СОДЕРЖАНИЕ

Перечень условных обозначений, символов и терминов 7

Введение 8

1 Особенности передачи информации по оптическим волокнам 10

2 Методы несанкционированного вывода информации с боковой поверхности оптического волокна 43

3 Разработка устройства обнаружения несанкционированного съема данных при передаче информации по волоконно-оптического каналу связи 51

4 Охрана труда 54

5 Технико-экономическое обоснование разработки устройства xx

Заключение xx

Список использованных источников xx

**ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ, СИМВОЛОВ И ТЕРМИНОВ**

|  |  |
| --- | --- |
| СМИ | Средства массовой информации |
| DVB | Стандарт цифрового телевидения |
| IP | Протокол сетевого уровня стека TCP/IP |
| IPTV | Технология цифрового телевидения в сетях передачи данных по протоколу интернета |
| UDP | Протокол пользовательских датаграмм |
| TCP | Протокол обмена данными |
| HTTP | Протокол передачи гипертекста |
| Smart TV | Технология, позволяющая за счет подключения телевизора к интернету расширить его возможности |
| STB | Ресивер цифрового телевидения |
| SCP |  |
|  |  |
|  |  |
|  |  |

ВВЕДЕНИЕ

В современном мире значительную популярность приобретают информационные технологии, мобильная связь, телевидение. Появление интернет-технологий и информационного века сделало подачу новостей мгновенной и эффективной, а телевидение стало более функциональным и качественным. Не стоит забывать, что, как и все современные технологии интернет-телевидение должно обеспечивать информационную безопасность.

IPTV — это технология передачи телевизионного сигнала по каналам Интернет-связи, применяемая операторами цифрового телевидения и провайдерами Интернет-услуг для доставки телевизионных каналов посредством широкополосного доступа в Интернет. IPTV также называют IP Телевидение, Интерактивное Телевидение или Интернет Телевидение. Это отличный способ передавать телевизионные программы по каналам Интернета. На данный момент наиболее актуальны варианты доставки видео потоков по протоколам UDP или HTTP.

Основным преимуществом IPTV перед обычным цифровым телевидением является возможность просмотра множества ТВ каналов в высоком разрешении не только на компьютерах, но и на других бытовых устройствах с экраном: планшетах, смартфонах, телевизорах со Smart TV или STB-приставках. Отличительной особенностью IPTV являются дополнительные интерактивные возможности, такие как выбор языка озвучки трансляции, доступ к эфирной информации (телепередача, обзоры, отзывы), а также возможности платных сервисов с высоким качеством изображения по сравнению с другими вариантами доставки видео-контента или интеграцией дополнительных услуг.

Целью данной работы является исследование требований, механизмов и понятий информационной безопасности IPTV.

Задачи работы:

– изучение требований по информационной безопасности, предоставляемых к IPTV;

– изучение архитектуры и механизмов информационной безопасности IPTV;

– изучение основных понятий защиты информационной безопасности контента и абонентов IPTV;

– изучение управления информационной защитой и копированием контента DVB.

1 ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

IPTV

1.1 Общие требования безопасности

К общим требованиям безопасности, предъявляемым к IPTV, относится:

– при внедрении безопасности архитектура IPTV должна учитывать 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.

1.2 Требования безопасности контента

Требования, которые по отдельности или все вместе относятся к контенту или защите контента, предъявляемые к архитектуре:

– архитектура IPTV должна поддерживать 1) защиту контента, 2) обеспечение соответствия контента с защитой и метаданными управления контентом, 3) безопасную доставку защиты контента и метаданных управления контентом, включая метаданные прав использования, 4) метаданные прав использования контента, которые обеспечивают различие между правами использования, включая рендеринг(просмотр), хранение, перераспределение, а также их комбинации, 5) защиту контента распространяемого для очень большого числа абонентов одновременно (масштабируемость), 6) защиту потокового контента многоадресной и/или одноадресной передачи, 7) 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;

– запрещается, чтобы архитектура IPTV препятствовала обеспечению передачи информации отслеживания контента;

– 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;

– 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.

Требования к алгоритмам скремблирования, которые по отдельности или все вместе относятся к контенту или защите контента:

– алгоритмы скремблирования потоков вещательной передачи должны обеспечивать периодическое обновление необходимых криптографических ключей;

– алгоритмы скремблирования IPTV должны создаваться с использованием общедоступных и стандартизованных алгоритмов шифрования.

1.3 Требования безопасности услуг

Требования к архитектуре, которые по отдельности или все вместе касаются услуг и защиты услуг:

– архитектура IPTV должна обеспечивать возможность защиты услуг;

– запрещается, чтобы архитектура IPTV препятствовала обеспечению обновления SCP или возобновления действия SCP в оконечном устройстве, осуществляемого со стороны сервера;

– архитектура IPTV должна обеспечивать возможность санкционирования и аутентификации конечного пользователя (абонента);

– архитектура IPTV должна поддерживать механизм для передачи оконечному устройству указания использовать определенный алгоритм скремблирования, основанный на стандартной схеме;

– архитектура IPTV должна иметь возможность использовать стандартные системы управления ключом, как требуется для обеспечения совместимости;

– архитектура IPTV должна обеспечивать 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.

– архитектура IPTV должна поддерживать механизмы SCP, не зависящие от конкретных форматов контента;

– архитектура IPTV должна поддерживать механизм защиты целостности и аутентификации источника данных для важных метаданных;

– архитектура IPTV должна поддерживать механизм безопасности доставки прав и информации управления доступом оконечных устройств к контенту;

– архитектура IPTV должна обеспечивать контроль использования контента, например, воспроизведения;

– архитектура IPTV поддерживала различные режимы воспроизведения, например, ограничение на количество воспроизведений, ограничение по времени воспроизведения, ограничение ускоренной перемотки вперед или назад;

– архитектура IPTV должна поддерживать механизм сохранения конфиденциальности сообщений сигнализации между сервером SCP и клиентом SCP;

– архитектура IPTV должна поддерживать механизм сохранения достоверности и целостности сообщений сигнализации между сервером SCP и клиентом SCP;

– архитектура IPTV должна поддерживать механизм безопасного получения и обновления параметров SCP;

– запрещается, чтобы архитектура IPTV препятствовала обеспечению возможности включения и выключения функции отслеживания контента в программируемой форме;

– 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 эксплуатаци 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;

1.4 Требования к безопасности сети

Требования к архитектуре, которые по отдельности или все вместе касаются сетей и их защиты:

– архитектура IPTV должна поддерживать возможность смягчения DoS атаки;

– архитектура IPTV должна поддерживать меры безопасности по блокировке нелегального или нежелательного трафика;

– архитектура IPTV должна быть устойчива к атакам на функции многоадресной передачи;

– канал связи между оконечными устройствами в пределах домашней сети должен быть защищен для безопасности передачи оплаченного контента;

– архитектура IPTV должна поддерживать аутентификацию DNG при помощи функции управления IPTV;

– архитектура IPTV должна поддерживать аутентификацию функции управления IPTV при помощи DNG.

1.5 Требования к безопасности оконечного устройства

Требования к архитектуре, которые по отдельности или все вместе касаются оконечных устройств (TD) и их защиты:

– архитектура IPTV должна поддерживать защиту, аутентификацию и устойчивость TD к злонамеренным физическим манипуляциям;

– архитектура IPTV должна поддерживать 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;

– архитектура IPTV должна поддерживать 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;

– 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. Эти процессы включают дескремблирование и последовательное представление среды;

– архитектура IPTV должна определять необходимость физической защиты 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 обмену контентом между TD и другими физическими или логическими устройствами при условии, что использование такого контента предусматривает такой обмен;

– архитектура IPTV должна поддерживать механизм, позволяющий TD аутентифицировать серверы SCP;

– запрещается, чтобы архитектура IPTV препятствовала обеспечению возобновления действия SCP в TD;

– архитектура IPTV должна поддерживать цифровой или аналоговый выход, который должен быть защищен согласно требованию клиента SCP на внешнем устройстве хранения, в случае если ТD обладает цифровым или аналоговым видео/аудио выходом.

1.6 Требования к безопасности абонентов

Требования к архитектуре, которые по отдельности или все вместе касаются абонентов и конечных пользователей или их защиты:

– архитектура IPTV должна обеспечивать защиту неприкосновенности частной жизни пользователя;

– архитектура IPTV должна позволить абоненту устанавливать механизм управления доступом, например, с использованием пароля, для того чтобы ограничить доступ к контенту и/или услугам;

– архитектура IPTV должна быть способна указать причину отказа пользователю в доступе к контенту;

– архитектура IPTV должна поддерживать механизм, позволяющий абоненту запрашивать расширения прав пользования, связанных с определенными элементами контента.

2 АРХИТЕКТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

IPTV

Общая архитектура безопасности для IPTV изображена на рисунке 2.1 и делится на четыре области.

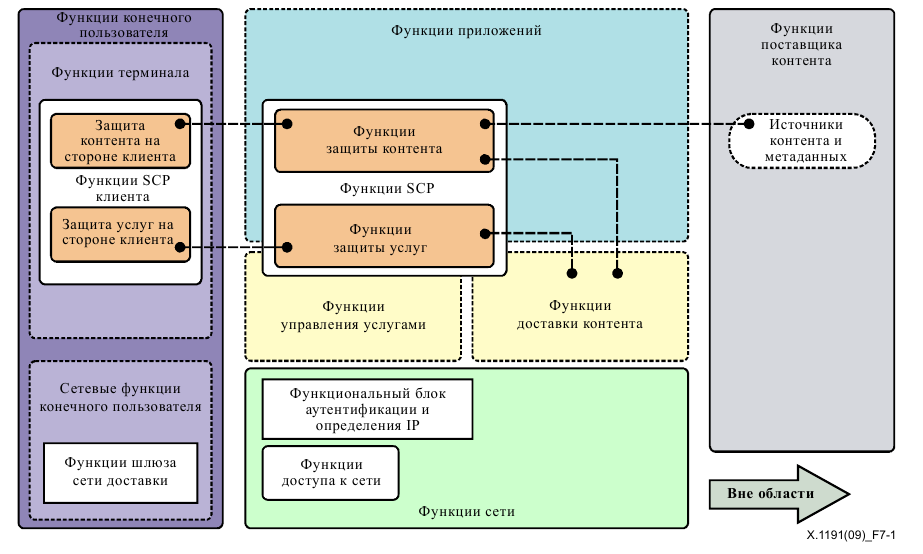


Рисунок 2.1 – Общая архитектура безопасности для IPTV

Функции поставщика контента. 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.

Функции защиты контента и услуг (SCP). 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. 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.

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.

Рассмотрим более подробное описание функций и функциональных блоков 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.

Функции приложений: разделены между стороной сервера (поставщик услуг) и стороной клиента (территория конечного пользователя); состоят из функциональных компонентов, которые подготавливают, 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).

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 IP-соединений, получают IP-адреса (адресов), а также IP-конфигурацию оконечного устройства.

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 шифрованных данных либо самостоятельно, либо в сочетании с функциями защиты контента.

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 обработки среды передачи, местного, защищенного 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.

3 МЕХАНИЗМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ IPTV

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, распределения или перераспределения конечным пользователем. К таким механизмам относится шифрование контента, отслеживание и идентификация контента, создание меток и маркировка контента.

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

Механизмы безопасности, обеспечивающие защиту сети. Как правило, механизмы обеспечения безопасности, задействованные поставщиками услуг IPTV и оконечными 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.

Механизмы безопасности оконечных 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.

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, оконечным устройством и поставщиком услуг, которые, возможно, собирают, сохраняют и повторно используют эту информацию.

4 ЗАЩИТА БЕЗОПАСНОСТИ КОНТЕНТА И АБОНЕНТОВ IPTV

Защита контента включает в себя 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.

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. По рекомендации МСЭ-T X.1191, услуга IPTV может дополнительно обрабатывать минимальный объем личных данных абонента, необходимый для предоставления услуг IPTV. Также до сбора информации, необходимой для доставки услуг IPTV разъяснить использование личных данных абонента и получить согласие от абонента, личные данные абонента, ставшие ненужными для продолжения предоставления услуг, следует удалить. Если личными данными абонента управляет поставщик услуг, то услуга IPTV может дополнительно хранить собранные данные в режиме строгой секретности.

Для предотвращения утечки абонентских данных, поставщику IPTV услуг рекомендуется уделять особое внимание следующему: разделить персональные данные абонента на те, которые требуют контроля и те данные, которые контроля не требуют; обеспечить безопасное администрирование персональными данными абонента, требующими контроля; обеспечить, чтобы личные данные абонента, требующие контроля, не использовались для иных целей, отличных от необходимых.

Поставщики услуг IPTV иногда хранят личные данные абонента в оконечном устройстве в целях повышения эффективности обслуживания. В таком случае, требуется: обеспечить, чтобы никакая третья сторона не могла легко прочитать личные данные абонента, хранящиеся внутри TD; и обеспечить, чтобы личные данные абонента, хранящиеся в TD, могли быть полностью удалены абонентом или поставщиком услуг.

5 УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ ЗАЩИТОЙ И

КОПИРОВАНЕМ КОНТЕНТА DVB

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.

Если говорить об архитектуре, то 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.

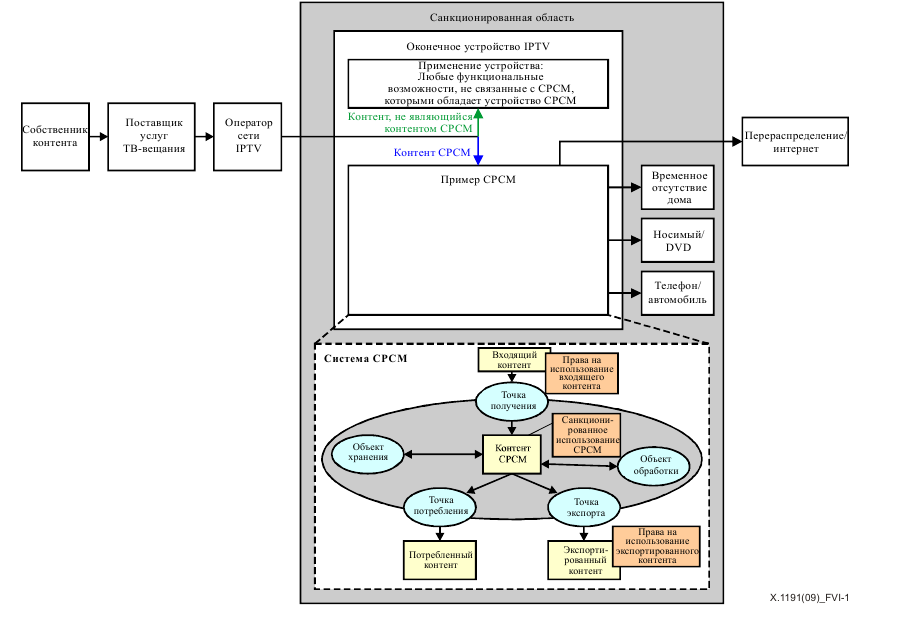


Рисунок 5.1 – Потоки контента в среде СРСМ

CPCM 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 CPCM, 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 CPCM 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 CPCM 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 CPCM не требует онлайн авторизации от поставщика услуг для добавления или удаления устройств в/из санкционированной области.

Система защиты контента CPCM 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 CPCM не является обязательным, если не оно представлено, однако, в таком случае TD не будет предоставлен доступ к любому CPCM-защищенному контенту. Тем не менее, TD не нужно внедрять все CPCM 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 CPCM, если ему не требуются функции хранения или экспорта CPCM.