Апухтин Р.В., Коржихин Е.О.

Магистрант кафедры
телевидения МТУСИ

СИСТЕМЫ УСЛОВНОГО ДОСТУПА И ЦИФРОВОГО УПРАВЛЕНИЯ ПРАВАМИ ДЛЯ IPTV

В статье рассматриваются особенности формирования систем условного доступа CAS при предоставлении услуг телевидения по IP протоколу и технологии и методы защиты правообладателей предоставляемого контента.

1 Назначение и функции систем условного доступа.

Необходимость использования системы условного доступа (Conditional Access System, CAS) при предоставлении услуг IP TV вызвана тем, что оператору связи, оказывающему эти услуги, необходимо контролировать предоставление платных услуг и предотвратить несанкционированное потребление этих услуг. Контроль предоставления платных услуг заключается в том, чтобы обеспечить предоставление пользователям только того контента, за который они обязуются внести или уже внесли соответствующую плату, а также обеспечить предоставление контента на бесплатной основе. Весь остальной контент должен быть недоступен для пользователей. Таким образом, система условного доступа даёт возможность оператору получать доход от предоставления платных услуг пользователям.

Система CAS должна обеспечивать:

- шифрование контента, включая шифрование информации, передаваемой в направлении от пользовательского оборудования к сети связи;
- поддержку форматов телевизионного сигнала MPEG-2 (ISO13818), MPEG-4 (H.264, ISO14496-10);
- поддержку видеоизображения в стандартном разрешении кадра (SD) и телевидения высокой четкости (HD);
- шифрование во время предоставления контента (session) и предоставление предварительно зашифрованного контента при оказании услуг VOD;
- работу на различных типах сетей доступа (IP/Ethernet/DSL, HFC/MMDS и др.);
- управление доступом пользователей к контенту;
- различные способы оплаты за услуги IP TV, в том числе оплату за просмотр (Pay Per View, предварительная плата (Prepaid service), абонентскую плату и т.п.;

– интеграцию в существующие у операторов связи системы биллинга.

Системы CAS представляет собой совокупность технических средств и программного обеспечения, необходимых для предоставления платных услуг IP TV пользователям.

Системы CAS предусматривают, что оплата просмотров телевизионных и видеопрограмм может осуществляться несколькими способами, включая:

– подписка (Subscription), когда взимается фиксированная плата за пользование услугами в течение заданного срока;
– плата перед просмотром (Pay Per View, PPV), которая обычно применяется для услуг мультимедиа по запросу;
– оплата по повремённому тарифу или за объем данных (Impulse PPV, IPPV) и другие.

Системы условного доступа имеют, так называемые, «базовые» функции, которые предлагают все основные производители. Расширение функциональности CAS осуществляется производителями путем добавления новых модулей. К таким «базовым» функциям можно отнести:

– аутентификация и авторизация пользователей;
– шифрование контента при IP-телевещании в реальном времени;
– шифрование контента, который хранится на серверах VoD для его последующего предоставления по запросу пользователя;
– подписка на пакет каналов (subscription);
– плата перед просмотром PPV (Pay-Per-View).

Также, обычно за отдельную плату, производители предлагают программные модули для обеспечения других функций. Это могут быть такие функции, как:

– Impulse PPV, когда плата взимается за просмотр программы по повременному тарифу или когда плата взимается за объем трафика;
– оценка рейтинга телепередач (Audience Measurement System – AMS);
– оплата с помощью кредитной карты;
– использование «билетов», которые применяются при реализации «Домашнего кинотеатра»;
– родительский контроль за доступом к телевизионным передачам;
– защита от воспроизведения видео, записанного на устройстве видеозаписи путем реализации функций цифрового управления правами (Digital Right Management, DRM) и др.

