовершеннолетних, просматривающих конкретный канал или контент, например, с использованием кода PIN.
- Обеспечил, чтобы опекуны, которые не находятся в непосредственной близости от юридически несовершеннолетних лиц, могли дистанционно контролировать и получать контент для юридических несовершеннолетних из сетевого хранилища копий.

Заметим, что для каждой администрации или региона в связи с третьими организациями может потребоваться рассмотрение условий по устранению вредного контента, поскольку это связано с управлением потоками контента и доступов. Можно предположить, что при подготовке исходного контента его создатель надлежащим образом учитывает вопросы одновременной передачи вещательных программ, и следовательно, увеличивается необходимость уделять достаточное внимание задержкам передачи и росту затрат на распределение.

Дополнение I

Угрозы безопасности

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации)

В этом дополнении описывается ряд выявленных угроз безопасности, затрагивающих некоторые требования и механизмы, описанные в данной Рекомендации.

Модель угроз безопасности и другие основные материалы были рассмотрены в соответствии со следующими Рекомендациями МСЭ-Т:

- [b-ITU-T X.800] определяет общие архитектурные объекты, связанные с обеспечением безопасности, которые могут быть соответствующим образом применены в условиях, когда требуется защитить связь между открытыми системами;
- [b-ITU-T X.805] определяет архитектуру безопасности сети для обеспечения сквозной безопасности сети.

Рекомендуется, чтобы стороны, интересующиеся аспектами безопасности IPTV, прочли указанные основные Рекомендации по безопасности; предполагается, что читатель данной Рекомендации знаком с информацией, представленной в этих Рекомендациях.

В [b-ITU-T X.800] и [b-ITU-T X.805] определяются следующие угрозы безопасности для сетей, которые также являются угрозами безопасности для услуг и приложений контента, применимых к IPTV:

- уничтожение информации и/или других ресурсов;
- искажение или изменение информации;
- кража, удаление или потеря информации и/или других ресурсов;
- раскрытие информации;
- прерывание обслуживания.

I.1 Модель угроз безопасности

Угрозы безопасности для IPTV можно разделить на следующие виды: угрозы безопасности контента, угрозы безопасности услуг, угрозы безопасности сетей, угрозы безопасности оконечных устройств и угрозы безопасности абонента.

На рисунке I.1 изображена модель угроз безопасности, которая показывает взаимосвязь между этими угрозами.

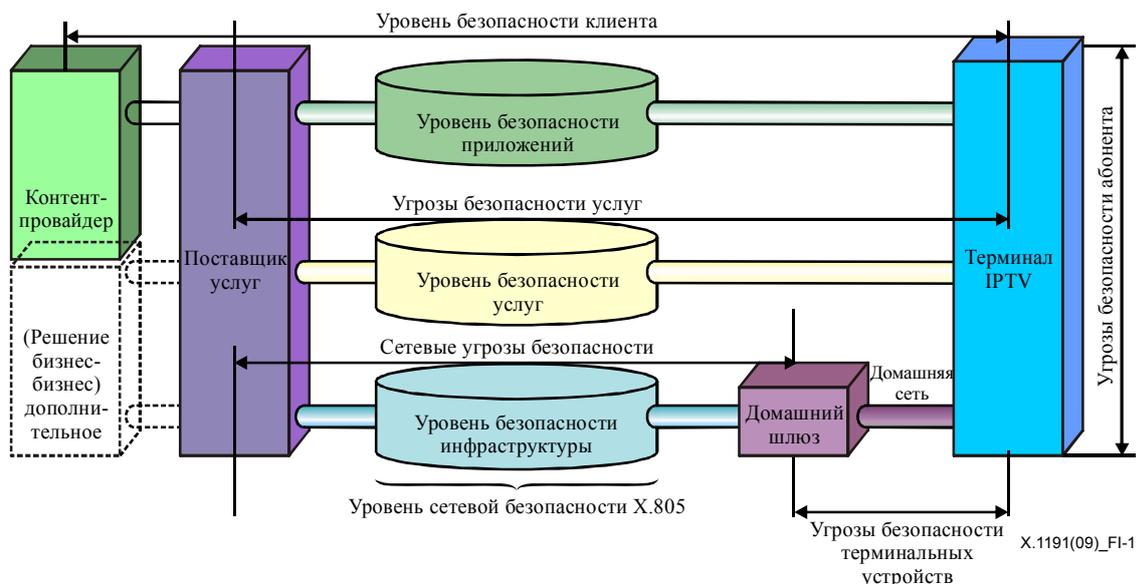


Рисунок I.1 – Модель угроз безопасности

I.1.1 Угрозы безопасности контента

Активы контента: активы, которые принадлежат поставщику контента и/или поставщику услуг, могут потребляться конечным пользователем с помощью TD.

Активы контента, которые должны быть защищены, включают контент линейного ТВ, контент VoD, контент опроса VoD, контент PVR, загруженные приложения и т. д.

Ниже перечислены угрозы для этого контента:

- Перехват: нарушение конфиденциальности цифрового контента посредством незаконного мониторинга сетей предоставления услуг;
- Несанкционированный просмотр;
- Несанкционированное воспроизведение или распространение.

I.1.2 Угрозы безопасности услуг

Активы услуг: активы, которые принадлежат поставщику услуг; они включают в себя медиасерверы, серверы SCP, а также оперативную информацию, как минимум, такую, как регистрация услуг и информация биллинга.

Ниже перечислены угрозы для услуг:

- Нарушение авторских прав на программы, предоставляемые абонентам на платформе услуг IPTV;
- Нелегальное проникновение/обман (спуфинг) поставщика услуг IPTV;
- Злонамеренные угрозы, ориентированные на серверы IPTV (серверы SCP, медиасерверы и т. д.), могут включать в себя взлом, с целью вызвать утечку прикладного программного обеспечения или протокола связи, атаку типа "отказ в обслуживании" и т. д.;
- Кража информации абонента, при которой часто используются вредоносные программы, такие как Троянский конь, это может быть идентификатор, информация биллинга, информация о подписке.

I.1.3 Угрозы безопасности сети

Активы сети: активы, которые принадлежат поставщику сети; они могут включать в себя физическое оборудование, например маршрутизаторы, коммутаторы и сетевые ресурсы, например, пропускную способность, услуги многоадресной передачи и т. д.

