Денис Буличенко
DENIVIP Media

Онлайн-видеосервисы и технологии DRM

Последние несколько лет мультимедийные технологии развиваются в геометрической прогрессии. Еще двадцать лет назад вершиной было эфирное аналоговое вещание. Сейчас все большее влияние на телеиндустрию оказывают онлайн-видеосервисы.

Обзор технологий видеоплатформ

Основные тенденции развития онлайн-видеосервисов:

Многоэкранность — доступ с любых устройств и просмотр в любое удобное время.

Разнообразные бизнес-модели — множество вариантов доступа к видеоконтенту: онлайн-просмотр, аренда, скачивание, просмотр с рекламными прерываниями.

Технологическая сложность — разнообразие модулей видеоплатформ и особенностей их использования (загрузка, обработка и защита контента, доставка контента, балансировка видеонагрузки, воспроизведение видео и др.).

Предоставление абонентам доступа к премиум-контенту и, соответственно, необходимость использовать для него средства защиты — крупнейшие киностудии предъявляют высокие требования для обеспечения сохранности очень дорогого контента (многомиллионные бюджеты фильмов — уже стандартная ситуация).

Упрощенная схема современной видеоплатформы для вещания в интернете предполагает подготовку контента, его защиту и распространение для проигрывания на устройстве пользователя (рис. 1). Исходный контент, как правило, поступает в систему транскодирования, где из него генерируется набор видео для разных конечных устройств, для каждого устройства в разных качествах (для реализации динамического битрейта). Подготовленный контент отправляется в сеть доставки видео, которая может быть своей внутренней (in-house, с использованием собственной инфраструктуры оператора) или внешней (CDN-провайдер).

Существует несколько наиболее популярных вариантов доставки контента пользователю:

- Скачивание файла с видеоконтентом и дальнейший просмотр загруженного файла в специальном приложении (HTTP Download).
- Скачивание файла по кусочкам, склеивание кусочков в видеоплеере и просмотр загруженной части видео-контента в процессе загрузки (HTTP Streaming) .
- Онлайн-стриминг при помощи специализированных протоколов и воспроизведение видеопотока (RTSP, RTMP, MPEG2-TS).

Если контент требует качественной защиты, то перед передачей в сеть доставки выполняется его шифрация при помощи DRM-решения.

Видеоплеер при попытке воспроизведения поступившего контента может обнаружить зашифрованные данные и обратиться к серверу лицензий за разрешением доступа и ключом для дешифрации видео. На уровне видеоплеера (клиентское устройства) весьма популярна реализация видеоаналитики — сбор подробных данных по просмотру видеоконтента, отслеживание параметров качества и т.п.

Особенности защиты контента

Практически все DRM-решения построены по единой архитектуре и состоят из двух частей: серверной (бизнес логика) и клиентской (плеер). Серверная часть, в свою очередь, состоит из двух модулей: шифратора, который подготавливает (шифрует) контент, и сервера лицензий, который выдает пользователям лицензии на его воспроизведение[1].

С точки зрения сети доставки контента, никакой разницы между защищенным и открытым контентом нет. DRM-решения используют асимметричные алгоритмы шифрования, в этом случае контент шифруется основным мастер-ключом, а пользователям для дешифрации требуются свои уникальные ключи, которые генерируются для конкретной сессии просмотра. В случае LIVE-видеотрансляций для более надежной защиты контента, как правило, используются механизмы ротации ключей: ключ меняется в заданные интервалы времени. В случае VOD используются разный ключ для разных единиц контента и, если правообладатель это предусмотрел, механизм кеширования лицензий. То есть на определенное количество просмотров или определенный промежуток времени у пользователя на локальном устройстве хранится ключ, поэтому обращаться к серверу лицензий для каждого просмотра не требуется.

[1] Лицензия DRM содержит правила воспроизведения контента (политику защиты) и ключ для дешифрации. Как правило, взаимодействие клиентского приложения с сервером лицензий выполняется по зашифрованному каналу поверх HTTP.

Основные производители DRM-решений

На рынке существует множество систем защиты контента (DRM), обладающих своими сильными и слабыми сторонами. Ситуация усугубляется высокой степенью сегментации пользовательских устройств: Windows (в том числе и разные браузеры), MacOS, iOS, Android, телевизоры и приставки со своими операционными системами и технологиями. Большому числу игроков на рынке весьма трудно договориться о единых технологиях и стандартах, поэтому появляются группы технических решений, а об универсальной технологии можно забыть (по крайней мере, на некоторое время).