В системе для предоставления услуг IPTV система условного доступа имеет важное значение наряду с системой поддержки интерактивных приложений или промежуточным

программным обеспечением (Middleware). Обычно система CAS входит в состав оборудования для головной станции IPTV и взаимодействует с Middleware и существующей у оператора системой операционной поддержки и поддержки бизнеса (Operation Support System/Business Support System, OSS/BSS) (Рисунок 1.1).

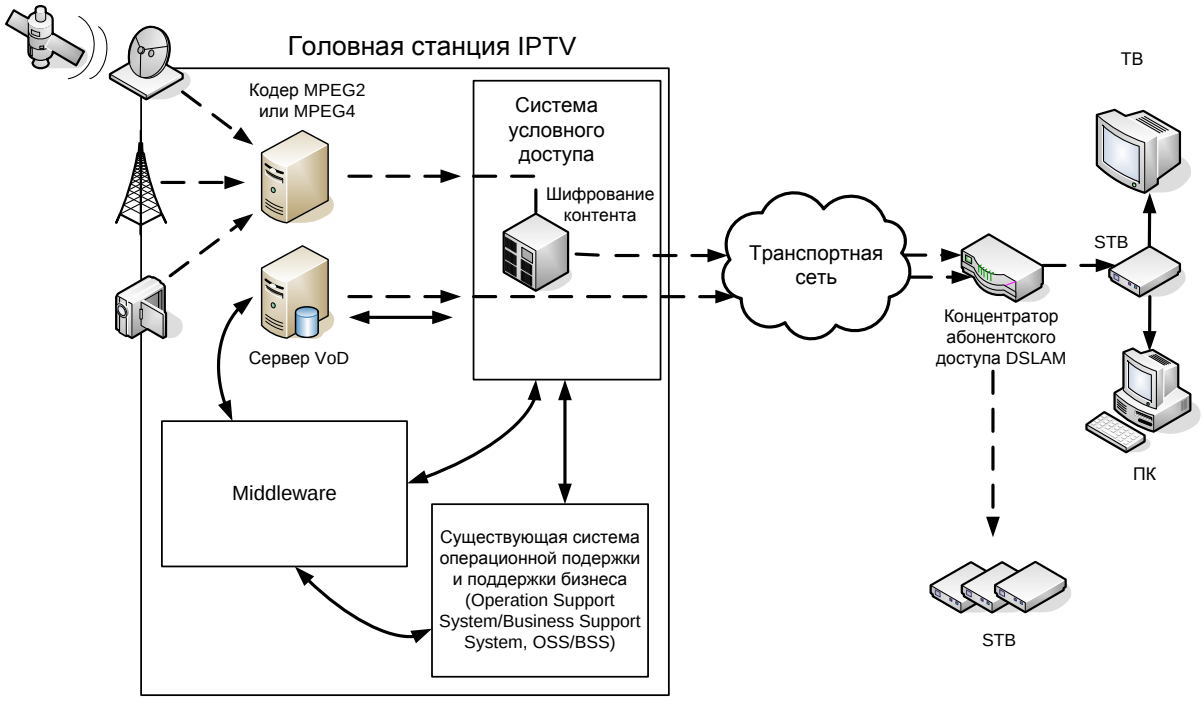

Рисунок 1.1 – Место системы условного доступа в системе IPTV

Требования к производительности системы условного доступа определяются с учетом:

- количества потенциальных пользователей услугами;
- количества зашифрованных каналов;
- количества пакетов программ, на которые могут подписаться пользователи и др.

2 Способы реализации систем условного доступа

Системы условного доступа обычно реализуются двумя различными способами: с использованием смарт-карт или без использования смарт-карт.

К особенностям первой реализации относятся:

- аппаратное шифрование контента;
- дешифрование контента в STB;
- использование смарт-карт для получения доступа пользователя к контенту.

Схема такой реализации показана на Рисунок 2.1. Шифрование контента в этой системе осуществляется специальным устройством в головной станции IPTV (IPTV headend).

Зашифрованный контент передаётся от головной станции до абонентского оборудования. по сети с коммутацией пакетов.