Ниже приводятся сетевые угрозы:

- Умышленные угрозы, нацеленные на сетевое оборудование или ресурсы (пропускную способность): злонамеренные атаки на канал передачи сети, подобные отказу в обслуживании;

- Угрозы безопасности для техники многоадресной передачи, используемой в канале передачи сети IPTV, например нелегальное проникновение/обман (спуфинг) источников ТВ сигнала для многоадресной передачи или незаконная многоадресная передача членам групп;
- Злонамеренные атаки, например DoS или взлом, на узлах сети распределения контента.

1.1.4 Угрозы безопасности конечных устройств

Активы конечных устройств: Активы, которые принадлежат конечному устройству, которые могут быть использованы конечным пользователем для обработки и хранения контента и другой соответствующей информации для услуг IPTV.

Ниже перечислены угрозы для конечных устройств:

- Незаконный доступ к чистому контенту путем злонамеренных манипуляций аппаратным или программным обеспечением устройства, например чистый контент может быть скопирован путем перехвата с шины данных или взлома программного обеспечения;
- Незаконный доступ к ключам или другой секретной информации в устройствах с использованием взлома программного обеспечения или манипуляций аппаратными средствами; злоумышленники могут манипулировать памятью устройства или анализировать поток данных для получения ключей и других секретных данных. Действия с ключами контента приводят к утечке контента, а утечка ключа устройства приводит к заимствованию прав устройства;
- Сбой функций устройства аппаратными методами, такими как управление системными часами устройства для отключения функций SCP систем, либо с помощью программных методов, таких как загрузка вирусов для исчерпания ресурсов устройства;
- Несанкционированные приложения, например программы, которые были загружены, запущены и хранятся в конечных устройствах;
- Сбой работы конечного оборудования (аппаратный и программный), вызванный злонамеренными кодами/вирусами из сети;
- Неаутентифицированные конечные устройства, подключенные к домашней сети;
- Несанкционированное использование ресурсов абонентами.

1.1.5 Угрозы безопасности абонента

Активы абонента: Активы, которые принадлежат абоненту, они могут включать в себя информацию об абоненте, семье абонента их соединениях IPTV и т. д.

Для обеспечения безопасности абонента требуется, чтобы механизм обеспечения безопасности контента и механизм обеспечения безопасности услуг работали в тесной взаимосвязи друг с другом, поскольку услуга IPTV включает в себя услугу, в которой безопасность контента и безопасность услуг действуют в тесной взаимосвязи друг с другом.

Примеры угроз абонента перечислены в таблице 1.1.

Таблица 1.1 – Категории безопасности абонентов

	Безопасность абонента		
	Пример услуги	Пример угрозы	Пример механизма защиты
Безопасность контента	Линейное ТВ, услуга VoD	Нелегальное копирование	Идентификация TD (защита услуг, защита контента)
Безопасность услуг	Двунаправленная услуга	Фишинг	Персональная идентификация (защита личных данных, PIN/пароль)
	Родительский контроль	Спуфинг	Персональная идентификация (PIN/пароль, аутентификация)
Безопасность сети	Не определена	Подслушивание	Идентификация абонентской линии Шифрование данных, совместный контроль многоадресной передачи
Безопасность конечных устройств	Услуга P2P	Нелегальное копирование	Защита контента (P2P)

Дополнение II

Функциональная совместимость систем SCP

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации)

II.1 Обзор функциональной совместимости систем SCP

Существует несколько сценариев функциональной совместимости систем SCP: SCP-EE, SCP-B и SCP-IX. Функционально совместимая система SCP может применяться либо в области поставщика услуг, либо в области конечного пользователя. Это дополнение касается только стороны конечного пользователя.

II.2 Сценарии функциональной совместимости систем SCP

Сценарии функциональной совместимости систем SCP подразделяются как минимум на три вида: сквозная SCP (SCP-EE), мостовое подключение SCP (SCP-B) и обмен SCP (SCP-IX).

(1) Сквозная SCP (SCP-EE)

SCP-EE: Два или более устройств, использующих одну SCP, обмениваются контентом и получают доступ к нему в соответствии с предоставленными правами. Этот режим проще всего реализовать, поскольку используется только одна SCP.

(2) Мостовое подключение SCP (SCP-B)

SCP-B: На одном TD задействовано две или более системы SCP. Контент, приобретенный через одну систему SCP, например, из сети, может быть доступен через другую SCP, расположенную в том же устройстве, в соответствии с предоставленными правами.

(3) Обмен SCP (SCP-IX)

SCP-IX: Данный случай характеризуется двумя или более устройствами, при этом каждое устройство имеет одну или более используемых SCP. Контент, приобретенный одним устройством через одну из его систем SCP, может быть безопасно передан и получен на другом устройстве с помощью различных систем SCP в соответствии с предоставленными правами.

На рисунке II.1 иллюстрируется модель, описанная выше.

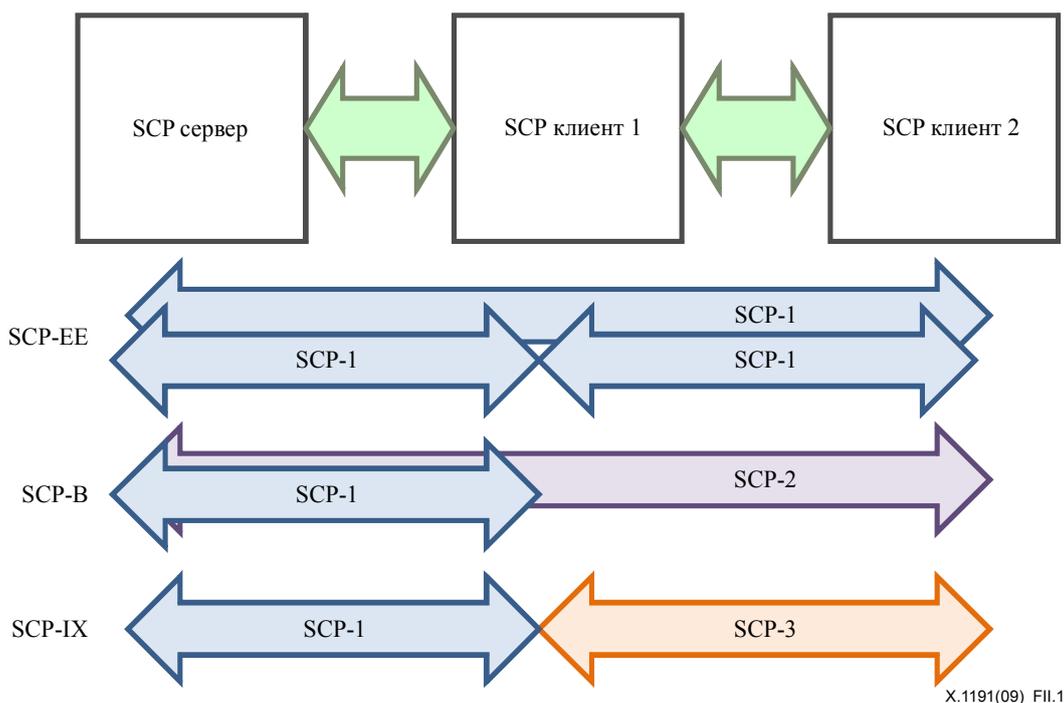


Рисунок II.1 – Режим функциональной совместимости систем SCP

II.3 Технические области функциональной совместимости систем SCP

Следующие области представляют собой ключевые элементы функциональной совместимости SCP в режимах SCP-EE, SCP-B и SCP-IX.

