Системы доступа на рынке ТВ-услуг

При подготовке этого номера мы задали ряд вопросов разработчикам наиболее известных и востребованных систем условного доступа, чтобы выяснить их взгляды на развитие телевизионного рынка, представление о своем месте на этом рынке, а также направления их эволюции и приоритеты при разработке продукции.

На наше предложение поделиться своими мыслями, планами, а также рассказать о последних разработках откликнулись представители семи компаний:

- Давид Мординсон, технический консультант компании NDS;
- Вернер Страйдом, вице-президент по технологиям компании Irdeto;
- Александр Гитин, директор по продажам Verimatrix в России и СНГ;
- Том Йар , EVP Products & Partners, Conax;
- Джим Уэлч, отдел международного маркетинга и коммуникаций SecureMedia® A Motorola;
- Дмитрий Броннер, директор по продажам Nagravision в России;
- Станислав Кирющенко, директор по развитию ООО «Цифра» (DRECrypt).

Их видение потребностей рынка во многом пересекается, а отличия чаще всего связаны с разницей сегментов, в которых они работают.

Новшества, внедряемые компаниями в отношении защиты контента, наиболее перспективные направления развития бизнеса компании

Передача на много экранов, распространение видео через интернет

На первом месте оказались решения для раздачи видеоуслуг на разные устройства и связанные с ними решения для OTT-передачи — то есть использования интернета как среды доставки. Эти направления воспринимаются как самые востребованные с точки зрения заказчиков-операторов.

NDS: «Операторы ищут пути для расширения зрительской аудитории. В связи с широким распространением портативных устройств и значительным улучшением их функциональных возможностей пользователи данных устройств также становятся целевой аудиторией для операторов, а сами устройства — полноценной заменой традиционным STB. Речь идет и о предоставлении традиционного вещательного контента, а также видео по запросу и других услуг на так называемые «множественные экраны», включая STB и телевизор, смартфоны, ПК и ноутбуки, планшетные компьютеры и т.д».

Давид Мординсон, технический консультант компании NDS

В качестве примера данных услуг можно привести новый сервис SkyGo, реализованный недавно британской компанией Sky (BSkyB) на базе комплекса решений NDS VideoGuard Connect™. На этой же платформе подобный сервис реализует и крупнейший спутниковый оператор США DirecTV.

Кроме того, сегодня все большую популярность получает вещание через интернет: все больше операторов используют данную платформу для предоставления контента. NDS и ее дочерняя компания CastUp разработали и уже развернули для нескольких заказчиков комплексное решение для вещания по сети, включающее создание частной сети доставки контента (Private CDN)».

IRDETO: «Помимо безопасности мы активно разрабатываем комплексные решения для видео на много экранов, так как видим растущий интерес операторов к этой области. Данное направление было ключевым на нашей экспозиции на IBC 2011, где мы представили сервисную платформу на базе облачной архитектуры, предназначенную для передачи услуг на планшетники, смартфоны и прочие iOS и Android-устройства».

Verimatrix: «Основное требование практически всех операторов, с которыми мы сотрудничаем в настоящее время — возможность применения системы в сетях разного типа. Дополнительно они хотят интегрировать в свою сеть различные абонентские устройства с предустановленными сторонними системами DRM.

VCAS-3 обеспечивает обе эти возможности. Verimatrix развивает возможности своего мультисетевого и мультиDRM-решения с поддержкой любых типов абонентского оборудования. Причем клиентские устройства могут интегрироваться с DRM от Verimatrix (ViewRight®) или сторонней DRM, такой как Microsoft PlayReady или Marlin DRM.

Будущее платного телевидения плотно связано с мультисетевыми услугами, и сейчас мы только в начале этого пути».