Наиболее популярными технологиями защиты контента для онлайн-видеосервисов являются:

- Adobe Flash Access — учитывая его популярность (основная часть видео в интернете реализована при помощи Adobe Flash), данное решение является идеальным для защиты контента в браузерах и на персональных компьютерах, Android-устройствах.
- Microsoft PlayReady — наследник Windows Media DRM, одного из первых решений по защите контента. Поэтому SDK Microsoft PlayReady попал на большинство устройств Connected TV (LG, Samsung и т.п.) и, само собой, в операционные системы Windows (приложение Media Player).
- Widevine DRM — относительно недавно ставшая частью Google, компания-разработчик решений по защите контента, популярная вследствие поддержки большого набора потребительских устройств (телевизоры, игровые приставки, iOS-устройства[2]).
- Marlin DRM — одно из немногих DRM-решений, поддерживаемых в телевизорах Philips, устройствах Sony PS3 и PSP. Примечательно базированием на открытых стандартах и доступностью по SaaS модели (оплата за транзакции по получению лицензий).

Отдельно стоит отметить так называемый Adobe Protected Streaming — RTMPE, защищенную доставку контента в режиме стриминга (RTMPEncrypted). Это альтернатива DRM, где защита реализована на уровне транспорта при передаче контента, а не на уровне самого контента, как в DRM.

В этом случае шифруется канал передачи мультимедийного контента от Flash Media Server'а до Flash Player'а. Не самое надежное решение, но, тем не менее, одобренное большинством крупнейших правообладателей. Технология RTMPE подразумевает использование дополнительных механизмов защиты контента на уровне приложений: токенизация ссылок на контент (предотвращение возможности обращения к контенту напрямую, минуя логику видеосервиса), авторизация пользователя. По сравнению с полноценными DRM стоит отметить существенно меньшую стоимость (в разы) и простоту запуска (минимальная сложность настройки). Кроме того, от пользователя не требуется никаких действий по установке DRM-компонент.

Однако по мере развития новых технологий распространения, в частности — HTTP-стриминга, от этого решения приходится отказываться в пользу более универсального DRM. Кроме того, существуют средства для взлома RTMPE.

Архитектура DRM-решений

Практически любое DRM-решение состоит из трех частей:

Сервис шифрации контента (сервер) — выполняет предварительную шифрацию контента для распространения по открытым каналам (интернет) исключительно

[2] Apple iOS предлагает лишь один механизм реализации DRM – это AES-128 шифрация видео, никаких встроенных средств управления ключами Apple не предлагает, их нужно реализовывать самостоятельно. Это и делают многие производители DRM-решений, совместимых с Apple iOS.