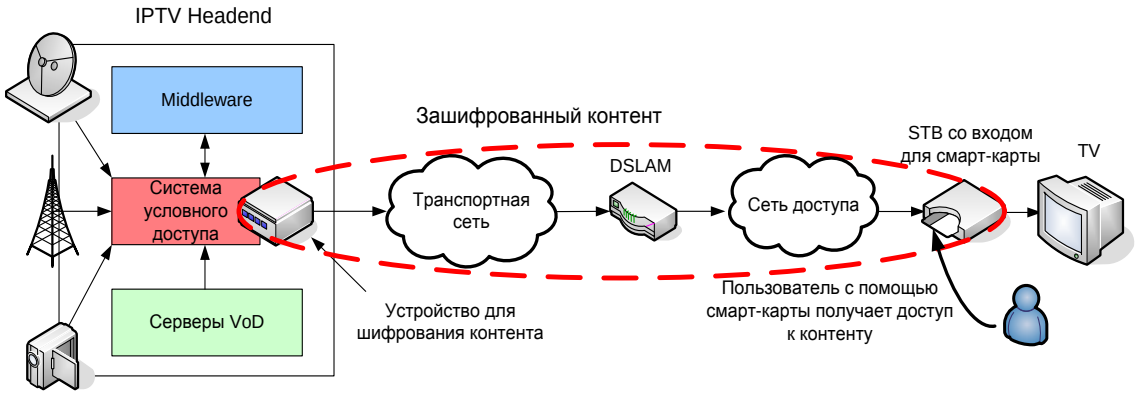

Рисунок 2.1 – Схема системы условного доступа с использованием смарт-карт

К особенностям системы условного доступа без использования смарт-карт можно отнести:

- шифрование контента в центре TVoIP осуществляется, как правило, с помощью программного обеспечения;
- дешифрование контента осуществляется в концентраторах абонентского доступа (DSLAM);
- доступ пользователя к контенту осуществляется без пользования смарт-карт путем ввода имени пользователя и его пароля.

Схема реализации условного доступа без использования смарт-карт показана на Рисунок 2.2. Дешифрование контента осуществляется в DSLAM, в котором реализована функция идентификации. Оборудование DSLAM разрешает доступ к контенту пользователям, имеющим право на пользование услугами, и предотвращает несанкционированный доступ. Обычно идентификация осуществляется по MAC-адресу оконечного оборудования (STB).

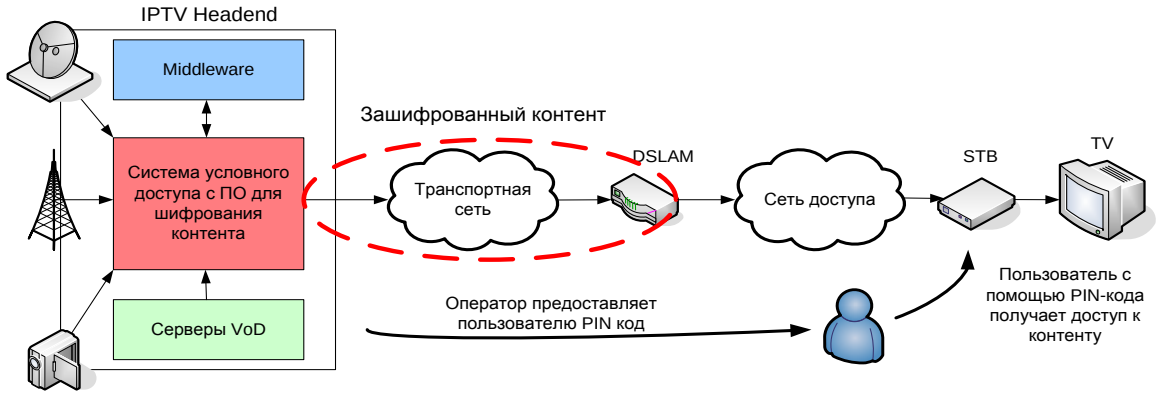

Рисунок 2.2 – Схема системы условного доступа без смарт-карты

Основными преимуществами системы CAS без использования смарт-карт являются:

- упрощается смена протокола шифрования. Это делается посредством автоматической загрузки нового ПО, в том числе в пользовательское оборудование. При этом устраняется необходимость в замене STB и кодирующего оборудования в головной станции. В то же время, если оператор, использующий систему CAS со смарт-картами, решит сменить протокол шифрования контента, то ему придется менять все STB пользователей и кодирующую аппаратуру в головной станции;
- снижается риск несанкционированного доступа, так как отсутствует необходимость в использовании смарт-карт, которые сравнительно легко подделать;
- снижается стоимость пользовательского оборудования (STB), поскольку дешифрация контента осуществляется в DSLAM.

Важно отметить, что если на рынке появляется критическое количество подделанных смарт-карт, то оператору, чтобы продолжать получать доход от оказания услуг IP TV, потребуется сменить протокол шифрования. Поскольку, как показывает практика, рано или поздно любая система шифрования взламывается злоумышленниками, то протокол шифрования оператору менять всё равно придётся. Таким образом, оператору, который использует систему условного доступа со смарт-картой, придётся периодически и заблаговременно менять метод шифрования, что потребует дополнительных затрат.

3 Системы DRM

Под цифровым управлением правами (Digital Right Management - DRM) понимаются технологии и методы, которые используются для защиты интересов правообладателя контента. Изначально системы DRM разрабатывались для защиты от копирования внешних носителей, таких как компакт-диски.

В общем случае система DRM не должна допускать несанкционированного воспроизведения и/или копирования контента и должна предоставлять пользователям возможность предварительного просмотра или воспроизведения контента для того, чтобы принять решение о приобретении этого контента. В то же время, система DRM должна предусматривать возможность санкционированного копирования контента с одного устройства на другое, например, с мобильного терминала на компакт-диск, и одновременно обеспечивать контроль за использованием контента. В частности, необходимо контролировать: количество копий контента; срок, в течение которого можно пользоваться контентом; количество просмотров или воспроизведений контента и т.п.

В системах DRM для выполнения этих задач применяются шифрование контента, ключи и лицензии, определяющие права на использование контента. Обычно авторизированные пользователи услугами должны приобрести лицензию на использование защищённого контента. Под контентом понимаются файлы, музыкальные записи, видеофильмы, записанные видеопрограммы и т.п.

При работе систем DRM предусматривается использование системы открытых ключей (PKI – Public Key Infrastructure).

Пользователи могут получать зашифрованный контент разными способами, например, путем загрузки с Web-сайта или корпоративного сервера, пересылки по электронной почте или копирования с компакт-диска. В любом случае для воспроизведения или просмотра скопированного или закаченного контента пользователю потребуется соответствующая лицензия. Таким образом, контент можно размещать в сети связи без риска, что доступ к ней получат посторонние лица.

В общем случае, для получения лицензии приложение или пользовательское оборудование для воспроизведения защищенной информации должно обратиться к соответствующему серверу по адресу, который указан в метаданных, размещенных на зашифрованном носителе или в файле. Обычно указывается адрес URL сервера, хранящего ключ для расшифровки. После расшифровки информации лицензия принимается. Лицензия может принадлежать устройству, приложению или пользователю.

Существует много компаний, которые занимаются разработкой систем DRM, часть из них разрабатывают системы для защиты контента для мобильных телефонов. В то же время, некоторые компании уже ведут разработку систем DRM для предоставления услуг IPTV. К таким компаниям относятся: Contenguard, Intertrust, Microsoft и другие.