SecureMedia: «SecureMedia в основном профилируется на программных решениях, используемых в IP-сетях, и в настоящее время фокусируется на работе для сетей, реализующих принцип доступности видео где угодно и когда угодно. Наиболее перспективной для себя мы считаем разработку платформы Encryptonite ONE™, которая будет развиваться

поддержкой большего числа абонентских устройств, а также альтернативных платформ распространения видео. В частности, планируется поддержка стриминговой платформы Dynamic Adaptive Streaming over HTTP (DASH), разрабатываемой в настоящее время консорциумом DVB».

Conax: «В последнее время одним из наших приоритетных направлений является осуществление и обеспечение безопасности распределения при доставке видеосигнала на приставку (OTT) и применении нескольких устройств. В данном направлении мы работаем над несколькими инновационными решениями, которые, по нашему мнению, позволяют нашим клиентам воспользоваться возможностями, предоставляемыми этими и другими новыми разработками. Недавно мы запустили Contego™ Unite, обеспечивающий оператору управление различными распределительными сетями и целым рядом клиентских устройств».

DRECrypt: «Перспективным направлением видится развитие в области предоставления видеоуслуг через интернет. Технологии IPTV и OTT имеют высокий приоритет в портфеле разработок и продуктов нашей компании. Сюда же следует отнести решения для защиты контента, передаваемого между разными устройствами по домашним сетям».

Nagravision: «Следуя желаниям потребителей получать видео в любое время, в любом месте и через разные сети доставки, NAGRA разработала Media Player — интегрированное решение, обеспечивающее возможность безопасной передачи ТВ на ПК и другие открытые устройства».

Следует отметить, что решения NAGRA — для универсальной среды. Передачи плеером отнюдь не ограничиваются, у них уже давно готова комплексная платформа с облачной архитектурой для предоставления видеоуслуг по любым, в том числе интернет-каналам.

Компания говорит о готовности интегрировать свои компоненты с любыми решениями: «Наши интегрированные решения всегда могут быть изменены для включения наших компонентов в состав других экосистем».

Она также предлагает свои услуги в качестве консультанта и поставщика различных решений для безопасной передачи видео по интернету: «Наше «Киберпредложение» сочетает услуги консультирования и пакет решений, включающий программные компоненты безопасности, мониторинга услуг, технических контрмер и правовых методов борьбы с пиратством. Это предложение à la carte».

Домашние сети

Доставка защищенного контента на разные экраны подразумевает не только распространение видеоконтента на устройства через интернет-доступ, но и раздачу видеоконтента, получаемого по закрытым каналам вещательной сети на различные устройства бытовой электроники внутри дома с использованием домашней сети. При этом также стоит задача защиты этого контента от несанкционированных записи и воспроизведения.

NDS: «NDS совместно с ее дочерней компанией Jungo разработали новую концепцию для домашней сети — унифицированный домашний шлюз (Unified Home Gateway). Решение реализует в себе все функции телекоммуникационного портала и медиацентра, позволяя пользователю получить простой и эффективный доступ к контенту, услугам оператора связи и всем функциям медиацентра, используя внутри домашней сети более простые и дешевые устройства для просмотра контента. Для оператора связи данное устройство с расширенными функциями удаленной диагностики позволяет снизить операционные расходы и повысить качество обслуживания абонентов».

SecureMedia: «Encryptonite ONE™ HLS+ интегрирована с системой Mobility's Internet Protocol Rights Management-Home Network IPRM-HN от «Моторолы», позволяющей управлять безопасной передачей видеоконтента между устройствами домашней сети. Это решение «Моторолы» одобрено и DTLA (Digital Transmission Licensing Administrator), и CableLabs».

Внедрение дополнительных услуг в сетях DVB

Актуальность внедрения таких услуг была отмечена только DRECrypt: «Кроме новаций в отношении основного нашего продукта мы активно развиваем платформу дополнительных сервисов. После внедрения в своей сети цифрового телевидения перед оператором неизбежно встанет задача как дальнейшего развития, так и повышения лояльности абонентов. Этого можно достичь, внедряя популярные и удобные для услуги. Тенденции развития отрасли платного ТВ немногим отличаются от сетей подвижной связи. В настоящее время доходы от VAS (Value Available Services) сопоставимы с доходами от основной услуги — передачи голоса (в нашем случае — передачи ТВ-каналов)».

NDS упомянул о желании оператора иметь единую систему и для традиционных вещательных, и для «альтернативных» сетей: «У оператора должна быть возможность брендинга своих услуг и контента, а также инструменты для разработки и реализации смежных бизнес-моделей, которые работали бы как при традиционной, так и в более продвинутых схемах предоставления услуг. В качестве примера подобных решений можно назвать NDS Unified Headend™, NDS MediaHighway™, NDS VideoGuard Connect™, NDS Service Delivery Platform (SDP) и другие решения компании».

Системы водяных знаков

Несколько лет назад решения для наложения водяных знаков считали своим долгом предлагать практически все компании, имеющие отношения к разработке систем доступа или системной интеграции. Ожидалось, что с появлением ТВЧ наложение водяных знаков станет частым требованием студий, предоставляющих ТВ-операторам свой ценный контент. Первое поколение таких систем предполагало наложение водяных знаков в абонентском устройстве. Это наиболее очевидный подход, так как задача водяных знаков — нести код приставки, с которой сделана пиратская копия. Но это требовало апгрейда приставок, причем часто аппаратного. Возможно, это одна из причин, почему водяные знаки так и не получили распространения. Однако уже второй год, как появились два серверных решения для их наложения.

Вернер Страйдом, вице-президент по технологиям компании Irdeto

Александр Гитин, директор по продажам Verimatrix в России и СНГ;

[1] Принцип работы этой системы описан в статье «IBC 2010. Системы условного доступа и гибридное телевидение» (Т/С № 11, 2011).

Verimatrix: «Существенная область разработок Verimatrix, которой компания занимается уже более десяти лет — технология наложения водяных знаков. Вначале появилась система VideoMark™, обеспечивающая наложение водяных знаков на выходе STB или ПК. А затем была представлена система StreamMark™, позволяющая накладывать водяные знаки непосредственно на потоки, направляемые с сервера. Эта система, в частности, допускает маркировку видео, распространяемого по каналам OTT и принимаемого пользовательскими устройствами без поддержки функции водяных знаков».

Irdeto: «Одной из наиболее перспективных разработок является система водяных знаков TraceMark™. Их наложение, позволяющее отследить маршруты пиратских копий, становится все более частым требованием со стороны голливудских студий при предоставлении недавно вышедших материалов. Это серверная система, позволяющая маркировать не только видео по запросу (индивидуальные трансляции), но и вещательные потоки[1]».

Новинки в области защиты контента для традиционных DVB-сетей

Для Verimatrix, традиционно профилирующейся на решения для двунаправленных сетей, новинкой стала классическая система доступа, приобретенная путем покупки компании-разработчика. До недавнего времени две компании объединяли партнерские отношения.

Verimatrix: «Весной этого года Verimatrix приобрел компанию DVB CA firm Convenient GmbH. Это позволило дополнить решение Verimatrix Video Content Authority System (VCAS™) поддержкой однонаправленных сетей. Причем эта DVB-совместимая система используется не параллельно с VCAS, а интегрирована с остальными функциональным компонентами этого решения, такими как система администрирования абонентской базы и middleware. В результате Verimatrix получила комплексное решение для всех типов сетей распространения видео: DVB (C,S,T), гибридных DVB/IPTV и OTT».

А традиционные производители классических систем продолжают их эволюцию.

DRECrypt сформулировал требования к современной системе следующим образом: «Предлагаемые на данный момент на рынке решения для защиты контента в сетях DVB должны обладать, во-первых, оперативной поддержкой изменяющихся бизнес-моделей оператора, во-вторых, адаптироваться к новым появляющимся видам угроз практически мгновенно и, в-третьих, быть гибко интегрированными с сопутствующими системами других производителей».

К этому определению хочется добавить требования более простого и наглядного управления и мониторинга и возможности обслуживать одновременно разные среды вещания. Эти требования нашли отражения в новом решении Conax:

«Contego — новая и усовершенствованная версия Conax CAS. Эта полностью модернизированная

система позволяет оператору легко осуществлять управление все более сложными распределительными системами. Много усилий было вложено в графический пользовательский интерфейс GUI, обеспечивающий комплексную поддержку мониторинга и регистрации. Интерфейс имеет модульную основу и может поддерживать как небольшие операции с одним только абонентским доступом через абонентскую приставку, так и большие с гибридными распределительными сетями, использованием нескольких устройств и широким диапазоном бизнес-моделей. Все внешние интерфейсы разработаны для обеспечения простоты интегрирования в изделия третьей стороны-партнера».

Обобщая полученную информацию, можно выделить два направления развития традиционных систем — борьба с картшарингом и бескарточные системы.

Кардшаринг

DRECrypt: «Особое внимание по-прежнему уделяется защите вещаемого контента от «шаринга» и от незаконного копирования и распространения, для чего мы предлагаем интегральные решения и самостоятельно разработанные технологии».

Решения для противодействия кардшарингу есть у всех крупных разработчиков CAS, но подробно на этом вопросе остановился только **NDS**: «Основные изменения в подходе к защите контента обусловлены новой тенденцией пиратства, начавшейся в первой половине 2000-х годов. Поскольку анализ и взлом смарт-карт становится для пиратов все более трудной задачей, в последнее время основным направлением телевизионного пиратства стал так называемый кардшаринг (от англ. card-sharing), который использует тот факт, что канал передачи контрольного слова (ключа к открытию скремблированного контента) от смарт-карты на STB оставался недостаточно защищенным. В течение последнего десятилетия компания NDS в сотрудничестве с ведущими производителями видеопроцессоров (чипов для абонентских приставок) разрабатывала аппаратные средства защиты, встроенные в видеопроцессор, использование которых делает кардшаринг практически неосуществимым. Данная технология получила сегодня широкое распространение, она так же известна, как, например, Secure Video Processor или Control Word Encryption. На сегодня применение STB на базе данных видеопроцессоров со встроенными функциями защиты является обязательным условием на всех платформах, использующих NDS VideoGuard. Как результат — кардшаринг отсутствует на всех новых платформах с NDS VideoGuard, где используются STB на базе данных видеопроцессоров. Ожидается, что и на платформах со «старыми» STB проблема кардшаринга продержится еще пять-семь лет, поскольку ресурс подобных STB составляет, в среднем, до десяти лет, и в связи с амортизацией и заменой STB предыдущих поколений уже идет процесс модернизации парка STB».

Том Йар , EVP Products & Partners, Conax

Бескарточные системы для однонаправленных сетей

NAGRA: «Традиционно NAGRA предлагает два решения — систему со смарт-картами для однонаправленных сетей Media Access CLK, а также встроенное решение для двунаправленных сетей. Новое решение NAGRA Media Access DLK, является бескарточным и ориентировано на однонаправленные сети, привлекательность которых для пиратства не очень высока. Обеспечивает разумный уровень безопасности, исключая затраты на покупку карт и расходы на логистику».

NDS: «Компания NDS разработала и развертывает систему для защиты контента в односторонних сетях без применения смарт-карты, которая является расширением обычной «карточной» системы. Это межплатформенное решение для эффективного перехода на закрытое цифровое эфирное вещание, позволяющее оператору контролировать рынок абонентских устройств и оградить своих абонентов от демпинговых низкокачественных приставок. К тому же оно является весьма бюджетным, так как доступ к социальному пакету телеканалов предоставляется без использования смарт-карты».

Irdeto: «В качестве важнейшей новинки можно выделить появление у Irdeto бескарточного решения Cloaked CA. Оно направлено на снижение расходов владением системой при сохранении прежнего уровня надежности. Эта надежность Cloaked CA признана основными голливудскими студиями. Решение интегрировано в модули CI Plus, используемые с приставками общего назначения, и в такой форме уже внедряется в операторских сетях».

Джим Уэлч, отдел международного маркетинга и коммуникаций SecureMedia® A Motorola

Последняя фраза цитаты указывает на еще один тренд — возрастающую важность модулей доступа. В условиях роста количества телевизоров со встроенными тюнерами модули CI, вернее — CI+, с их расширенной функциональностью, возможно, возьмут на себя все функции приставки, кроме РЧ-приема.

Conax: «Значительный рост продаж цифрового телевидения с интеграцией служб (IDTV) определяет спрос на модули условного доступа (CAM) с высокой безопасностью. Conax обеспечивает значительную поддержку таких модулей. При этом в настоящее время основное внимание уделяется поддержке CI+ v1.3. Этот продукт обеспечивает высокую степень безопасности вещательного режима без необходимости использования абонентских приставок».

On-Chip Security

При разработке бескарточных систем, равно как и для защиты от шаринга, важную роль играет аппаратная реализации защиты данных в чипсете приставки. Подобные решения компании NDS упомянуты выше. Они являются актуальным направлением разработок и для других поставщиков CAS и DRM.

SecureMedia: «Хотя работа SecureMedia напрямую не связана с однонаправленными вещательными сетями, тем не менее, мы тоже работаем с производителями защищенных чипсетов, поставляя им защитные алгоритмы, которые аппаратно реализуются в их чипсетах. Аналогичные решения с использованием наработок «Моторолы» делаются и для систем WiMAX».

Verimatrix: «Компания разработала свое лицензированное решение для аппаратной защиты CryptoFirewall. Оно представляет собой ядро, реализованное на основе ASIC, позволяющее защитить в чипсете криптографические ключи и алгоритмы, даже если остальные компоненты безопасности взломаны. CryptoFirewall интегрирован в ряд SOC-видеодекодеров, предоставляя, в частности, механизмы защиты от шаринга одной из основных проблем операторов крупных DVB-сетей».

NAGRA: «В 2003 году мы запустили наш Set Top Box Security Certification (NASC). NASC. Этот документ содержит спецификацию внедрения механизмов безопасности и описание процесса сертификации приемных устройств. Одной из составляющих NASC является описание механизмов безопасности, которые должны быть реализованы в чипсете NAGRA On-Chip Security (NOCS); на сегодняшней день NOCS внедрен в 80 миллионов чипсетов».

Недавно NAGRA выпустила очередную версию спецификации NASC 3.0, включающую новый вариант NOSC. Он ориентирован на работу в условиях конвергенции телевизионных и интернет-сетей, усиливающих риски атак через разные среды и в отношении разных абонентских устройств. NOSC 3.0 предусматривает усиленные меры безопасности, в частности, возможность применения закрытого нестандартизированного алгоритма скремблирования как самого надежного средства борьбы с кардшарингом».

Сфера применения чисто програмных решений

Самым решительным сторонником программных решений, как и следовало ожидать, оказалась компания SecureMedia: «В своих программных разработках мы следуем принципам:

Данные о правах доступа хранятся исключительно на сервере, а не в устройстве клиента. Это повышает надежность решения, снижает загрузку клиентского устройства, а также позволяет поддерживать широкую линейку клиентских устройств.

Управление ключами шифровки и их доставка отделены от управления правами доступа. Это позволяет создавать гибкие распределенные структуры продажи медиапродукции. В системах с обратным каналом обязательными являются идентификация и авторизация клиентских устройств механизмами защиты от клонирования и вмешательство в клиентское ПО. При выполнении этих трех условий мы не видим никаких ограничений для применения чисто программных решений».

Verimatrix высказался неоднозначно: «Рассматривая этот вопрос, на наш взгляд, следует учитывать гибкие возможности интеграции программных решений в абонентские устройства, например, на базе iOS или Android, для которых аппаратные решения непригодны. С этой точки зрения уместнее рассматривать ограничения аппаратных решений, а не программных».

Но в то же время: «Наиболее грамотным и надежным подходом мы считаем совмещение программных методов защиты и аппаратной технологии System-on-a-Chip (SOC) и реализуем его в наших решениях для STB».

Дмитрий Броннер, директор по продажам Nagravision в России

Позиция традиционных разработчиков решений для DVB-сетей была схожей. По существу, они допускают возможность чисто программной защиты в интерактивных сетях но с некоторыми оговорками на уровень ценности передаваемых услуг.

DRECrypt: «Выбор того или иного технического решения всегда зависит от конкретного проекта и от требований безопасности к нему. В некоторых случаях применение исключительно программных средств вполне оправданно, но для крупных операторов или проектов делать ставку исключительно на программную защиту весьма опасно. На данный момент наблюдается некоторая тенденция в использовании технологий программной защиты, хорошо зарекомендовавших себя в интернете, но DVB имеет другую природу, и подтверждения стабильности таких систем в вещательном телевидении пока нет».

Conax: «Необходим баланс между стоимостью, угрозой, сроком вывода продукта на рынок и т.д. и уровнем безопасности. Ни одно решение не является оптимальным для любого устройства и любого контента при любой операции. Тем не менее, следует отметить, что обычно мы не верим в эффективность чисто программных решений в условиях чистого вещания».

NDS: «Любое ПО достаточно легко анализировать, даже если применяются специальные меры для защиты от анализа, так называемая обфускация (от англ. obfuscation). Хакеры не раз доказывали на практике свои возможности преодолеть различные меры защиты ПО и успешно взламывали различные механизмы обфускации. Шифрование и частые обновления ПО, использование различных версий, смена и «перепрятывание» ключей и т.д. способны лишь незначительно отложить неминуемый взлом. Бороться же со взломом по факту при наличии только программных средств практически невозможно. Сложность анализа аппаратных компонентов на несколько порядков выше и требует специального оборудования и навыков. Поэтому для односторонних вещательных сетей без устойчивого канала обратной связи требуется решение, основанное на аппаратных компонентах. Это же верно и для так называемых гибридных сетей, где единая система должна поддерживать абонентов односторонних и двусторонних сетей. Именно такие решения предлагает NDS: традиционный подход со смарт-картами и решение без смарт-карт, которое использует определенные аппаратные функции безопасности, заложенные в видеопроцессор абонентской приставки».

Станислав Кирющенко, директор по развитию ООО «Цифра» (DRECrypt)

Nagra: «При использовании чисто программного решения возможности защиты от несанкционированного вмешательства ограничены. В этом случае особенно важными оказываются мониторинг клиентского и серверного ПО, а также частота и оперативность проведения контрмер. В любом случае, уровень защиты должен быть таким, чтобы сделать пиратские атаки экономически невыгодными».

Irdeto: «Программная система безопасности требует выполнения двух условий. Во-первых, в ней должны быть предусмотрены механизмы защиты от модификации интегрированного в абонентский приемник ПО и возможности извлечения секретной информации. Для этого используются механизмы «белой криптографии», позволяющие шифровать и распределенным образом прятать ключи внутри ПО абонентского устройства. Во-вторых, программное решение должно предусматривать механизм его привязки к конкретному абонентскому устройству, исключающий возможность клонирования ПО». Однако далее: «Для гарантии надежной привязки клиентской части Cloaked CA к абонентскому приемнику Irdeto сформулировал набор требований к производителям чипсетов для STB, и каждый новый вариант чипсета проверяется на безопасность независимой лабораторией».

Разница между CAS и DRM

Мы попытались выяснить разницу между CAS и DRM как в плане технической реализации, так и в области применения. Полученные ответы скорее подтвердили отсутствие ясности в этом вопросе, вернее — невозможность на сегодняшний день корректно разделить эти понятия.

Irdeto: «Сформулировать различия между системой доступа и DRM с технологической точки зрения становится все сложнее, так как эти технологии все более переплетаются. Кроме того, разные люди подразумевают под этими понятиями разные вещи».