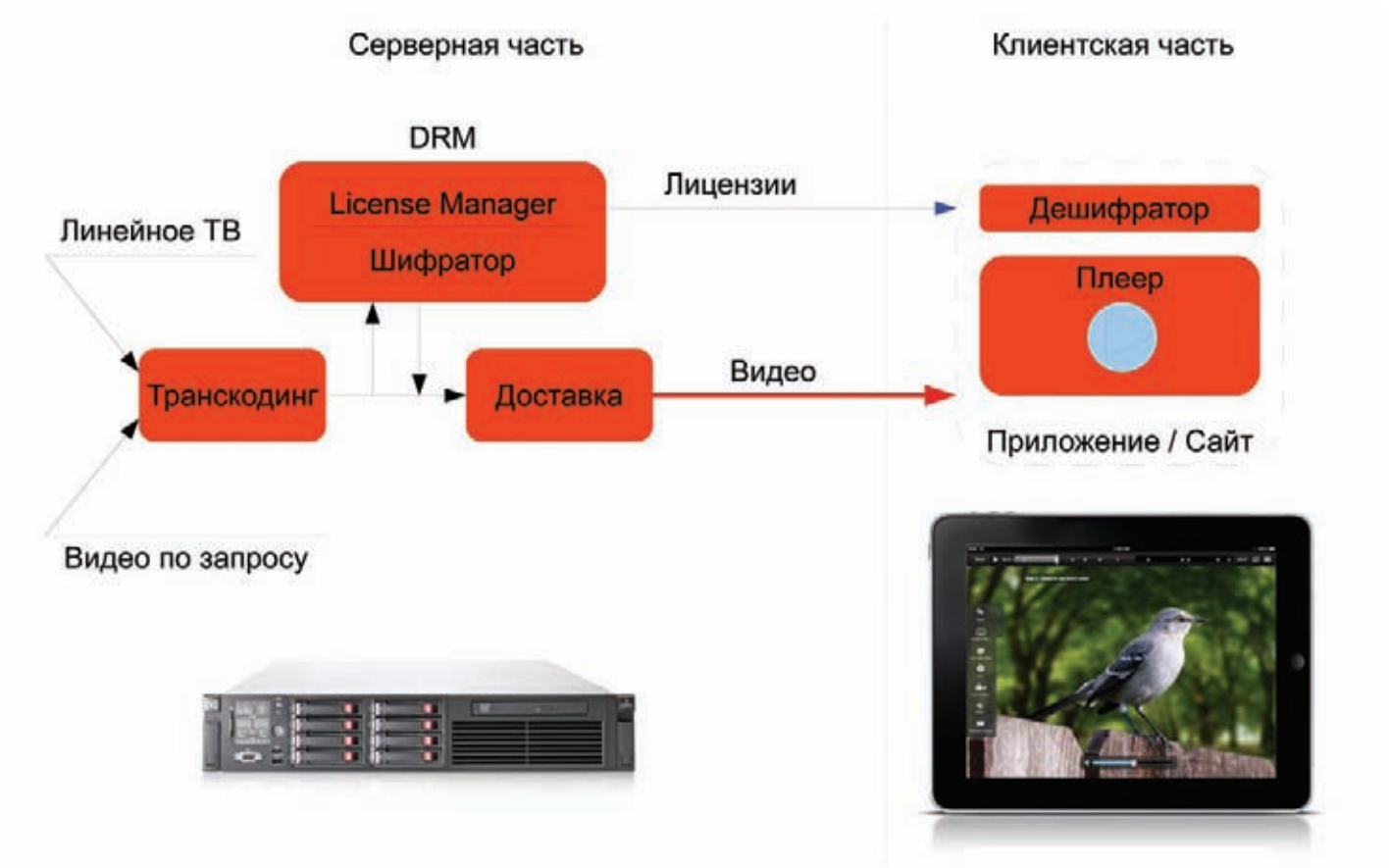


Рис. 1. Упрощенная схема онлайн-видеоплатформы

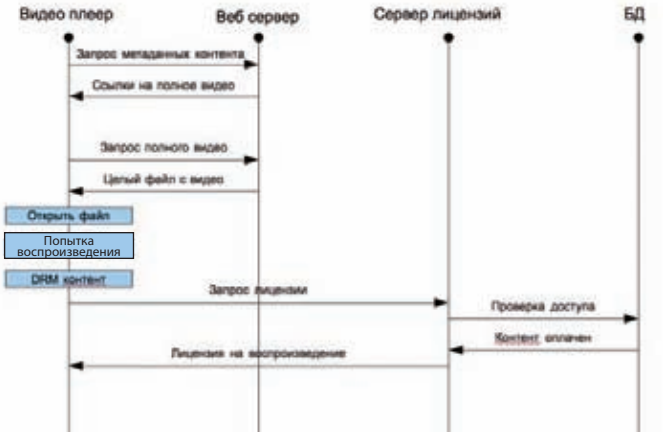
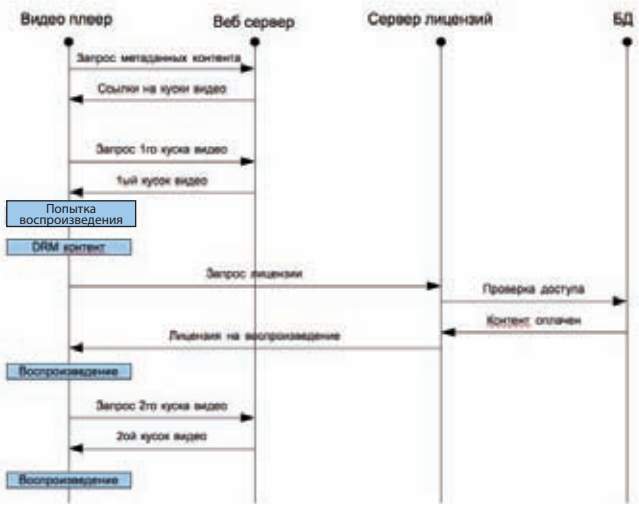


Рис. 2. Алгоритм работы DRM для загружаемого видео



Алгоритм работы DRM для потокового видео

Как видно на рисунках, с точки зрения DRM нет никакой разницы между потоковым вещанием и видео по запросу. Как правило, все сводится лишь к применению альтернативных алгоритмов проверки возможности доступа (оплачено ли скачивание или только просмотр онлайн).