Однако на настоящий момент времени все предлагаемые системы DRM являются фирменными и обычно несовместимы между собой. Поэтому контент, защищённый какой-либо системой DRM, как правило, не может быть воспроизведен приложениями или на

пользовательском оборудовании, поддерживающими другую систему DRM. Более того, иногда разные версии одного приложения также поддерживают различные системы DRM. Такая ситуация является очень неудобной для пользователей, которые работают с разными приложениями на разных терминалах. Например, пользователю неудобно, когда документ, с которым он работает на КПК (карманный ПК), нельзя просматривать и редактировать на ПК. Исходя из этого, стала очевидной необходимость обеспечить совместимость между системами DRM разных производителей.

Учитывая, взрывной рост абонентов сетей подвижной связи и то, что рост доходов операторы сетей подвижной связи связывают с услугами с контентным наполнением, впервые такая задача была поставлена организацией OMA (Open Mobile Alliance), в которую входят порядка 350 компаний. Среди них операторы связи, производители мобильных терминалов и разработчики программного обеспечения.

На сегодняшний день организация OMA выпустила две версии спецификаций: OMA DRM 1.0 в ноябре 2002 года и OMA DRM 2.0 в июле 2004 года.

Спецификация OMA DRM 1.0 разработана для защиты, так называемого, «легкого» контента (light-media content), который не требует высокой скорости передачи. «Легким» считается относительно недорогой контент, цена на который не превышает 1-2 доллара США. К такому контенту относятся рингтоны для мобильных телефонов, заставки, Java игры, видео и аудио клипы, скринсейверы (хранители экрана) и т.п.

Спецификация OMA DRM 1 предусматривает три способа загрузки контента в терминал:

- «сцепка» (forward-lock);
- совместная доставка (combined delivery);
- раздельная доставка (separate delivery).

«Сцепка» используется, чтобы предотвратить несанкционированную передачу контента с одного устройства на другое. Этот способ обычно применяется для предотвращения несанкционированного использования контента, доставляемого по подписке, например, новостей. Незашифрованный контент размещается в сообщении DRM. Получив на терминал сообщение DRM, пользователь на этом терминале может воспроизвести, просмотреть полученный контент, однако не может копировать этот контент на другие терминалы или устройства.

Совместная доставка позволяет не только предотвратить несанкционированную передачу контента пользователю, но и шифровать контент, а также контролировать использование контента. Сообщение DRM содержит контент и права на его использование. Права определяют правила использования контента, которые, в зависимости от используемой

бизнес-модели, могут ограничивать доступ к контенту по времени, по количеству воспроизведений и т.п.

При использовании механизма раздельной доставки контент и права на его использование передаются пользователю раздельно. При реализации этого механизма пользователь, не имеющей лицензии, может скопировать контент. Однако, если этот пользователь попытается воспроизвести скопированный контент, то система DRM автоматически обратится к серверу, где хранятся права на использование (лицензия), чтобы пользователь смог приобрести соответствующую лицензию с ключом для данного контента.

Спецификация OMA DRM 2.0 направлена на предоставление услуг мультимедиа, в том числе обеспечение телевизионного вещания на мобильные телефоны – Mobile TV. Эта спецификация, по сравнению с OMA DRM 1.0, предусматривает реализацию более широких возможностей, как для обладателя контента, так и для пользователя.

Обладатель контента получает следующие возможности:

- расширенная безопасность: привязка защищённого контента к конкретному пользователю, индивидуальные права на дешифровку контента с использованием открытого ключа (public key);
- проработанный механизм доверия: взаимная аутентификация между устройством, которое получило контент, и генератором прав на контент, который определяет права на использование контента для устройства, получившего контент;
- поддержка защищенного вещания в режимах multicast и unicast, при этом ведется совместная работа OMA с организациями 3GPP и 3GPP2 по форматам файлов для защищённого вещания и последовательной загрузки;
- экспорт контента в другие защищенные системы, например, перенос музыки в мобильный музыкальный проигрыватель;
- поддержка различных бизнес-моделей, включая: ограничение использования контента по времени, определение прав для пакета контента;
- поддержка передачи сообщений между равноправными устройствами (peer-to-peer) для распространения контента между устройствами одного производителя.