1 Аутентификация устройств, пользователей и систем SCP

Прежде чем может быть произведена передача контента между объектами, необходимо безопасно установить идентификатор оконечного устройства и его возможного(ых) пользователя(ей). Кроме того, поскольку поставщики контента не могут доверять конкретным SCP, необходимо сделать возможной аутентификацию принимающих SCP или уровней реализации до взаимного обмена контентом. Такая аутентификация должна иметь надежную криптографическую основу и возможность использовать различные широко известные методы цифровой подписи. Шифрование с открытым ключом, в частности, обеспечивает надежный механизм для цифровых подписей в протоколах аутентификации.

2 Обмен выражениями прав

Различные SCP используют различные языки выражения прав или форматы лицензий. Для режимов функционирования SCP-B и SCP-IX требуются общие средства выражения прав. Они могли бы принять форму общего языка выражения прав (REL) или транслятора выражения прав. Другим возможным механизмом обмена выражениями прав является согласование лицензий.

3 Общие алгоритмы шифрования для обмена контентом

Для безопасной передачи контента из зоны контроля одной SCP до зоны контроля другой SCP или в пределах той же SCP, но на другие физические устройства, требуется шифрование контента. Контент становится непригодным к использованию любыми объектами, за исключением тех, которые имеют соответствующий ключ или ключи, необходимые для дешифрования. Существует множество различных типов алгоритмов шифрования (блочный шифр, потоковый шифр, шифрование с открытым ключом и т. д.), но те алгоритмы, в которых используются симметричные ключи, как правило, наиболее подходят для высокоскоростного обмена контентом. В целях функциональной совместимости должно быть выбрано небольшое количество общеизвестных алгоритмов. В идеале должен быть определен один алгоритм по умолчанию.

4 Управление или обмен ключами управления для общих алгоритмов шифрования

Прежде чем может иметь место обмен безопасным контентом, необходимо передать или, в общем случае, сгенерировать ключи, которые будут использоваться в конкретных случаях. Управление ключами, как правило, в системе безопасности является наиболее трудной частью для выполнения. Такие методы, как шифрование с открытым ключом, упростили распределение ключей для устройств, но для установления и поддержания адекватности этих ключей требуется инфраструктура открытых ключей (PKI). Такая инфраструктура может быть санкционирована и может поддерживаться лицензирующим органом, ответственным за защиту контента, в отличие от общей сетевой безопасности.

5 Безопасность загрузки клиента SCP

В идеале, любое оконечное устройство должно иметь возможность обмениваться контентом, законным образом полученным от других устройств и/или с использованием каких-либо SCP в соответствии с предоставленными правами, например в режиме SCP-IX. Заметим, однако, что предварительная загрузка каждой системы SCP на каждое TD в процессе производства, требуемая рынком, вряд ли практична, поэтому необходимо обеспечить безопасный механизм для загрузки и выполнения выбранной системы SCP на оконечном устройстве. В этой области взаимодействия определенную роль играют такие объекты, как безопасная загрузка и протоколы безопасной загрузки.

ПРИМЕЧАНИЕ. – При использовании взаимодействия SCP в оконечных устройствах и системах, устройства IPTV должны иметь надежную архитектуру для обеспечения функциональной совместимости систем защиты контента.

6 Безопасный экспорт прав

Для безопасного экспорта цифровых прав клиент SCP IPTV должен проверить, разрешают ли права использовать экспорт, ориентированный на систему SCP. Цифровые права могут иметь форматы, позволяющие целевой системе SCP экспортировать права. В этом случае, клиент SCP IPTV должен проверить эти форматы прав и разрешить соответствующей целевой системе SCP экспорт цифровых прав.

II.4 Функционально совместимые архитектуры SCP

Можно рассмотреть два вида совместимой архитектуры SCP: первый основан на архитектуре обеспечения функциональной совместимости с помощью посредника, которая для выполнения транзакций для обработки совместимой передачи использует промежуточную систему, расположенную между двумя системами SCP. Другой вариант является архитектурой на основе стандартного протокола, использующей стандартные интерфейсы и протоколы для преобразования защищенного цифрового контента и связанной с ним информации между двумя различными системами SCP.

Два возможных варианта архитектуры приведены на рисунках II.2 и II.3.

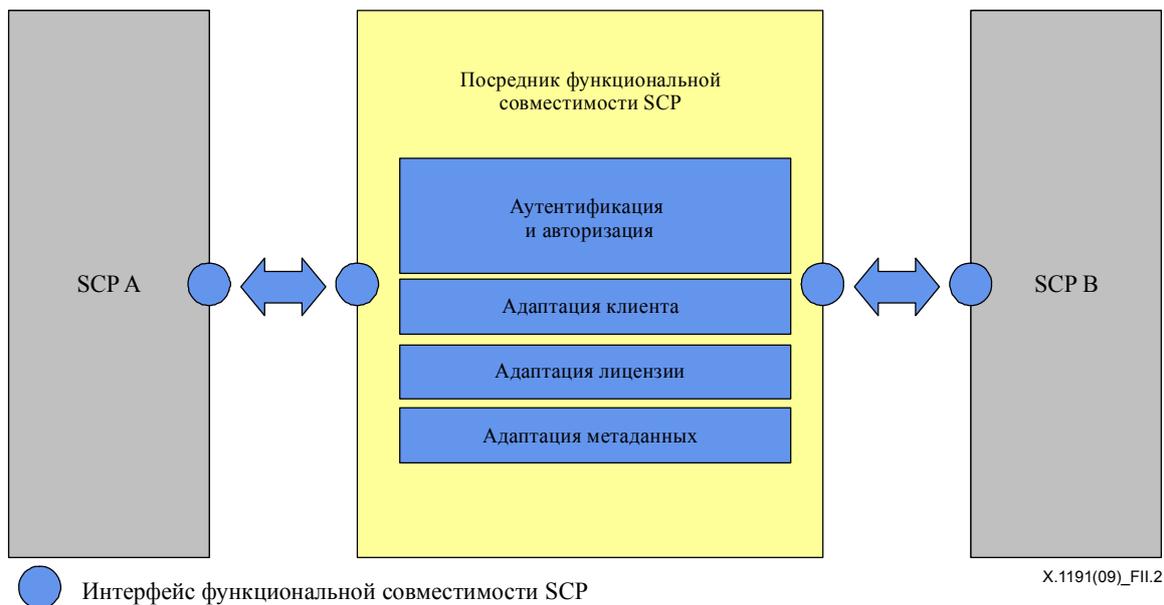


Рисунок II.2 – Архитектура обеспечения функциональной совместимости с помощью посредника