в защищенном виде. В большинстве решений используется AES-128 алгоритм. Многие вендоры поддерживают использование HSM модулей для оптимизации процессов шифрации и разгрузки основного процессора[3]. Сервис выдачи лицензий (сервер) — принимает решение о выдаче (или невыдаче) ключа на дешифрацию видеоконтента в соответствии с бизнес-логикой (правилами распространения контента). Проверяются наличие активной оплаты или достаточность денежных средств у зрителя. В большинстве случаев это сервер приложений (например, на базе Java).

SDK (набор программных библиотек) для работы с защищенным контентом в видеоплеере интегрирует логику взаимодействия с сервисом выдачи лицензий в видеоплеер, а также осуществляет дешифрацию видеоконтента перед его воспроизведением. Также в SDK реализуются средства дополнительной защиты: контроль доступа к памяти видеоплеера, защита аналоговых и цифровых выходов, детектирование попыток взлома. SDK контролирует применение всех технических и логических ограничений, выставленных на сервере для контента и для конкретного пользователя, например, возможность записи на диск или мобильные устройства.

Таким образом, на вход системы защиты контента поступают контент и бизнес-правила ограничения доступа к нему, а на выходе получается воспроизведение видео на широком спектре пользовательских устройств.

Как уже отмечалось выше, в случае использования решений DRM доставка контента осуществляется независимо от его защиты и определяется, прежде всего, бизнес-моделью. Так, один и тот же защищенный контент в разных случаях может предоставляться как для скачивания (в том числе и через P2P-сети с целью минимизации затрат), так и для потокового вещания на сайте (стриминг и онлайн-просмотр). Однако при выборе DRM нужно все же уточнять, какие модели доставки и бизнес-модели ограничения доступа поддерживаются данным решением.

Выше приведены диаграммы взаимодействия модулей видеоплатформы при работе с защищенным контентом в режиме стриминга и при предварительной загрузке.

Выбор поставщика DRM

Одним из основных вопросов при выборе решения по защите контента является ассортимент потребительских устройств, поддерживаемых решением. Приоритет потребительских платформ у каждого онлайн-видеосервиса свой. Мы лишь рассмотрим основные особенности систем защиты контента для разных платформ:

- Интернет-браузеры в Windows / MacOS / Linux.
- Desktop-приложения.
- Интернет-браузеры в Android.
- Android-приложения.
- Интернет-браузеры в iOS.
- iOS-приложения.
- Connected TV.

Ключевые отличия различных решений по защите контента лежат как раз в качестве поддержки вышеуказанных технологических платформ. Так, Adobe Flash Access предоставляет удобные для пользователя средства защиты контента, не требующие установки дополнительных плагинов, так как Flash Player практически везде уже установлен (по данным Adobe, на 99% компьютеров и 80% мобильных устройств). Необходимость установки дополнительных плагинов отсекает тех потенциальных пользователей сервиса, у которых нет прав администратора или низок уровень компьютерной грамотности. Кроме того, на базе технологий Adobe работает огромное сообщество Flash-разработчиков, имеющих многолетний опыт создания кроссплатформенных приложений с насыщенным интерактивным интерфейсом (что немаловажно для онлайн-видеосервисов). Другие технологии отличаются меньшим уровнем распространенности плееров и бóльшим дефицитом технических специалистов. Но стоит отметить, что решения на базе Widevine предоставляют эффективный метод защиты контента для телевизоров Samsung, LG и iOS-устройств. Решения на базе Windows Media DRM исторически поддерживаются в еще большем числе Connected TV. А Verimatrix нет равных в поддержке среди производителей STB-оборудования.

[3] HSM, hardware security module, — устройство, которое может как хранить ключ, так и использоваться для дешифрации. Пример — смарт-карта спутникового ТВ.

Недавно Adobe потрясла всю отрасль заявлением о прекращении развития Flash-плагина в мобильных браузерах (по сути, в Android), объяснив это фокусированием на разработке мобильных приложений (AIR) и HTML5. Буквально на следующий день, чтобы пояснить свою позицию, Adobe сообщила, что ведет работы по созданию DRM для HTML5. Похоже, нас ждет что-то очень интересное.

Быстрому распространению нового формата передачи видео HTML5 мешают отсутствие единых стандартов использования видеокодеков (MP4, WebM, Ogg Theora) в разных браузерах и отсутствие единой надежной DRM-системы защиты контента, которая удовлетворила бы правообладателей. Разные видеоконтейнеры (mp4, wmv, ogg, mkv) поддерживаются разными решениями по защите контента. Сейчас большая часть видео в интернете использует mp4, поэтому все производители DRM заботятся о поддержке mp4. Но в случае с HTML5 mp4 поддерживается далеко не везде.