Пользователи получают следующие возможности:

- продвинутое управление контентом: контент и права на его использование можно переносить между различными устройствами одного пользователя;
- контент можно воспроизводить на множестве устройств, находящихся в одном домене, например, на устройствах, принадлежащих одной семье или другой группе пользователей, если это разрешено генератором прав;
- воспроизведение контента на устройствах, которые не подключены к сети связи;

- предварительный просмотр: можно предварительно просмотреть или воспроизвести фрагмент контента без оплаты;
- экспорт в другие системы DRM, включая передачу контента в абонентскую приставку STB или ПК.

Существует две модели предоставления прав на использование контента: пост-поставка (postdelivery) и пред-поставка (predelivery). Пост-поставка получила также название супердистрибуция (superdistribution). Эта модель позволяет пользователям получать контент от другого пользовательского оборудования. При этом пользователь перед принятием решения о получении контента может предварительно его просмотреть или воспроизвести. После поучения контента необходимо получить права на его использование у генератора прав.

В модели пред-поставки права на использование контента предоставляются незаметно для пользователя, т.е. без каких-либо дополнительных действий с его стороны, перед закачкой или непосредственно при закачке контента.

Представляется целесообразным использовать комбинацию описанных выше моделей, предоставляя пользователю вместе с защищенным контентом права на его использование, с ограничением срока или количества просмотров или воспроизведений контента. По истечении этого срока или количества просмотров (воспроизведений) контента пользователь может обратиться к генератору прав и приобрести постоянную лицензию без ограничения доступа к контенту.

Поскольку все предлагаемые на сегодняшний день DRM системы являются фирменными решениями, остро стоит вопрос об обеспечении их взаимодействия. Для его решения был создан форум производителей Coral Consortium, Участники форума должны протестировать взаимодействие систем DRM в рамках проекта NEMO (Networked Environment for Media Orchestration) для различных услуг и с использованием различных терминалов. Рассматриваются три возможных сценария обеспечения взаимодействия систем DRM разных разработчиков: online, offline и hybrid.

Сценарий «online» предусматривает разработку шлюза Right Mediator, обеспечивающего взаимодействие между различными системами DRM. В данном сценарии контент не передается непосредственно между оборудованием пользователя, в котором реализованы разные системы DRM. При попытке передачи контента от одного пользовательского устройства к другому происходит автоматическое обращение к шлюзу Right Manager для организации взаимодействия между различными системами DRM.

Сценарий «offline» предусматривает создание между пользовательским оборудованием, в котором реализованы разные системы DRM, защищенного канала (Secure Authenticated Channel - SAC), по которому осуществляется обмен контентом и правами на его использование.

При этом требуется интеграция в оконечное оборудование программного обеспечения «Coral credentials». В этом сценарии нет необходимости в установке шлюза Right Mediator.

Сценарий «hybrid» предусматривает, что шлюз Right Mediator обеспечивает взаимодействие между различными системами DRM, а передача контента осуществляется непосредственно между пользовательским оборудованием по каналу SAC. Этот сценарий представляется более предпочтительным, поскольку поддерживает различные бизнес-модели.

Список использованных статей.

1. *Решения для защиты контента. Журнал "Broadcasting. Телевидение и радиовещание" #4, 2009.*
2. *Косарев А. Бизнес в интерактивном телевидении (IPTV). Журнал "Broadcasting. Телевидение и радиовещание" #2, 2008.*
3. *В.Л. Карякин. Цифровое телевидение. - М.: «Солон-Пресс», 2008.-456 с.: ил.*
4. *М.Ф. Тюхтин. Системы Интернет-Телевидения. – М.: «Горячая линия-Телеком», 2008,-515 с.: ил.*