Рисунок II.3 – Архитектура обеспечения функциональной совместимости на основе стандартного протокола

Описание функциональных блоков

- **Адаптация контента:** Адаптация контента отвечает за преобразование алгоритма шифрования. Несколько заданных предварительно определенных стандартных алгоритмов шифрования упростят этот процесс.
- **Адаптация лицензии:** Адаптация лицензии отвечает за преобразование лицензии. Любая временная или стандартная лицензия, известная обеим сторонам, должна поддерживать почти такое же право поведения (активы среды передачи и пара полномочий потребления), которые определены в первоначальной лицензии. Ряд преобразований прав (преобразование форматов прав и семантическое преобразование) может быть включен в адаптацию лицензии. Кроме того, адаптация лицензии может нести ответственность за изменение информации о правах и ее безопасную доставку целевым клиентам SCP.
- **Адаптация метаданных:** Адаптация метаданных отвечает за преобразование информации метаданных. Временные или стандартные метаданные, известные обеим сторонам, должны поддерживать ту же информацию, что исходные метаданные. В адаптацию метаданных может быть включен ряд преобразований метаданных (синтаксические и семантические преобразования). Кроме того, адаптация метаданных может нести ответственность за повторную информацию, метаданных и надежно доставлять их на другой участок SCP.
- **Аутентификация и санкционирование:** Каждая вовлеченная сторона SCP должна рассудить, соответствует ли другая сторона целям достижения функциональной совместимости SCP. Обычно это сопровождается процессом взаимной аутентификации в качестве предварительного шага между двумя сторонами SCP.

Исключительный случай: Если SCP A и SCP B находятся в одном и том же устройстве или в случае специального защищенного канала связи между двумя SCP, процесс адаптации контента может не потребовать функциональной совместимости.

II.5 Сценарии, при которых SCP-B или SCP-IX применяются в оконечном устройстве

В этом пункте описывается три возможных сценария, требующих взаимного обмена SCP между защитой услуг и защитой контента.

II.5.1 Определения терминов используемых в схеме

- Входной порт, через который защищаемый контент IPTV поступает на SCP;
- Выходной порт, через который защищаемый контент IPTV покидает SCP.

II.5.2 Сценарий 1: SCP с SCP_IX

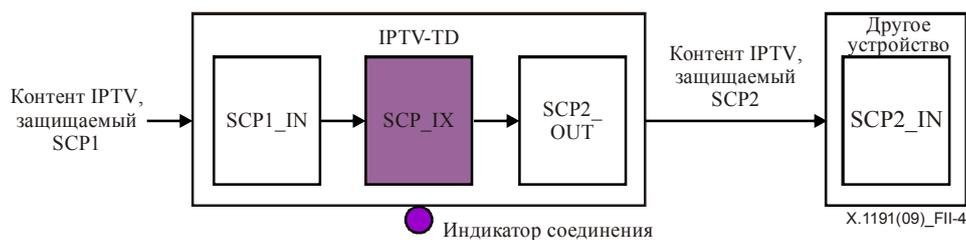


Рисунок II.4 – SCP с SCP_IX

В этом случае оконечное устройство (TD) IPTV имеет систему SCP с SCP_IX для поддержки функциональной совместимости между IPTV TD без хранения, которая принимает только определенные услуги безопасности и внешние устройства с функцией хранения, имеющие только определенную защиту контента.

Для обеспечения безопасной и гибкой связи с внешними устройствами, принимающими различные механизмы защиты контента, IPTV TD должны иметь скорее SCP_IX, нежели осуществление время от времени безопасного соединения между двумя устройствами.

II.5.3 Сценарий 2: SCP с дополнительным SCP-B и хранением

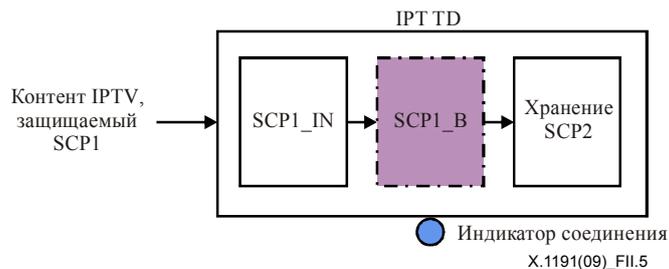


Рисунок II.5 – SCP с дополнительным SCP-B и хранением

В данном случае TD IPTV имеет SCP с SCP-B для обеспечения функциональной совместимости между защитой услуг и защитой контента на одном устройстве.

Производитель IPTV TD может применять собственный механизм защиты контента для внутреннего хранения. В таком случае, SCP_B не является необходимым и для хранения может использоваться SCP1.

Для поддержки гибкого подключения к какому-либо виду внутреннего хранения, принимающему различные механизмы защиты контента, рекомендуется, чтобы TD IPTV было оборудовано SCP_B, а не случайным вариантом реализации безопасного соединения между защитой услуг и защитой контента.

II.5.4 Сценарий 3: SCP с хранением и SCP_IX

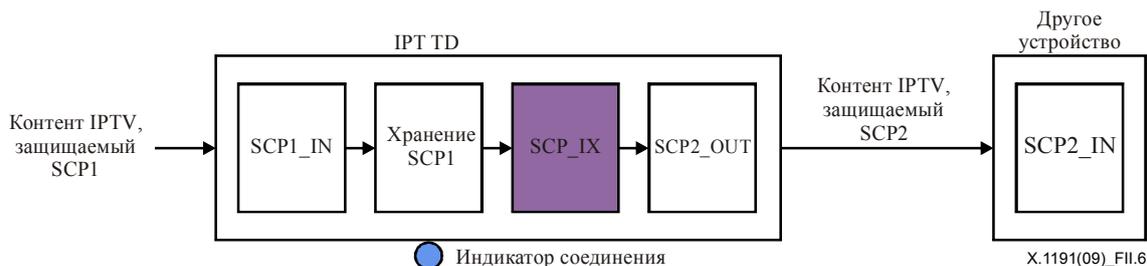


Рисунок II.6 – SCP с хранением и SCP_IX

В этом случае, IPTV TD имеет SCP с хранением и SCP_IX для поддержки функциональной совместимости между внутренним и внешним механизмами защиты контента.