В случае Desktop-приложений все существенно проще — производители предлагают различные варианты SDK для интеграции в видеоприложения.

Защита контента на iOS-устройствах является отдельной большой темой вследствие того, что компания Apple пошла своим путем, отказалась от flash и выбрала HTML5 с H.264 видео (как наиболее популярный на сегодняшний день). Для разработчиков видеосервисов доступен лишь один метод защиты контента — потоковое блочное шифрование AES-128. Такая схема поддерживается, например, в последней версии Adobe Flash Media Server 4.5. Но реализацию механизмов управления лицензиями нужно делать самостоятельно либо использовать SDK от Widevine или других производителей. В случае воспроизведения в браузере управление лицензиями придется реализовать в JavaScript, что является существенной уязвимостью. В случае воспроизведения в приложении нужно использовать Objective C SDK, что дает существенно бóльший уровень защиты.

В мире музыки DRM-решения не прижились, особенно после отказа от DRM FairPlay в составе Apple iTunes. На наш взгляд, это связано с существенно меньшей себестоимостью аудиоконтента по сравнению с голливудскими блокбастерами. В результате позиция правообладателей в случае видеоконтента существенно жестче. Известные западные киностудии предъявляют длинные списки технических требований к компаниям, планирующим заниматься цифровым распространением контента. Примерами использования систем защиты контента могут служить практически все решения IPTV-операторов и крупнейших интернет-площадок рунета с премиум-контентом.

Все DRM-решения масштабируются и все потребляют примерно одинаковые ресурсы — алгоритмы шифрации везде единые. При выборе DRM-решения мы рекомендуем составить список целевых пользовательских устройств по приоритетам. Поддерживаемые устройства (а также контейнеры и кодеки), цена, удобство для пользователя, поддерживаемые бизнес-модели и технологии доставки контента — вот основные критерии выбора.

Компания «СмартЛабс» первой в России получила статус CWIP-партнера Widevine. Компания Widevine, недавно ставшая одним из подразделений Google, является ведущим мировым разработчиком решений для защиты цифрового контента. На наши вопросы о решении Widevine ответил Вадим Макматов, менеджер по работе с ключевыми клиентами компании «СмартЛабс».

Вадим Макматов: Технологии Widevine обеспечивают комплексную защиту авторских прав и оптимизацию работы с цифровым видео, включая доставку зашифрованного контента по технологии Adaptive Streaming. Клиентами Widevine являются такие крупные компании, как VUDU, Blockbuster, Cinema Now, Dish Online. Именно поэтому программное обеспечение Widevine установлено уже более чем на 300 млн устройств. Это телевизоры, мультимедийные плееры, планшетные компьютеры, смартфоны, приставки, игровые консоли.

Расскажите, пожалуйста, о конкурентных преимуществах данного решения защиты контента – в каких случаях его оптимально применять?

В.М.: Сейчас, будучи уже подразделением Google, Widevine не рассматривает других участников рынка как прямых конкурентов. Теперь она позиционирует себя в первую очередь как поставщика технологий, необходимых для увеличения востребованности видеоконтента в интернете. Именно поэтому компания Google приняла решение сделать DRM-систему Widevine бесплатной. Безусловно, это очень выгодное преимущество, поскольку ранее покупка DRM такого уровня требовала значительных вложений.

Чем Вы объясняете относительно низкую известность Widevine на рынке СНГ, какие видите перспективы в данном ключе?

В.М.: Решения Widevine в первую очередь предназначаются для защиты контента в сетях OTT. Первые успешные OTT-проекты были запущены в США, именно на этом рынке компании Widevine удалось заручиться поддержкой компаний-мейджоров и производителей электроники.

На рынке платного ТВ России и СНГ наиболее популярными продолжают оставаться спутниковое и кабельное телевидение, в меньшей степени — IPTV. OTT-проекты только начинают набирать популярность, при этом, в о основном OTT-сервисы ориентированы на пользователей персональных компьютеров и ноутбуков.

Рост популярности в России устройств на базе iOS и Android, ConnectedTV, игровых консолей предоставляет операторам OTT-сервисов новые способы дистрибуции контента. Именно для таких мультиплатформенных систем подходит единое DRM-решение компании Widevine. Поддержка всех популярных устройств, одобрение мировых мейджоров, поддержка AdaptiveStreaming и отсутствие лицензионных отчислений — все эти преимущества Widevine DRM позволят российским операторам OTT-сервисов увеличить свой доход.

При этом существующие OTT-решения для владельцев персональных компьютеров также могут использовать преимущества DRM Widevine, так как эта система полностью поддерживает популярный Adobe FlashPlayer.