Conax: «Наш опыт говорит о том, что попытки определить различие между CAS и DRM только усложняют картину. У разных людей существуют различные ассоциации с этими терминами. Conax предпочитает не дифференцировать эти два понятия, а использовать их как единый термин. А еще лучше — говорить о конкретных функциях: защите контента, защите услуги, обслуживании прав, контроле за перераспределением, защите от копирования, поддержке обеспечения безопасности оборудования, восстановлении и т.д.»

Verimatrix: «С распространением цифровых видеомагнитофонов в сетях DVB появилась необходимость, наряду с CAS, добавлять управление доступом к видеоматериалам, записанным на диск. С другой стороны, DRM сейчас используются и для защиты «живых» видеопотоков, а не только файлов с контентом. Поэтому мы не думаем, что эти различия продолжают быть существенными, и в своем комплексном решении VCAS 3 предлагаем комбинацию обоих подходов. Тем не менее, различия в восприятии терминов по-прежнему есть, причем одинаковые у разработчиков как классических, так и программных решений».

SecureMedia: «Вероятно, различие проще всего определить следующим образом — CAS накладывается на транспортную структуру, используемую для передачи видео (MPEG-2TS прим. ред.), а DRM непосредственно на контент. Кроме того, в CAS используются смарт-карты или другие аппаратные системы защиты, в то время как решения DRM — чисто программные».

NDS: «CAS — это своего рода билетный контролер на входе в кинозал — он проверяет наличие билета и впускает (или не впускает) в зал. Функции DRM в данном примере менее очевидны; скажем, это кто-то, кто мешает (или обязан помешать) зрителю в кинотеатре снять фильм на портативную камеру, а потом делать пиратские копии, либо пре-

пятствует продаже данных копий. CAS регулирует доступ к услугам платного ТВ, в обязанности DRM входит регулирование доступа к записанному контенту, например, количество просмотров, и гарантия авторских прав при переносе контента на другие устройства: портативные компьютеры, мобильные телефоны и т.д. Обычно CAS включает в себя определенную функциональность DRM».

DRECrypt: «Часто данные решения предлагаются в комплексе, в котором CAS используется для защиты вещательного live-потока, а DRM — для шифрования файлов, которые хранятся либо на внутреннем, либо на внешнем носителях. При этом проигрывание файла возможно только на том устройстве, на котором он был записан. Классическая CAS подразумевает шифрование по CSA-алгоритму, что делает проигрывание записанного потока, шифрованного CAS, и переключение с записанного потока на вещаемый и обратно не всегда удобными для пользователя ввиду периодической смены ключей. Поэтому записываемый поток расшифровывается и зашифровывается еще раз по другому алгоритму, который не содержит данный недостаток».

Наиболее полно различия были перечислены **Irdeto**:

«С определенной степенью приближения можно выделить следующие:

- CAS в большинстве случаев работает на базе аппаратного модуля, такого как смарт-карта.
- DRM, как правило, реализована программно, используя программные средства сокрытия секретной информации, а также привязки к ПО к конкретному приемнику. Тем не менее, сейчас все чаще встречаются DRM'ы, реализованные непосредственно в защищенном чипсете (secure silicon).
- CAS обычно защищает однонаправленные вещательные каналы, но та же технология хорошо работает и в гибридных /двунаправленных сетях.
- DRM, как правило, используется в двунаправленных (IP) сетях.
- CAS для защиты одного видеоматериала обычно использует множество ключей. Двухчасовое видео, например, может быть разбито на фрагмент по 10 секунд, каждый из который шифруется с помощью своего ключа. Это дает вещателю возможность лишить абонента права просмотра практически в любой момент, например, если у него появится подозрения, что абонент ретранслирует получаемый им спортивный матч.
- DRM для защиты одного видео обычно использует один ключ. Если подписчик получил доступ к событию, прервать этот доступ практически невозможно.
- CAS, как правило, закрывает контент, распространяемый по сетям DVB.
- DRM обычно используется в отношении контента, распространяемого по IP-сетям».

Материал подготовила **Анна Бителева**