Для поддержки гибкого подключения к какому-либо виду внутреннего хранения, принимающему различные механизмы защиты контента, рекомендуется, чтобы TD IPTV было оборудовано SCP_B, а не случайным вариантом реализации безопасного соединения между защитой услуг и защитой контента.

Дополнение III

Пример процесса защиты контента IPTV

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации)

Ниже описывается пример обработки VoD приложения для защиты контента:

- *Этап аутентификации абонента*
 - Абонент выбирает приложение VoD посредством "функционального блока клиента для обнаружения и выбора услуг и приложений".
 - После получения "функционального блока профиля приложения", "функции приложений IPTV" отправят запрос для проверки этого абонента. В случае успешной авторизации, информация, относящаяся к этому абоненту, будет сохраняться в кэш-памяти "функционального блока профиля приложения" для поиска.
- *Этап выбора контента*
 - Абонент может выбрать определенную среду контента из ECG и "функциональный блок приложения VoD" доставит на TD информацию о местоположении выбранного контента (URL).
 - "функциональный блок клиента для приложения VoD" получит данные о местоположении контента для передачи в "функции доставки приложений клиента".
- *Этап шифрования доставляемого контента*
 - "функции доставки приложений клиента" применяются для (шифрованного) медийного контента, используя информацию о местоположении контента, они также применяются к правам и ключам из "функционального блока клиента для защиты контента", относящимся к этому контенту.
- *Фаза распределения ключей и прав*
 - Если нет прав и ключей, "функциональный блок клиента для защиты контента" запросит такую информацию у "функционального блока управления правами и ключами" поставщика услуг IPTV.
 - "функциональный блок управления правами и ключами" применит информацию авторизации, связанную с этим абонентом, к "функциональному блоку профиля приложения" для проверки с помощью имеющейся информации, имеет ли данный абонент права получить запрошенный контент.
 - При успешной проверке, права и ключи для выбранного контента будут доставлены на "функциональный блок клиента для защиты контента".
 - После получения прав и ключей, "функциональный блок клиента для защиты контента" передаст ключ и право "функциям клиента для доставки контента", для расшифровки контента и управления его использованием.

Дополнение IV

Управление защитой и копированием контента DVB

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации)

В настоящем дополнении содержится краткое изложение ряда спецификаций по защите контента и управлению копированием DVB (DVB-CPCM), которые были разработаны ETSI.

Система DVB-CPCM является примером полностью стандартизированной системы защиты телевизионного и другого контента в домашней сети и за ее пределами. Система DVB-CPCM может получать контент от определенных МСЭ (или другими организациями) механизмов защиты контента IPTV и поддерживать защиту контента IPTV в течение всего жизненного цикла контента от получения до потребления, включая хранение, обработку и экспорт защищенного контента на другие механизмы обеспечения безопасности IPTV при одновременном сохранении правильного санкционированного использования.

IV.1 Введение

Система DVB CPCM является системой для защиты контента и управления копированием коммерческого и бесплатно распространяемого цифрового контента, доставляемого для использования домашними устройствами и сетями. Система CPCM управляет использованием контента на всех этапах: от подачи его в систему CPCM до конечного потребления или экспорта из системы CPCM в соответствии с особыми правилами использования такого контента. Система CPCM предназначена для использования при защите всех типов контента, например аудио-, видео- и связанных с ними приложений и данных. Система CPCM предоставляет спецификации для облегчения взаимодействия такого контента после подачи его в систему CPCM сетевыми потребительскими устройствами как для домашних сетей, так и для удаленного доступа. Спецификация состоит из частей, некоторые из которых определяют сигнализацию и действия, необходимые для соблюдения технических требований, а другие части объясняют логику предпосылок спецификации, в том числе Реализацию руководящих принципов. Эталонная Модель является основой для системы CPCM и служит концепцией, на которой базируются остальные объекты спецификации.

IV.2 Определения

Наряду с терминами, содержащимися в основном тексте, в настоящем Дополнении определяются следующие термины:

IV.2.1 получать (acquire): Означает прием и поглощение системой CPCM контента извне CPCM системы.

IV.2.2 точка получения (acquisition point (AP)): Абстрактный функциональный объект системы CPCM, в котором происходит получение контента.

IV.2.3 получение (acquisition): Прием и поглощение системой CPCM контента извне CPCM системы.

IV.2.4 санкционированная область (authorized domain ((AD)): отличительный набор CPCM DVB-совместимых устройств, которые находятся в собственности, арендуются или управляются членами одного домохозяйства; домохозяйством считается ячейка общества, состоящая из всех людей, которые живут вместе, занимая одно и то же место жительства. Здесь не делается никаких предположений относительно физического расположения устройств, принадлежащих, арендуемых или управляемых членами семьи.

IV.2.5 санкционированное использование (authorized usage): Разрешенное использование контента, состоит из ряда утверждений правил использования, применяемых к данному контенту.

IV.2.6 потреблять (consume): Означает материальную передачу контента или вывод ограниченного контента из ограничений любого другого использования.

IV.2.7 точка потребления (consumption point (CP)): Абстрактный функциональный объект системы CPCM, в котором происходит потребление контента.

IV.2.8 потребление (consumption): Материальная передача контента или выходного устройства, содержащая преобразование или сигнал, препятствующий любому другому использованию, нежели немедленное преобразование контента в звук и изображение.

IV.2.9 единица контента (content item): Дискретный экземпляр контента конечной длительности, например программа/мероприятие или их неполная часть.

IV.2.10 лицензия контента (content license): Безопасно поддерживаемая и доставляемая структура данных, содержащая информацию, необходимую для управления безопасностью единицы контента системы CPCM.

IV.2.11 контент (content): Данные, которые охраняются системой CPCM; обычно этот термин относится к аудиовизуальному контенту, включая дополнительные данные сопровождения, например субтитры, картинки/графику, анимацию, веб-страницы, текст, игры, программы (как исходные коды, так и объектные коды), скрипты или любую другую информацию, доставляемую и потребляемую пользователем.

IV.2.12 копия (copy): Процесс, управляемый системой CPCM, в результате которого из полученного контента или из существующих хранимых единиц контента создается новая единица контента.

IV.2.13 устройство CPCM (CPCM device): Устройство, содержащее один или более экземпляров CPCM.

IV.2.14 система CPCM (CPCM system): Набор полностью совместимых CPCM устройств.

IV.2.15 приложение устройства (device application): Любая функциональная возможность в CPCM устройстве, не относящаяся к CPCM.

IV.2.16 точка экспорта (export point (EP)): Абстрактный функциональный объект системы CPCM, в котором CPCM контент покидает систему CPCM.

IV.2.17 экспорт (export): Передача контента CPCM из-под четкой защиты и управления системы CPCM на контролируемый CPS, доверенный CPS или в недоверенную область.

IV.2.18 переместить (move): процесс копирования, при котором оригинал удаляется, стирается или становится недоступен.

IV.2.19 выход (output): Устройство интерфейса или CPS, используемое для передачи контента CPCM, потребленного контента или экспортированного контента.

IV.2.20 блок обработки (processing entity (PE)): Абстрактный функциональный объект системы CPCM, в котором обрабатывается контент CPCM.

IV.2.21 обработка (processing): CPCM-совместимые операции по шифрованию или дешифрованию контента на этапе потребления или экспорта, например контент CPCM проходит разрешенное преобразование из своей первоначальной формы для создания нового преобразованного контента CPCM или такой извлеченной из контента информации, как уровень громкости звука или неподвижные изображения.

IV.2.22 информация о состоянии использования (usage state information ((USI)): Метаданные контента CPCM, сообщающие о санкционированном использовании сигналов для каждой единицы контента CPCM.

IV.2.23 просматривать (view): Потреблять.

ПРИМЕЧАНИЕ. – Это также включает в себя прослушивание только аудио контента.

IV.2.24 просмотр (viewing): Потребление.

ПРИМЕЧАНИЕ. – Это также включает в себя прослушивание только аудио контента.

IV.3 Сокращения и акронимы

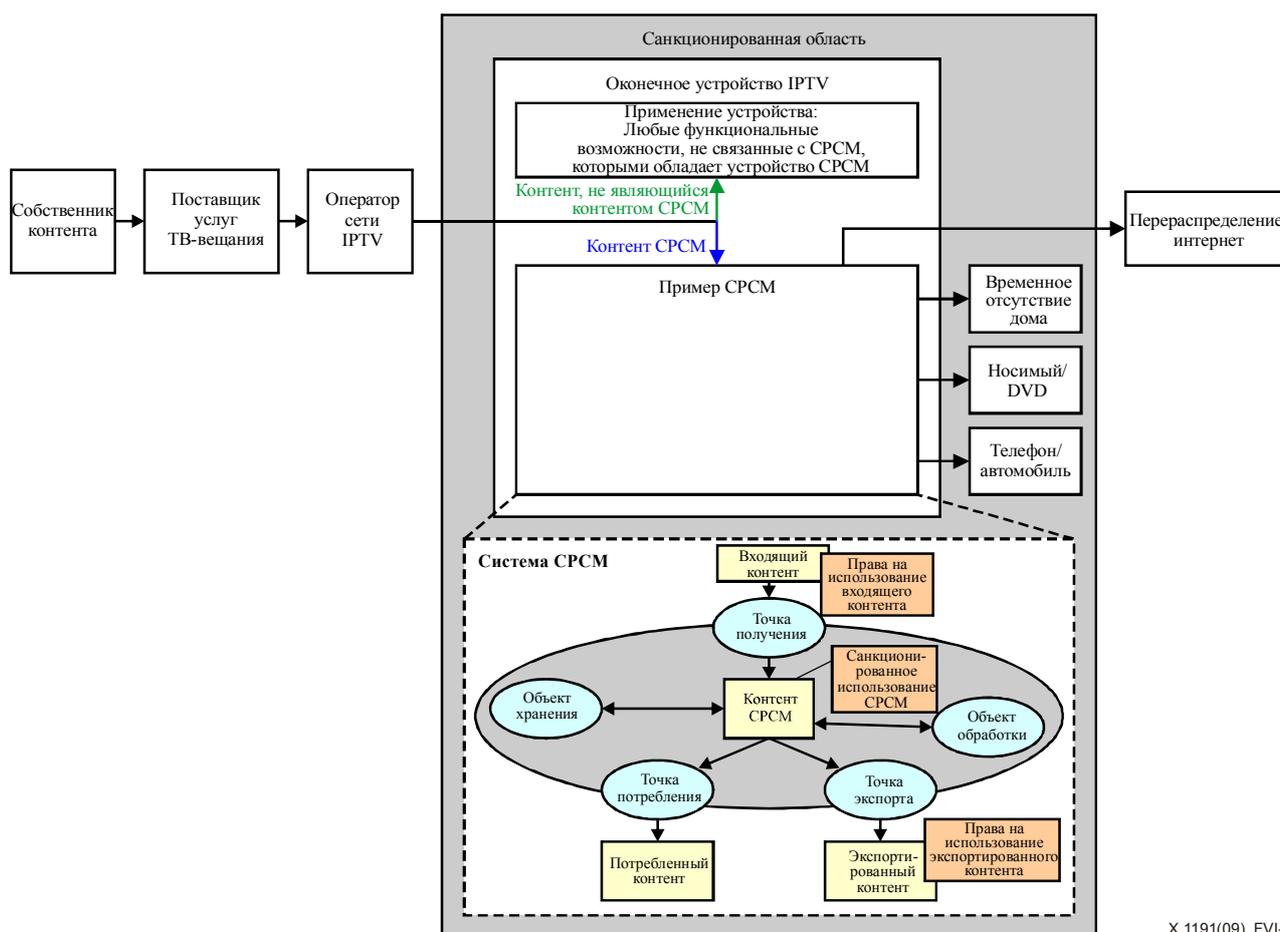
Наряду с сокращениями, содержащимися в основном тексте, в настоящем Дополнении используются следующие сокращения:

AP	Acquisition Point	Точка получения
APECS	Acquisition, Processing, Export, Consumption, Storage	Получение, обработка, экспорт, потребление, хранение
CL	Content License	Лицензия контента
CP	Consumption Point	Точка потребления

CPCM	Content Protection and Copy Management	Защита контента и управление копированием
CPE	Customer Premise Equipment	Абонентское оборудование
CPS	Content Protection System	Система защиты контента
DVB	Digital Video Broadcasting	Цифровое телевизионное вещание
EP	Export Point	Точка экспорта
PE	Processing Entity	Блок обработки
SE	Storage Entity	Блок хранения
USI	Usage State Information	Информация о состоянии использования

IV.4 Архитектура CPCM

В центре системы CPCM расположена "санкционированная область" – совокупность устройств, принадлежащих домохозяйству, даже если они расположены далеко от дома. Концепция AD признает, что в эпоху сетевых развлечений привязка контента к одной телевизионной приставке (TD) и присоединение к ней ТВ-дисплея недостаточно. Система CPCM получает контент из надежных источников, таких как система SCP IPTV, на целое TD или его часть и защищает полученный поток или файл контента, управляя тем, как он может быть просмотрен, перемещен и скопирован. Являясь основой модели управления контентом CPCM, входящий контент поступает в систему CPCM и становится контентом CPCM. Управление контентом CPCM и его защита осуществляется в системе CPCM; контент покидает систему CPCM, когда он потребляется пользователем или экспортируется в другую систему.



X.1191(09)_FVI-1

Рисунок IV.1 – Поток контента в среде CPCM

СРСМ поддерживает различные виды использования контента в домашней сети, она также может управлять доступом к контенту из удаленных мест, таких как ноутбук при широкополосном соединении с интернетом. Используя систему СРСМ, поставщики услуг могут сообщать производителям устройств разрешенные сценарии для каждого типа контента. Это охватывает многие методы защиты, такие как применяемые в технологиях SCP IPTV, когда контент, как правило, ограничивается от точки к точке кабелем связи между источником контента, например телевизионной приставкой и устройством воспроизведения цифрового контента.

Система СРСМ выходит за рамки подобной локализованной защиты, предоставляя вещателям, операторам сетей и собственникам контента возможность разрешить члену семьи доступ из удаленного места, например из гостиницы во время командировки или отпуска.

Система СРСМ также может разрешить пользователям копирование контента на портативные устройства и съемные носители, например DVD. Пока устройство воспроизведения принадлежит к той же санкционированной области, устройство сможет воспроизводить содержимое, даже если оно отключено от дома и исходных услуг. Контент СРСМ не требует он-лайн авторизации от поставщика услуг для добавления или удаления устройств в/из санкционированной области.

Система защиты контента СРСМ не является автономным образованием, она включается/входит в общую сквозную систему распределения SCP IPTV. По сути, она сосуществует с системой SCP IPTV, а не заменяет ее. В любом TD использование системы СРСМ не является обязательным, если не оно представлено, однако, в таком случае TD не будет предоставлен доступ к любому СРСМ-защищенному контенту. Тем не менее, TD не нужно внедрять все СРСМ объекты. Требуется внедрять только те, что полезны для данного TD в свете выполнения им функциональных потребностей. Например, простое устройство может осуществлять только функциональные возможности получения и потребления СРСМ, если ему не требуются функции хранения или экспорта СРСМ.

IV.5 Эталонная модель СРСМ и функциональные объекты

Эталонная модель определяет набор из пяти абстрактных функций управления, охватывающих все сценарии использования контента в среде потребителя: получение, хранение, обработка, потребление и экспорт. Эти функции преобразуются в пять функциональных объектов: точка получения, объект хранения, объект обработки, точка потребления и точка экспорта. На рисунке VI.1 показан вид системы СРСМ с точки зрения набора абстрактных функциональных объектов.

Таким образом, контент, входящий в систему СРСМ, для того чтобы стать контентом СРСМ, должен быть получен в точке получения устройством СРСМ, выполняющим роль такой точки получения. Контент СРСМ может храниться или обрабатываться соответствующими функциональными объектами (объектом хранения, объектом обработки) реализованными в устройстве СРСМ. Контент СРСМ покидает систему СРСМ при его потреблении в точке потребления или при его экспорте в точку экспорта. И в этом случае эти функциональные объекты могут быть реализованы в любом устройстве СРСМ.

IV.6 Санкционированная область СРСМ

Устройства СРСМ могут быть логически сгруппированы в санкционированной области. Если все эти устройства принадлежат одному домохозяйству, то они могут определять санкционированную область домохозяйства (AD). Таким образом, санкционированную область определяет место назначения для контента, преобразуемого в рамках одного домохозяйства. В общем случае, AD можно рассматривать как логическое группирование всех устройств СРСМ, принадлежащих одному домохозяйству, устройств, расположенных в основном месте жительства, устройств, расположенных в другом месте жительства (например, в коттедже), переносных портативных устройствах, которые только периодически связываются с вышеуказанными стационарными устройствами или устройствами, установленных на транспортном средстве(ах), принадлежащих этому домохозяйству. AD предназначен для автономной логической группы устройств, она не требует какого-либо внешнего управления. Заметим, однако, что могут быть случаи, когда AD связана с конкретным поставщиком услуг, который может предложить управление AD, как часть предоставляемых потребителю услуг.

IV.7 Правила использования контента СРСМ

Санкционированная область для любой единицы контента СРСМ – это ряд установок использования, выраженных в правилах использования контента СРСМ. Правила использования СРСМ могут быть установлены для поставщика контента или поставщика услуг или преобразованы из формата доставки (например, бесплатное радиовещание). Степени, до которых могут выполняться операции хранения, потребления и экспорта операций, могут быть предметом санкционированного использования контента. СРСМ определяет общий набор правил использования, каждый поставщик контента может выбрать и извлекать необходимую санкционированную область контента в соответствующей системе СРСМ. Набор правил использования СРСМ разработан достаточно гибким, чтобы охватывать все соответствующие варианты защиты контента и модели управления, а также кратким, чтобы сохранить четкие и относительно простые модели использования контента для потребителя.

IV.8 Метаданные информации о состоянии использования

Санкционированная область единиц контента закодирована в виде метаданных контента СРСМ, называемых информацией о состоянии использования (USI). Контент СРСМ управляется и защищается в соответствии с USI, применяемой для каждой единицы контента. Помимо соответствующей USI состояние передачи косвенно отслеживается системой СРСМ, объекты, обладающие правом законной авторизации контента в системе СРСМ, могут выполнять другие изменения состояния USI единицы контента после поступления его в систему СРСМ.

IV.9 Контент СРСМ

Термином "контент" в общем случае называют аудиовизуальное содержание плюс дополнительные данные, например субтитры, картинки, графику, анимацию, веб-страницы, текст, игры, программы (исходный и объектный коды), скрипты или любую другую информацию, которая будет доставлена и потреблена пользователем. Контент СРСМ – это контент, защищаемый и управляемый в соответствии с системой СРСМ. Единица контента является дискретным экземпляром конечной продолжительности. Каждая единица контента СРСМ сопровождается лицензией контента, заключающей в себе соответствующую USI с расширенными метаданными СРСМ. Система СРСМ может обрабатывать содержание лицензии контента и единицу контента по-разному в зависимости от целевой функции и/или правила использования, как того требует USI.

IV.10 Устройство СРСМ

Устройство СРСМ представляет собой устройство, которое осуществляет любые функциональные возможности СРСМ совместимым образом. Реализация функциональных возможностей СРСМ называется экземпляром СРСМ. Устройство СРСМ представляет собой устройство, на котором находится один или несколько экземпляров СРСМ. В дополнение к своим СРСМ функциональным возможностям оно также может содержать другие, не совместимые с СРСМ функции. Обработка СРСМ контента производится экземплярами СРСМ только внутри устройства. Не СРСМ компонент устройства не имеет доступа к контенту СРСМ. Устройство СРСМ может также выполнять не СРСМ функциональную возможность обеспечения безопасности для контента, поступающего из других систем защиты или для безопасного экспорта (или возможного потребления) контента СРСМ.

IV.11 Правило использования и информация о состоянии использования

Правило использования в СРСМ является конкретной операцией или характеристикой контента, которые должны контролироваться в рамках системы СРСМ. Полный набор утверждений правил использования для конкретной единицы контента называется санкционированным использованием этих единиц контента СРСМ. Санкционированное использование единиц контента выражается его кодированием в информации о состоянии использования (USI), метаданных контента СРСМ, сигнализирующих о санкционированном использовании данного конкретного контента.

Дополнение V

Схема безопасного транскодирования

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации)

V.1 Обзор схемы безопасного транскодирования

Транскодирование контента привлекало много внимания в связи с ростом популярности различных типов устройств, таких как КПК, не-PC устройств, сотовых телефонов, мобильных устройств и смарт-телефонов. Транскодирование относится к процессу преобразования мультимедийного контента, например картинок, текста, звука и видео из первоначального формата в другой формат или качество.

Транскодирование стремится уменьшить задержку загрузки мультимедийного контента по каналам доступа с низкой пропускной способностью, например каналам с модемом и каналам беспроводного доступа, и разрешить несоответствие формата кодирования устройства клиента и формата кодирования устройств поставщика мультимедиа контента. Оно также позволяет окончному устройству с ограниченными вычислительными возможностями отображать закодированный контент на основе возможностей транскодирования.

Существуют три объекта схемы безопасного транскодирования: отправитель, промежуточный сетевой узел и пользователь окончного устройства IPTV. Функция транскодирования находится на промежуточном сетевом узле, расположенном между поставщиком контента и окончным устройством. Существует два типа архитектуры транскодирования: традиционная архитектура транскодирования и безопасная архитектура транскодирования.

В традиционной архитектуре транскодирования в качестве промежуточного сетевого узла между сервером и окончным устройством используется модуль-посредник транскодирования. Отправитель шифрует контент с соответствующим коэффициентом компрессии и передает зашифрованный контент на промежуточный сетевой узел, называемый модулем-посредником транскодирования. Модуль-посредник транскодирования декодирует зашифрованный контент с декомпрессией. Затем он изменяет размеры контента или формат с новым сжатием и, в заключение, вновь шифрует транскодируемые данные для передачи на окончное устройство. Окончное устройство декодирует зашифрованный контент и декомпрессирует его с помощью нового алгоритма компрессии. Заметим, однако, что проблема безопасности возникает в модуле-посреднике транскодирования, то есть после того, как контент был расшифрован в модуле-посреднике транскодирования, и до того, как он будет зашифрован, в модуле-посреднике транскодирования находится незашифрованный контент. Иными словами, наблюдатель может получить доступ к незакодированному контенту посредством подслушивания. Такой незашифрованный контент ослабляет гарантии сквозной безопасности конфиденциальности, в которой только отправитель и легитимный клиент должны получить доступ к контенту в незашифрованном состоянии.

Для решения проблемы безопасности была предложена архитектура безопасного транскодирования. Схема безопасного транскодирования представляет собой своего рода схему безопасности, позволяющую промежуточным сетевым узлам выполнять транскодирование без расшифровки при сохранении сквозной безопасности. Эта схема может быть описана сочетанием масштабируемого кодирования, прогрессивного шифрования и пакетирования. Для передачи информации отправитель выполняет функцию безопасного транскодирования, создавая масштабируемые зашифрованные пакеты видео, и добавляет заголовок в незашифрованном виде; промежуточный сетевой узел читает незашифрованный заголовок и использует эту информацию для сокращения или удаления соответствующих пакетов в зависимости от желаемой операции транскодирования, терминал IPTV расшифровывает зашифрованные пакеты и декодирует обычный текстовый пакет для создания видео.

Библиография

- [b-ITU-T H.222.0] Recommendation ITU-T H.222.0 (2006) | ISO/IEC 13818-1:2007, *Information technology – Generic coding of moving pictures and associated audio information: Systems*.
- [b-ITU-T H.622.1] Recommendation ITU-T H.622.1 (2008), *Architecture and functional requirements for home networks supporting IPTV services*.
- [b-ITU-T M.1400] Рекомендация МСЭ-Т М.1400 (2006 г.), *Обозначения для соединений между сетями операторов*.
- [b-ITU-T Q.1290] Recommendation ITU-T Q.1290 (1998), *Glossary of terms used in the definition of intelligent networks*.
- [b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for open systems interconnection for CCITT applications*.
- [b-ITU-T X.805] Рекомендация МСЭ-Т X.805 (2003 г.), *Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами*.
- [b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.
- [b-ITU-T Y.1901] Рекомендация МСЭ-Т Y.1901 (2009 г.), *Требования для поддержки услуг IPTV*.
- [b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.
- [b-ETSI TS 102 825] ETSI TS 102 825 (all parts), *Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM)*.
<<http://pda.etsi.org/pda/AQuery.asp>>
- [b-ATIS 0800001] ATIS 0800001, *IPTV DRM Interoperability Requirements, ATIS-IIF*, April 2007.
<<https://www.atis.org/docstore/product.aspx?id=21212>>
- [b-ATIS 0800006] ATIS 0800006, *IIF Default Scrambling Algorithm (IDSA) IPTV Interoperability Specification*, February, 2007.
<<https://www.atis.org/docstore/product.aspx?id=22663>>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	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 протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи