РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 840 412** (13) **C2**

(51) МПК
H04N 21/2347 (2011.01)
H04N 21/266 (2011.01)
H04N 21/458 (2011.01)
H04H 60/72 (2008.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

Статус: действует (последнее изменение статуса: 27.05.2025)
Пошлина: учтена за 5 год с 13.08.2026 по 12.08.2027. Установленный срок для уплаты пошлины за 6 год: с 13.08.2026 по 12.08.2027. При уплате пошлины за 6 год в дополнительный 6-месячный срок с 13.08.2027 по 12.02.2028 размер пошлины увеличивается на 50%.

(52) СПК
H04N 21/2347 *(2023.02);* ***H04N 21/4408*** *(2023.02);* ***H04N 21/458*** *(2023.02);* ***H04N 21/266*** *(2023.02);* ***H04H 60/72*** *(2023.02);* ***H04H 60/73*** *(2023.02)*

(21)(22) Заявка: **2022121944, 12.08.2022**

(24) Дата начала отсчета срока действия патента:
12.08.2022

Дата регистрации:
22.05.2025

Приоритет(ы):
(22) Дата подачи заявки: **12.08.2022**

(43) Дата публикации заявки: **12.02.2024** Бюл. № **5**

(45) Опубликовано: **22.05.2025** Бюл. № **15**

(56) Список документов, цитированных в отчете о поиске: **EP 1332621 B1, 2016.04.20. US 2009320072 A1, 2009.12.24. US 2015350719 A1, 2015.12.03. US 2005055551 A1, 2005.03.10. US 2012051541 A1, 2012.03.01. Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt, ETSI TS 103 197, v.1.5.1, October 2008. RU 2339077 C1, 2008.11.20. US 2007266419 A1, 2007.11.15. RU 2226746 C2, 2004.04.10.**

ГОСТ Р 53531-2009, Телевидение вещательное цифровое. Требования к защите информации от несанкционированного доступа в сетях кабельного и наземного телевизионного вещания. Основные параметры. Технические требования, дата введения 2010-12-01.

Адрес для переписки:
198216, Санкт-Петербург, а/я 21, Чугориной Е.Ю.

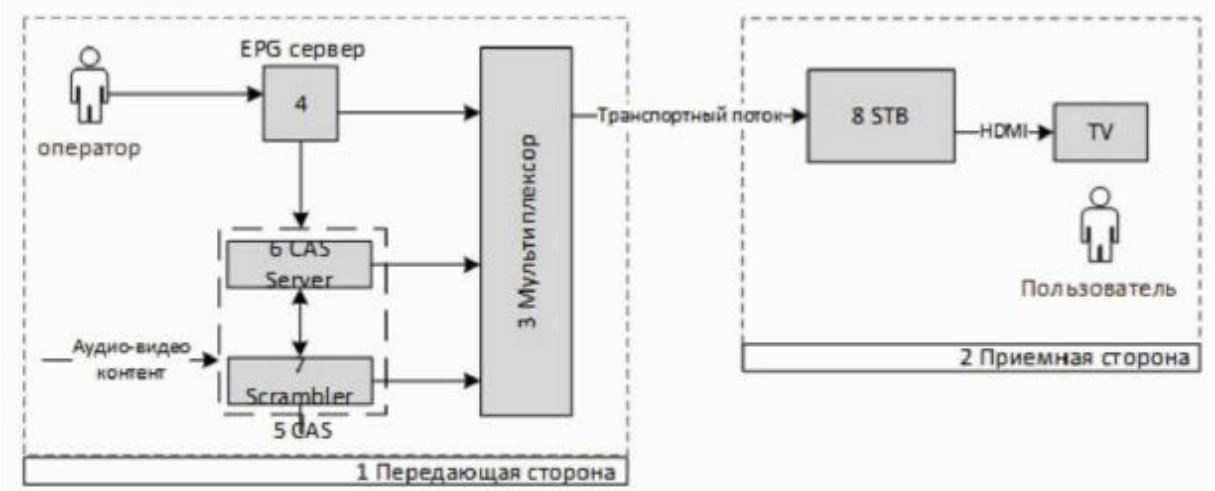
(72) Автор(ы):
Розов Дмитрий Геннадьевич (RU),
Самсонов Максим Станиславович (RU)

(73) Патентообладатель(и):
Общество с ограниченной ответственностью "Цифра" (RU)

(54) **СИСТЕМА И СПОСОБ ШИФРОВАНИЯ КОНТЕНТА СЕРВИСА ВИРТУАЛЬНЫХ КАНАЛОВ И ЕГО ДЕСКРЕМБЛИРОВАНИЯ**

(57) Реферат:

Изобретение относится к области спутникового вещания для создания выделенных "виртуальных" телевизионных каналов (ВК). Технический результат заключается в повышении надежности формирования транспортного потока сервиса предоставления ВК, обеспечивающего расширение возможностей трансляции контента без увеличения транспондерной емкости и объема памяти передающей стороны с сохранением или повышением уровня защиты контента. Предложены система и способ шифрования контента сервиса ВК и дескремблирования, где сервер электронной программы телевизионных передач (EPG) снабжен средствами формирования метаданных ВК и расписания ВК в виде компоновки выборки событий контента линейных каналов (ЛК) вещания, отбираемых по предустановленным для каждого ВК критериям и транслируемых в рамках сервиса ВК последовательно по времени, с установкой для каждого события выборки идентификатора соответствующего ВК и отметки использования события в его составе, а подсистема условного доступа (CAS) снабжена передающей и приемной частями, где передающая часть включает систему управления подписками SMS с биллинговой системой, средствами генерирования управляющих слов CW с шифрованием их сессионными ключами, средствами генерирования сообщений ECM и EMM для каждого ЛК и ВК сервиса с установкой прав доступа, причем одно и то же событие контента, транслируемое различными каналами, выполнено шифрованным общим управляющим словом, шифрованным разными сессионными ключами для каждого ЛК и ВК или их группы, а приемная часть снабжена средствами обработки EMM и ECM сообщений для установки прав доступа к каждому событию контента, получения и расшифровки ключей дескремблирования на основе CW каждого события контента, включенных в состав каждого сервиса ВК соответственно, а также средства дескремблирования на основании CW. 2 н. и 13 з.п. ф-лы, 8 ил., 2 табл.



Фиг.1

Назначение и область применения

Группа изобретений относится к области спутникового вещания и может найти применение при его организации и создании выделенных "виртуальных" телевизионных каналов.

Предшествующий уровень техники

Для систем цифрового телевидения часто характерно наличие большого количества, в основном, аудиовизуальных каналов, которые пользователь может переключать и отображать согласно своему желанию (при условии обладания соответствующими правами доступа к каждому каналу). Поэтому выбор разнообразных материалов, которые могут быть просмотрены в любой момент времени, весьма обширен, что обеспечивает пользователю возможность до определенной степени персонифицировать телевидение "под себя". Однако для

большинства пользователей отслеживание всех предлагаемых материалов, точная их классификация в соответствии со своими вкусами и составление расписания ("программирования") вывода программ, представляющих для них интерес, является задачей либо слишком сложной, либо не отвечающей их склонностям.

Кроме того, вещаемые рекламные материалы, являющиеся для вещательной компании существенным (а зачастую и жизненно важным) источником дохода, как правило, представляет интерес лишь для относительно небольшой части телезрителей. При этом адресная доставка рекламных материалов соответствующим целевым группам часто затруднена (а в большинстве обычных систем цифрового телевидения и вовсе невозможна) и неэффективна.

В публикации US20060156341 (Samsung Electronics Co Ltd, 2005г), раскрыто решение устройства для генерации виртуального канала содержащее модуль настройки виртуального канала для установки любого одного канала из множества каналов в качестве виртуального канала на пользователя; и модуль обработки виртуального канала для регистрации программы, выбранной пользователем, который установил виртуальный канал в списке программ, связанных с виртуальным каналом. Виртуальный канал может быть установлен для каждого пользователя, так что программа на любой вкус может быть просмотрена, даже если несколько пользователей используют один и тот же телевизор, с минимальным ручным вводом, требуемым через пульт дистанционного управления или встроенные кнопки выбора телевизора.

В публикации US20040205815 (Microsoft Technology Licensing LLC) раскрыто решение, согласно которому в реализации виртуальный канал связан с каждой из одной или нескольких записанных программ. Генерируется руководство по предварительному просмотру виртуального канала для отображения различных виртуальных каналов и связанных с ними записанных программ. В случае выбора виртуального канала начинается предварительный просмотр записанной программы, связанной с виртуальным каналом. В другой реализации руководство по предварительному просмотру виртуального канала включает в себя идентификаторы программ, каждый из которых соответствует записанной программе, и включает идентификаторы виртуальных каналов, каждый из которых связан с различным идентификатором программы. Руководство по предварительному просмотру виртуального канала также включает в себя выбираемый элемент управления, такой как идентификатор программы или идентификатор виртуального канала, который может быть выбран для запуска предварительного просмотра записанной программы. Кроме того, руководство по предварительному просмотру виртуального канала включает в себя предварительный просмотр для отображения предварительного просмотра записанной программы.

Из публикации патента на изобретение RU 2541923 (ВИАКСЕСС (FR), 2011) известно решение способа передачи и приема мультимедийного содержания, согласно которому способ содержит этапы, на которых: шифруют с помощью передатчика управляющее слово CWt с использованием рабочего ключа и исполняемого кода алгоритма шифрования, содержащегося в виртуальной материнской карте, для получения криптограммы Увеличенное изображение (открывается в отдельном окне) , генерируют сообщение ECM (сообщение управления предоставлением прав), содержащее криптограмму Увеличенное изображение (открывается в отдельном окне) , с использованием исполняемого кода конструктора синтаксиса в составе виртуальной материнской карты и передают указанное сообщение ECM на оконечное устройство, принимают с помощью оконечного устройства сообщение ECM, определяют местоположение криптограммы Увеличенное изображение (открывается в отдельном окне) в принятом сообщении ECM посредством исполняемого кода анализатора синтаксиса и, затем, расшифровывают криптограмму Увеличенное изображение (открывается в отдельном окне) с использованием рабочего ключа и алгоритма расшифровки. Данное решение направлено на повышение безопасности передачи данных за счет многоуровневого шифрования. К числу недостатков указанного решения можно отнести ограниченные возможности применения данного решения к отдельным мультимедийным объектам, без возможности формирования

виртуального канала на основе действующих линейных каналов без увеличения транспондерной емкости.

Наиболее близким к исследуемому решению является раскрытое в патентной публикации US20090320072 (Microsoft Corporation, 2008)) технология формирования пользовательских каналов. Технология представляет собой систему и способ генерирования виртуального канала в электронном программном гиде. Команды планирования, которые настраиваются пользователем, указывают контент, который должен быть представлен для выбора в виртуальном канале. Инструкции по планированию выполняются в порядке приоритета. Виртуальный канал заполняется описаниями контента, основанными на выполнении инструкций планирования. После того, как виртуальный канал изначально заполнен контентом, в виртуальном канале определяются промежутки вещания. В одном варианте осуществления каждый интервал трансляции заполняется другим контентом на основании настройки интервала трансляции, установленной пользователем. В другом варианте осуществления каждый интервал вещания остается пустой записью расписания в виртуальном канале.

К числу недостатков вышеуказанных аналогов и прототипа следует отнести необходимость для формирования и использования виртуального канала увеличения используемой транспондерной емкости, организации записи контента виртуального канала и наличия дополнительного запоминающего устройства для хранения записанного контента, а также необходимость в отношении воспроизводимого в составе виртуального канала контента его полного дескремблирования, как в составе виртуального канала, так и вне его. Кроме того, известные решения построены, в большинстве исходя из предпочтений пользователя, т.е. формируется на клиентском устройстве, что усложняет процесс формирования такого рода индивидуального канала, а также снижает защиту записанного контента. Таким образом, известные решения организации виртуального канала требуют существенных усложнения системы вещания при снижении уровня защиты контента и увеличении риска обеспечения несанкционированного доступа к программам линейных каналов вещания. Ограничения известных решений являются особенно существенными, если речь идет об организации виртуального канала на основе контента высокого качества. В этом случае, помимо ощутимо возрастающих вышеуказанных технических проблем существенно вырастает и стоимость решения для оператора вещания, в т.ч. за счет необходимости значительного расширения транспондерной емкости (из-за высокого битрейта контента), а также повышения рисков потери контроля над дорогостоящим контентом (пиратства).

Сущность изобретения

Техническая проблема, решаемая заявленной группой изобретений, заключается в устранении проблем, присущих предшествующему уровню техники.

Техническим результатом, достигаемым заявленным изобретением, является расширение эксплуатационных возможностей системы вещания, за счет расширения возможностей трансляции контента без увеличения транспондерной емкости и объема памяти передающей и клиентской части с одновременным повышением уровня защиты контента.

Заявленный технический результат достигается тем, что используют систему шифрования контента сервиса виртуальных каналов и его дескремблирования, включающая по меньшей мере сформированные на передающей стороне, соединенные между собой и с мультиплексором линиями связи, сервер EPG электронной программы телевизионных передач, снабженный средствами формирования расписания событий контента линейных каналов вещания, и подсистему условного доступа CAS, включающую шифрующее устройство, снабженное средствами шифрования и контроля доступа к шифрованному контенту линейных каналов, а мультиплексор снабжен, по меньшей мере, средствами формирования транспортного потока вещания линейных каналов , отличающаяся тем, что

- сервер EPG дополнительно снабжен средствами формирования метаданных виртуальных каналов, и расписания виртуальных каналов на основе формирования тематической выборки событий контента линейных каналов вещания, отбираемых по

предустановленным для каждого виртуального канала критериям параметрам и транслируемых в рамках виртуальных каналов сервиса последовательно по времени, с установкой для каждого события контента выборки идентификатора каждого соответствующего виртуального канала, в расписание которого включено событие контента и отметки использования каждого события контента в составе каждого соответствующего виртуального канала;

- а подсистема CAS, содержит выполненные программно-аппаратным образом передающую и приемную части, где передающая часть включает систему управления подписками SMS, соединенную с биллинговой системой, снабжена средствами генерирования управляющих слов CW с шифрованием их сессионными ключами, а также средствами генерирования сообщений ECM и EMM их содержащих, для каждого линейного и виртуального канала сервиса или их группы, с установкой прав доступа к трансляции указанного указанных виртуальных каналов сервиса и линейных каналов вещания, в расписании события линейного канала в составе виртуального канала и его приостановки по окончанию события., причем одно и то же событие контента, транслируемое различными каналами, выполнено шифрованным общим управляющим словом, шифрованным разными сессионными ключами для каждого линейного и виртуального канала или их группы, а приемная часть снабжена средствами обработки EMM и ECM сообщений для установки прав доступа к каждому событию контента, получения и расшифровки ключей дескремблирования на основе CW каждого события контента, включенных в состав каждого виртуального канала сервиса соответственно, а также средства дескремблирования на основании CW.

В одном из возможных вариантов осуществления заявленного решения, подсистема условного доступа CAS может быть снабжена средствами шифрования контента так, что одно и то же транслируемое событие шифруется общим управляющим словом, которое в свою очередь дополнительно шифруется разными сессионными ключами для каждого линейного и виртуального канала или их группы. При этом подсистема условного доступа CAS может быть снабжена средствами шифрования контента согласно алгоритму DVB CSA.

В еще одном возможносм варианте осуществления заявленного решения, транспортный поток на выходе мультиплексора является MPEG-2 транспортным потоком и включает, по меньшей мере: линейные каналы вещания, контент которых используют также в составе виртуальных каналов; основные и дополнительные метаданные сервиса виртуальных каналов; Linkage дескриптор; служебные таблицы MPEG-2 транспортного потока включающие: PMT таблицу структуры программ; CAT таблицу условного доступа; NIT таблицу сетевой информации; TDT таблицу даты и времени; BAT таблицу групп программ.

В другом варианте осуществления, метаданные виртуальных каналов могут быть сформированы с возможностью вещания в одном сервисе на одном транспондере, и снабжены служебной информацией со ссылкой на сервис с метаданными виртуальных каналов с возможностью обнаружения в транспортном потоке сервиса с метаданными. При этом служебная информация может быть снабжена Linkage дескриптором, добавленным в таблицу сетевой информации потока NIT с обеспечением возможности предоставления сервиса виртуальных каналов конечному пользователю без канала обратной связи пользователя. Причем служебная информация Linkage дескриптора может включать, по меньшей мере: параметры вещания метаданных виртуальных каналов SNT, идентификатор сервиса с метаданными виртуальных каналов и версию формата метаданных виртуальных каналов.

В возможном варианте осуществления, приемная часть может включать, по меньшей мере, тюнер/демодулятор, восстанавливающий входящий шифрованный транспортный поток в модулированном мультиплексором входном сигнале и передающий его на вход криптомодуля CAS module, снабженного установленной программно-аппаратным образом библиотекой системы условного доступа, интегрируемое в приёмное устройство (STB) для дескремблирования линейных и виртуальных каналов в соответствии с подписками, с обеспечением возможности дескремблирования входящего шифрованного транспортного потока и его передачу на

вход основного процессора CPU, выполненного с обеспечением возможности расшифровки входящего шифрованного транспортного потока, посредством встроенной системы безопасности, реализованной программно-аппаратным образом, и осуществления на основе предустановленного программно-аппаратным образом алгоритма обработку данных, предоставление конечному пользователю на аудио-видео выход контент каналов в модуле пользовательского интерфейса, при этом CPU снабжен секционным фильтром команд установки прав виртуального канала, обработчиком типа EMM сообщений, соответствующих виртуальному каналу и возможностью отправки команды на установку прав и сессионных ключей виртуального канала сервиса. Тогда как, крипотомодуль может быть сопряжен со смарт-картой SmartCard или снабжен встроенным эмулятором смарт-карты SmartCard emulator, содержащими ключи и права доступа к контенту.

В соответствии с любым возможным вариантом осуществления заявленного решения, передающая часть подсистемы CAS может , по меньше мере, включать средства генерирования EMM и ECM сообщений, соединенные линиями обратной связи со средством шифрования (Encryptor) управляющих слов CW сессионными ключами, причем один из входов средства генерирования ECM сообщений соединен с выходом средства генерирования EMM сообщений, а два других входа соединены по линиям обратной связи с EPG сервером и синхронизатором SCS процессов генерации CW, выход которых соединен с мультиплексором MUX, соединенным со средством шифрования транспортного потока с ключами CW(скремблером), соединенным со средством модуляции транспортного потока и его передачи на приемную часть, при этом второй вход средства генерирования EMM сообщений соединен с системой управления подписками SMS, соединенной с биллинговой системой.

Заявленный технический результат также достигается применением реализованного в выше рассмотренной системе способа шифрования контента и генерирования данных для дескремблирования сервиса предоставления виртуальных каналов, включающего последовательно осуществляемые этапы, на которых, по меньшей мере:

- формируют по предустановленным критериям на EPG сервере передающей стороны справочник виртуальных каналов сервиса, содержащий, по меньшей мере, название каналов и номер их позиции в списке каналов вещания, и расписание событий виртуальных каналов сервиса посредством компоновки выборки событий контента линейных каналов вещания, транслируемых в рамках виртуальных каналов сервиса последовательно по времени и одновременно с соответствующей трансляцией события линейного канала, с установкой для каждого события выборки идентификатора соответствующего виртуального канала и отметки использования события в его составе, с последующим формированием метаданных каждого виртуального канала.

- получают и шифруют управляющие слова, сгенерированные посредством скремблера подсистемы условного доступа, генерируют сессионные ключи и содержащие их ECM и EMM сообщения ECM и EMM линейных каналов вещания и виртуальных каналов системы сервиса, причем шифрование одного и того же транслируемого в составе линейного и виртуального каналов события осуществляют общим управляющим словом дополнительно шифрованным различными сессионными ключами для каждого линейного и виртуального канала или их группы с установкой прав доступа к трансляции указанного в расписании события линейного канала в составе виртуального канала и его приостановки по окончанию события, и передают файлы метаданных сервиса виртуальных каналов на вход мультиплексора, где формируют транспортный поток встраиванием метаданных сервиса в транспортный поток контента линейных каналов вещания и передают его на вход клиентского устройства.

В одном из возможных вариантов осуществления заявленного решения группы изобретений дополнительно осуществляют на передающей части CAS сервера генерирование, хранение, применение и автоматическое обновление по расписанию сессионных ключей технологических пакетов CAS, используемых для управления доступом к вещаемым событий линейных каналов через виртуальный канал.

При этом в другом возможном варианте осуществления, дополнительно осуществляют на передающей части CAS сервера генерирование EMM сообщений с командами управления доступом и сессионными ключами для технологических пакетов виртуальных каналов с обеспечением управления доступа абонентов к контенту сервиса виртуальных каналов в режимах в соответствии с данными о действующих подписках, полученными от биллинговой системы и/или свободного доступа абонентов, имеющих авторизированное оборудование и активацию функциональности виртуальных каналов по предустановленным в системе параметрам.

Возможен также вариант осуществления заявленного решения, в котором при формировании MPEG-2 транспортного потока посредством мультиплексора встраивают в транспортный поток, передаваемый впоследствии на вход клиентского устройства, дополнительную служебную информацию, являющуюся Linkage дескриптором в таблице сетевой информации (NIT), обеспечивающим динамическое обнаружение клиентским устройством метаданных сервиса виртуальных каналов в транспортном потоке, и на клиентском устройстве осуществляют обнаружение сервиса с метаданным в транспортном потоке посредством упомянутого Linkage дескриптора без канала обратной связи пользователя.

Согласно заявленному решению группы изобретений, при любом варианте его осуществления, возможно при генерировании расписания виртуальных каналов сервиса EPG сервером при пересечении по времени транслируемых разными линейными каналами вещания событий выборки для виртуального канала, в расписание добавляют событие с более ранним временем трансляции, а на время отсутствия отображения событий линейных каналов вещания в расписание виртуального канала добавляют предустановленное в системе сервиса технологическое событие.

Заявленный технический результат также достигается применением способа дескремблирования шифрованного контента сервиса предоставления виртуальных каналов, включающего последовательно осуществляемые посредством установленного программно-аппаратным образом в CPU приемной части алгоритма обработки сервиса виртуальных каналов этапы, включающих, по меньшей мере:

- обнаружение в транспортном потоке сервиса с метаданными виртуальных каналов;
- фильтрацию и обработку EMM и ECM сообщений с командами установки прав и сессионных ключей для доступа к событиям, включённым в виртуальные каналы, а также расшифровки управляющих слов для расшифровки событий контента, включённых в состав виртуальных каналов;
- получение метаданных виртуальных каналов и добавление виртуальных каналов в пользовательском интерфейсе STB на основе их параметров в списке линейных каналов;
- формирование расписания виртуальных каналов и его отображения в соответствующем модуле пользовательского интерфейса;
- обработка установки прав и ключей виртуального канала из потока;
- на основании подтвержденных прав доступа воспроизведение контента виртуального канала путем автоматического переключения на линейный канал вещания, осуществляющий трансляцию события контента согласно расписанию выбранного виртуального канала, расшифровку контента линейного канала вещания, транслируемого в составе выбранного виртуального канала при помощи управляющих слов в случае их успешной расшифровки;

При этом в одном из возможных вариантов осуществления заявленного решения группы изобретений, в режиме автоматического переключения на событие контента линейного канала в составе виртуального канала сервиса основной процессор CPU программно-аппаратным образом формирует и направляет запрос в криптомодуль на дескремблирование соответствующего контента, а криптомодуль инициирует обращение к смарт-карте или встроенному в криптомодуль эмулятору смарт-карты для расшифровки управляющего слова для дескремблирования контента виртуального канала и осуществляет настройку элементарных потоков для дескремблера в соответствии с информацией служебной таблицы PMT для получения

ECM сообщений, а также устанавливает в дескремблер управляющие слова CW, полученные от смарт-карты, с обеспечением возможности расшифровки входящего шифрованного потока посредством встроенной системой безопасности.

Очевидно, что как предыдущее общее описание, так и последующее подробное описание даны лишь для примера и пояснения и не являются ограничениями заявленной группы изобретений.

Любая особенность, касающаяся одного аспекта изобретения, может быть применена к другим аспектам изобретения в любом подходящем сочетании. В частности, признаки аспектов способов могут быть применены к аспектам систем и устройств, и наоборот.

Краткое описание чертежей

Ниже, исключительно в качестве иллюстрирующих примеров, будут описаны предпочтительные особенности изобретения со ссылками на прилагаемые графические фигуры:

фиг.1 обобщенная схема вещательной сети;

фиг.2 - пример формирования расписания с установкой пометки технологического перерыва: а) один виртуальный канал; б) два виртуальных канала;

фиг.3 - общая схема передающей части CAS;

фиг.4 - обобщенная схема клиентского устройства;

фиг.5 - логика управления доступом абонентов к виртуальным каналам, где SK - сессионный ключ; CW_i ($SK_{i)}$ - i-порядковое управляющее слово CW_i шифрованное i-порядковым сессионным ключом SK_i; CP ID - идентификатор пакета CAS;

фиг.6 - процесс обнаружения файла метаданных;

фиг.7 - работа сервиса виртуальных каналов на клиентском устройстве при взаимодействии с пользователем;

фиг.8 - переключение согласно расписанию виртуального канала.

Следует отметить, что прилагаемые чертежи иллюстрируют только часть некоторых из наиболее предпочтительных вариантов осуществления изобретения и не могут рассматриваться в качестве ограничений его содержания, которое включает и другие варианты его осуществления.

Осуществимость изобретения.

Заявленная группа изобретений относится к области организации спутникового вещания, а именно к системе и способу шифрования контента и генерации данных для дескремблирования сервиса предоставления виртуальных каналов конечному пользователю.

В рамках описания примера осуществления заявленного решения используются следующие термины и сокращения:

AC (Access Criteria) - критерий доступа, информация, необходимая генератору сообщений, управляющих правом доступа (ECMG), для формирования сообщения, управляющего правом доступа (ECM);

CAS (Conditional Access System) - система ограничения доступа; СОД;

CW (Control Word) - слово управления/управляющие слова: объект данных, используемый для скремблирования (операционный ключ низкого уровня, осуществляющий процесс скремблирования и дескремблирования. CW изменяется с периодичностью от 10 до 20 с);

CWG (Control Word Generator) - генератор слова управления;

DVB (Common Scrambling Algoritm) - единый алгоритм скремблирования;

ECM (Entitlement Control Message) - сообщение, управляющее правом доступа;

ECMG (Entitlement Control Message Generator) - генератор сообщений ECM;

EMM (Entitlement Management Message) - сообщение, предоставляющее право доступа;

EMMG (Entitlement Management Message Generator) - генератор сообщений EMM;

ES (Elementary Stream) - элементарный поток видеоданных (звукоданных, специальных данных) цифрового вещательного телевидения;

MPEG (Motion Pictures Expert Group) - группа стандартов сжатия видео- и аудиоданных;

MUX (Multiplexer) - мультиплексор, устройство, предназначенное для объединения нескольких потоков данных цифрового телевизионного сигнала в единый поток с

добавлением служебных битов;

PID (Packet Identifier) - идентификатор типа пакета;

SAS (Subscriber Authorization System) - система предоставления полномочий абоненту (система авторизации абонента): система, обеспечивающая организацию, упорядочение и доставку данных для формирования сообщений, предоставляющих право доступа (EMM), и сообщений ECM;

SCR (SCR DVB Compliant Scrambler; scrambler) - скремблер, соответствующий технологии DVB: устройство, предназначенное для преобразования структуры цифрового сигнала электросвязи, без изменения скорости передачи символов этого сигнала, с целью приближения его свойств к свойствам случайного сигнала;

SMS (Subscriber Management System) - система администрирования (управления) абонентами: система учета сведений об абонентах, содержащая базу данных об абонентах, о декодерах абонентов, о сервисах (службах), на которые абоненты подписались, о расчетах с абонентами и об учете платежей, поступающих от абонентов;

TS (Transport Stream) - транспортный поток данных цифрового вещательного телевидения;

Мультиплекс (multiplex) - транспортный поток на выходе транспортного мультиплексора;

Как следует из представленного на схемах фиг. 1-8 примере осуществления, система сервиса предоставления виртуальных каналов конечному пользователю (сервис виртуальных каналов) состоит из функционально связанных между собой передающей 1 (операторской) и приемной 2 (клиентской) сторон, где передающая сторона включает соединенные между собой и с мультиплексором 3 линиями связи сервер электронной программы телевизионных передач 4 (EPG сервер) и подсистему 5 условного доступа CAS (подсистема CAS), включающую сервер условного доступа 6 CAS (CAS Server) и шифрующее устройство 7, в частности, как представлено на схеме фиг.1, скремблер (Scrembler; SCR), снабженные средствами шифрования и предоставления доступа к шифрованному контенту линейных каналов. В качестве приемной 2 стороны используют клиентское устройство - цифровой спутниковый приемник 8 (set-top box, STB), оснащенный, по меньшей мере, тюнером/ демодулятором 18 (Tuner/Demodulator), принимающим входной сигнал MPEG-2 транспортного потока и передающий его после обработки на вход криптомодуля 19 (CAS module), отвечающего за дескремблирование входящего кодированный потока, вход которого соединен со входом основного процессора 23 (CPU), осуществляющим обработку данных и передающим аудио-видео сигнал, представляемый конечному пользователю пользовательским интерфейсом и контентом каналов, на аудио-видео выход. Согласно заявленному решению, вход EPG сервера соединен с внешними системами управления, в частности, управления предустановленными в памяти EPG сервера алгоритмами реализации заявленного решения посредством введения необходимых данных оператором, и/или системами головного оборудования в автоматическом режиме. При этом один из выходов EPG сервера соединен с первым входом подсистемы CAS, а второй - с одним из входов мультиплексора. На второй вход подсистемы CAS осуществляют подачу аудио/видео контента(контента) системы спутникового вещания. Как уже выше было отмечено, в обобщенной схеме реализации заявленного решения, представленной на схеме фиг.1, CAS Server и скремблер соединены между собой по линии обратной связи и снабжены выходами, связанными с соответствующими входами мультиплексора.

Функциональная связь между передающей и клиентской частью системы предоставления сервиса виртуальных каналов обеспечивается каналом передачи данных, в качестве которого используют спутниковый сигнал (Transport Stream; TS), MPEG-2 транспортный поток (ISO/IEC standard 13818-1, ETSI TS 102 154), формируемый мультиплексором передающей стороны и принимаемый клиентским устройством.

Входящие в состав системы сервиса виртуальных каналов модули, подсистемы, оборудование и аппаратные или конструктивные элементы и устройства, снабжены аппаратными, конструктивными и/или программно-аппаратными средствами, обеспечивающими функциональные возможности указанных элементов системы

сервиса виртуальных каналов согласно заявленному решению. Указанные конструктивные и аппаратные средства не выходят за рамки общепринятых конструктивных решений указанных элементов системы. При этом их функциональные возможности, прямо или косвенно, находясь в конструктивном или функциональном единстве элементов системы, регулируются заданными программно-аппаратным образом алгоритмами, предустановленными в памяти программируемых аппаратных средств системы спутникового вещания конечному пользователю, управляющие аппаратными и конструктивными средствами системы сервиса виртуальных каналов.

Сервер электронной программы телевизионных передач EPG (EPG server; EPG сервер) в составе передающей стороны системы сервиса виртуальных каналов представляет собой сервер, снабженный блоком памяти (на схеме не показан), изначально хранящим расписание передач на все каналы оператора, и снабженный средствами формирования расписания событий контента линейных каналов вещания, метаданных и расписания виртуальных каналов сервиса. Причем, расписание каждого из виртуальных каналов сервиса формируется в виде компоновки выборки событий контента линейных каналов вещания, отбираемых по предустановленным для каждого виртуального канала критериям и транслируемых в рамках виртуальных каналов сервиса последовательно по времени, с установкой для каждого события выборки идентификатора соответствующего виртуального канала и отметки использования события в его составе. Для формирования указанной выборки событий EPG сервер обеспечивает формирование метаданных виртуальных каналов, включающих основные данные: их название, позицию в общем списке каналов, расписание передач, а также дополнительные данные, например, такие как логотипы, иконки виртуальных каналов и баннеры. При этом EPG сервер также реализует формирование и генерацию метаданных сервисов и каруселей для вещания метаданных.

В общем случае реализации решения сервиса виртуальных каналов подсистема условного доступа CAS в рамках заявленного решения состоит из передающей и приемной части. Согласно представленному на схеме фиг. 3 примеру осуществления заявленного решения, передающая часть CAS осуществляет взаимодействие с EPG сервером 4 , биллинговой системой 16, мультиплексором 3, а также приемной 2 частью CAS и системы сервиса виртуальных каналов в целом, обеспечивая защиту и правила доступа пользователей к контенту линейных и виртуальных каналов за счет шифрования и предоставление доступа к шифрованному контенту линейных каналов вещания (линейных каналов) и виртуальных каналов сервиса, на основе расписания виртуальных каналов, получаемых от EPG.

Как следует из представленного на схеме фиг.3 варианта реализации заявленного решения, подсистема CAS на ее передающей стороне условно может быть подразделена на серверную 5 часть и часть, размещаемую на головном оборудовании 17. Данное разделение более удобно для выявления функциональных связей элементов подсистемы CAS, однако, для специалиста в данной области техники очевидно, что решение CAS может быть выполнено с иным распределением элементов системы, включаемых в серверную часть или головное оборудование, а также с использованием иного распределения элементов подсистемы, применяемого в данной области техники.

В соответствии с представленным примером реализации, серверная часть подсистемы CAS связанна с биллинговой 16 системой через систему управления подписками SMS 13, выход которой соединен с одним из входов генератора EMMG 9, предназначенного для генерирования EMM сообщений, формирующих право доступа к контенту линейных и виртуальных каналов сервиса, второй вход которого соединен по линиям обратной связи с шифратором 14 (Encryptor), предназначенным для шифрования управляющих слов CW и сессионных ключей. Encryptor 14, в рассматриваемом примере осуществления, реализован на базе специализированного криптопроцессора, который позволяет производить криптографические операции аппаратно в защищённом режиме. Второй вход Encryptor также по линиям обратной связи, соединен со вторым генератором сообщений ECMG 11, предназначенным для формирования управляющих ECM сообщений, второй и третий вход которого

соединен с EPG сервером 4 и генератором EMMG 9, соответственно. При этом генератор ECMG 9 соединен по линиям обратной связи через синхронизатор SCS 12 с генератором управляющих слов 10, скремблером SCR 7 и мультиплексором MUX 3 транспортного потока (мультиплексор), отнесенных на схеме фиг.3 к части связанной с головным оборудованием.

Поскольку мультиплексор 3, формирует единый транспортный поток из всех входных данных, включая вставку в транспортный поток линейных каналов и виртуальных каналов EMM сообщений, полученных от EMMG 9, вход мультиплексора 3 также соединен со выходами генератора EMMG 9 и EPG 4 сервера, а выход соединен со вторым входом скремблера SCR 7, обеспечивающего шифрование транспортного потока с ключами CW при помощи алгоритма Common Scrambling Algorithm (CSA) и, в свою очередь, соединенного с модулятором 15 (Modulator), выходные данные которого передаются на приемное устройство.

Для реализации задач предоставления сервиса виртуальных каналов, передающая часть CAS реализует сборку ECM и EMM сообщений, которые рассылаются абонентам (конечные пользователи, приемное оборудование, используемое конечными пользователями в системе трансляции контента) для расшифровки защищенного транспортного потока при условии наличия действующей подписки. Таким образом, CAS позволяет управлять доступом абонентов к своим сервисам для реализации услуг сервиса. Для управления доступом передающая часть CAS выполняет следующие действия:

1. При первом запуске EMMG генерирует исходные значения сессионных ключей, сохраняет их в базу данных CAS и передаёт в ECMG для шифрования управляющих слов CW (шаг - s1, фиг.3).

2. Система управления подписками SMS получает от биллинговой системы, обрабатывает и хранит данные о подписках абонентов на пакеты каналов (шаг- s2, фиг.3), среди которых:

- уникальный идентификатор смарт-карты абонента, используемый биллинговой системой и подсистемой CAS для идентификации абонента и адресации команд, передаваемых в EMM сообщениях;
- уникальный идентификатор пакета каналов, используемый биллинговой системой и подсистемой CAS для идентификации набора каналов, на которые выдаётся доступ в рамках данной подписки.
- дата и время начала подписки, используемые CAS для управления доступом абонента к просмотру заданного пакета каналов.
- дата и время окончания подписки, используемые CAS для управления доступом абонента к просмотру заданного пакета каналов.

3. Для формирования и рассылки прав и сессионных ключей согласно действующим подпискам, генератор EMMG с заданной в его настройках периодичностью формирует и направляет соответствующий запрос в систему управления подписками SMS, направляющей в ответ список актуальных данных (шаг-s3, фиг.3).

4. Генератор EMMG отправляет запросы на шифрование сессионных ключей (sk) в Encryptor, который осуществляет их шифрование и возвращает в шифрованном виде (sk`) в EMMG (шаг- s4, фиг.3), а EMMG генерирует и передаёт в мультиплексор (MUX) EMM сообщения (EMMs(sk`), фиг.3) согласно протоколу стандарта DVB-Simulcrypt (ETSI TS 103 197) (шаг-s5, фиг.3), которые, по меньшей мере, содержат:

- идентификатор технологического пакета CAS, который используется для управления доступом к каналам.
- права на доступ абонентов к пакетам каналов согласно действующим подпискам.
- идентификатор и значение сессионных ключей необходимых для расшифровки управляющих слов CW в ECM сообщении для дескремблирования каналов.

5. На следующем этапе генератор EMMG генерирует по расписанию новые сессионных ключи (sk), которые сохраняет в базу данных CAS и передаёт в ECMG для шифрования CW по аналогии с шагом 1 (s1 фиг 3), запуская новый цикл.

6. Одновременно, при смене скремблером с заданным интервалом, обычно 10-20 секунд, CW, по запросу от синхронизирующего компонента SCS (шаг - s7, фиг.3) генератор ECMG передаёт (шаг - s8, фиг.3) в Encryptor ключи (sk) для шифрования

CW, а затем ECMG упаковывает шифрованные сессионными ключами управляющие слова (CW`) в ECM сообщения и возвращает ECM сообщение (ECMs(CW`), фиг.3) в SCS в ответе на его запрос (шаг - s9, фиг.3) для передачи в скремблер и MUX (шаг - s10, фиг.3) сообщения, содержащие данные необходимые непосредственно для дескремблирования шифрованных каналов оборудованием STB:

- управляющие слова шифрованные сессионными ключами s(CW`);
- идентификаторы экземпляра сессионного ключа (sk), которым зашифрованы копии действующего CW;
- идентификатор технологического пакета CAS, подписка на который определяет права доступа к просмотру каналов соответствующего пакета каналов посредством доступа к сессионному ключу.

Таким образом, подсистема CAS снабжена средствами шифрования управляющих слов CW, генерирования и шифрования сессионных ключей, а также генерирования сообщений ECM и EMM их содержащих, для каждого линейного и виртуального канала системы сервиса или их группы, причем одно и то же событие контента, транслируемое различными каналами, выполнено шифрованным общим управляющим словом, шифрованным разными сессионными ключами для каждого линейного и виртуального канала или их группы.

Согласно заявленному изобретению, генератор ECM (ECMG), входящий в состав передающей части CAS, реализует сборку ECM сообщений по запросу головного оборудования (SCS). При этом в ECM передаются в зашифрованном виде CW, необходимые для расшифровки каналов из транспортного потока на приёмной стороне.

При этом генератор EMM (Entitlement Management Message Generator, EMMG) реализует сборку EMM сообщений с командами управления доступом к пакетам каналов на приёмной стороне. EMM должны содержать права (информацию о правах доступа к контенту) и сессионные ключи, необходимые для расшифровки CW. В соответствии с заданным расписанием EMMG опрашивает SMS и инициирует сборку EMM сообщений. Полученные EMM передаются в головное оборудование (MUX) по протоколу стандарта DVB-Simulcrypt с организацией цикличной рассылки с повторами команд в транспортном потоке. Согласно заявленному изобретению, MMG также генерирует и обновляет необходимые сессионные ключи в соответствии с заданным расписанием.

В соответствии с заявленным решением, мультиплексор (Multiplexer) передающей части снабжен средствами формирования транспортного потока, путем встраивания в него, по меньшей мере, контента линейных каналов вещания, расписания событий контента, команды для доступа к шифрованному контенту. При этом формирование транспортного потока (Broadcast Stream) осуществляется путем встраивания в транспортный поток медиа контента, поступающего на вход от оператора вещания, файла метаданных сервиса, дополнительных метаданных, команд для доступа к кодированному контенту, и дополнительной служебной информации. Согласно заявленному изобретению, транспортный поток на выходе мультиплексора, предпочтительно, является MPEG-2 транспортным потоком и включает, по меньшей мере: линейные каналы вещания, контент которых используют также в составе виртуальных каналов; основные и дополнительные метаданные сервиса виртуальных каналов; при необходимости, Linkage дескриптор; служебные таблицы MPEG-2 транспортного потока включающие: PAT таблица взаимосвязи программ; PMT таблицы структуры программ; CAT таблицу условного доступа; NIT таблицу сетевой информации; TDT таблицу даты и времени; BAT таблицу групп программ.

Передающая часть CAS работает в круглосуточном автономном режиме и поддерживает возможность автоматического и ручного резервного копирования данных CAS штатными средствами. Ключи хранятся только в шифрованном виде, а для шифрования CW и сессионных ключей используется специализированное аппаратное устройство - Encryptor, реализованный на базе криптопроцессора, который позволяет производить криптографические операции аппаратно в защищённом режиме. Для хранения учетных записей используются только базы данных с ограниченным доступом. Собственно и установка CAS и сервера CAS осуществляется на защищенные операционную систему и локальную сеть,

соответственно, с ограниченным доступом к программно-аппаратным средствами CAS, что обеспечивает должный контроль за безопасностью функционирования подсистемы шифрования и работы сервиса виртуальных каналов.

Приемная сторона заявленной системы сервиса виртуальных каналов, согласно представленному примеру осуществления (фиг.4), снабжена клиентским устройством STB 8, выполненным в виде цифрового спутникового приемника, снабженного, по меньшей мере, тюнером/демодулятором 18, принимающим входной сигнал MPEG-2 транспортный поток, криптомодулем 19, выполненным с обеспечением возможности расшифровки входящего шифрованного транспортного потока. В одном из вариантов осуществления заявленного изобретения, криптомодуль снабжен секционным фильтром команд установки прав виртуального канала, обработчиком EMM сообщений, соответствующих виртуальному каналу, с возможностью отправки команды на установку прав и сессионных ключей виртуального канала. При этом криптомодуль соединен с основным процессором CPU 23, осуществляющим обработку данных, предоставляющим конечному пользователю на аудио-видео выход контент линейных каналов вещания и виртуальных каналов сервиса в модуле пользовательского интерфейса. В другом варианте, основной процессор CPU клиентского устройства, выполнен с обеспечением возможности расшифровки входящего шифрованного транспортного потока, посредством встроенной системы безопасности, и осуществления обработки данных, предоставляющим конечному пользователю на аудио-видео выход контент каналов в модуле пользовательского интерфейса, при этом CPU снабжен секционным фильтром команд установки прав виртуального канала, обработчиком EMM сообщений, соответствующих виртуальному каналу и возможностью отправки команды на установку прав и сессионных ключей виртуального канала.

Процесс шифрования контента и генерирования данных для дескремблирования шифрованного контента сервиса предоставления виртуальных каналов фактически начинается с процесса формирования виртуальных каналов сервиса, поскольку на данном этапе закладывается структура данных для их шифрования и условий их дескремблирования при использовании сервиса виртуальных каналов пользователем. Сам процесс формирования контента сервиса виртуальных каналов не является предметом заявленного решения и рассматривается в данном примере осуществимости изобретения исключительно для целей пояснения сути заявленного решения и достижения заявленного технического результат его применением.

Процесс формирования виртуальных каналов сервиса осуществляется посредством последовательного выполнения следующих этапов их формирования, передачи и трансляции.

На первом этапе формирования виртуальных каналов сервиса, на EPG сервере, снабженном средствами формирования расписания событий контента линейных каналов вещания, в пользовательском интерфейсе программно-аппаратным образом, посредством оператора или в автоматическом режиме, формируют справочник виртуальных каналов, содержащий, по меньшей мере, основные данные, включающие название канала и номер позиции в списке каналов, а также дополнительные, но не обязательные, данные для каждого из каналов, например, логотип канала для отображения его в модуле пользовательского интерфейса клиентского устройства в качестве опознавательного признака канала, баннер для отображения в технологических перерывах, например, предназначенный для его применения когда в расписании виртуального канала отсутствует трансляция линейного канала. Справочник виртуальных каналов создается, хранится и редактируется исключительно на EPG сервере. Его корректировка со стороны клиентского устройства недоступна.

Формирование подборки событий, которые должны быть добавлены в расписание формируемых виртуальных каналов также может быть осуществлено программно-аппаратным образом, как вручную, так и автоматически. При этом, в качестве событий (передач) как единицы контента линейного и/или виртуального канала, могут быть приняты, например, фильмы, рекламные блоки, ток-шоу, мультфильмы, сериалы, спортивные события, новости, познавательные и/или обучающие программы, статические изображения и т.п. В качестве единицы расписания любое

событие характеризуется датой и временем его начала и окончания, а также набором метаданных, указывающих на исходный канал вещания в системе.

Формирование подборки событий виртуального канала оператором вручную осуществляется в соответствии с подбором программно-аппаратным образом событий, соответствующих заданной оператором тематики виртуального канала, либо, например, на основе результатов анализа потребления контента. Согласно предоставляемой выборке передач линейных каналов, посредством веб-интерфейса, для соответствующего события устанавливают отметку использования данного события в составе виртуального канала и идентификатор конкретного виртуального канала, в расписание которого должно быть добавлено событие. При этом одно и то же событие может быть отмечено для добавления в расписание нескольких планируемых виртуальных каналов. В свою очередь, автоматическое формирование подборки не требует непосредственного участия оператора, информация о передачах добавляется в файл метаданных программно-аппаратным образом автоматически, по результатам поиска событий в веб-интерфейсе по предустановленным критериям. Поиск осуществляется по заданным параметрам в соответствующей форме веб-интерфейса EPG сервера. В качестве параметров формирования подборки событий могут быть использованы, например, конкретные линейные каналы, жанры событий, ключевые слова и т.п.

После завершения формирования расписания на EPG сервере инициируют генерацию метаданных посредством выбора в пользовательском интерфейсе EPG сервера соответствующего предустановленного программно-аппаратным образом алгоритма и на основе данных, предустановленных или указанных оператором вручную. EPG сервер снабжен средствами генерирования на основе указанного алгоритма двух видов метаданных виртуальных каналов сервиса: основные метаданные и дополнительные метаданные, где:

- основные метаданные представляют собой расписание каждого из виртуальных каналов со справочником виртуальных каналов, где расписание для каждого из виртуальных каналов состоит из событий, транслируемых в составе линейных каналов вещания, отмеченных предустановленным образом при формировании подборки событий виртуального канала;
- дополнительные метаданные представляют собой графические данные, по меньшей мере, включающие баннер технологического перерыва, устанавливаемый в паузах между смежными трансляциями событий виртуального канала, и логотип канала и т.п. дополнительная информация, воспринимаемая в виде заставки или статичного изображения (логотипа).

При этом основные метаданные, по меньшей мере, содержат параметры событий, включая описание, время начала и окончания события, параметры линейного канала вещания в транспортном потоке SNT (Service ID, Network ID, Transport Stream ID), на котором транслируется событие виртуального канала, идентификатор виртуального канала, и параметры виртуальных каналов, включая название виртуального канала, позицию в списке каналов, ссылки на каждый из файлов дополнительных метаданных с привязкой их к виртуальному каналу, например, в виде "dvb:" URL (см. ETSI TS 102 851), то есть ссылок на конкретный файл в отдельно вещаемом сервисе.

Технологические перерывы в вещании виртуального канала могут быть вызваны, например, вследствие существующей разницы во времени между окончанием одного события (передачи) до начала вещания следующего за ним события (передачи), поскольку указанные события могут принадлежать разным линейным каналам вещания, либо разнесены по времени в расписании вещания одного линейного канала. На схеме фиг.2 представлены примеры формирования расписания виртуального канала, в том числе, с установкой пометки технологического перерыва (фиг.2а). Как следует из представленного на схеме фиг.2а) примера, в расписание виртуального канала может быть добавлено событие 1 транслируемое на линейном канале с 13:00 до 14:00 одного дня, событие 2 транслируемое на линейном канале с 14:30 до 15:00 того же дня. Возникающий между событиями временной интервал в период с 14:00 до 14:30 помечается в расписании технологическим перерывом (фиг.2а)). При генерировании расписания учитываются также и пресечения событий по времени (фиг.2а)). При пересечении событий в расписание добавляется событие,

которое начинается раньше. Например (фиг.2,а)), для одного виртуального канала оператором отмечены события линейных каналов с 13:00 до 14:00, с 13:30 до 14:30, при этом предустановленный на EPG сервере алгоритм формирования расписания виртуальных каналов и их метаданных, добавит в расписание данного виртуального канала событие с 13:00 до 14:00. Следующее событие, которое может быть добавлено в расписание данного виртуального канала должно иметь время начала события следующее только после окончания вещания первого события. В любом случае при генерировании расписания виртуальных каналов, на время отсутствия отображения событий линейных каналов сформированной выборки событий для их трансляции в рамках виртуального канала, предустановленный в памяти EPG сервера алгоритм добавляет в расписание виртуального канала отдельное событие, с типом технологического перерыва. Тип события добавляется посредством предустановленных программного аппаратным образом средств формирования метаданных и расписания виртуальных каналов EPG сервера, при генерировании файла метаданных в соответствующем параметре, например, так, как представлено в примере осуществления заявленного изобретения в таблице 1. При этом, как видно из представленного в Таблице 1 примере, для события типа «технологический перерыв» список необходимых параметров, указанных в файле метаданных, отличается от списка необходимых параметров событий линейных каналов, транслируемых в составе виртуальных каналов сервиса.

Описание информационных параметров файла метаданных и их в файле метаданных приводится в таблице ниже.

Таблица 1

Описание параметров файла метаданных виртуальных каналов

Блок	**Параметр**	**Описание параметра**	**Наличие**
schedule	channel_id	Идентификатор виртуального канала	Обязательно
	type	Тип события виртуального канала: 1 - событие линейного канала 2 - событие, являющееся технологическим перерывом	Обязательно
	transport_stream / service_id	Идентификатор линейного канала используемого события в транспортном потоке (Original Network ID, Transport Stream ID, Service ID)	Обязательно для события линейного канала
	transport_stream / transport_stream_id		
	transport_stream / original_network_id		
	start	Дата и время начала события	Обязательно
	end	Дата и время завершения события	Обязательно
	descriptions / …	Описание события согласно стандарту	Обязательно для события

			линейного канала
	production_date	Дата производства	Обязательно для события линейного канала
	content	Идентификатор жанра события	Обязательно для события линейного канала
	parental_rating	Возрастное ограничение события	Обязательно для события линейного канала
virtual_channels	id	Идентификатор виртуального канала	Обязательно
	name	Название виртуального канала	Обязательно
	logical_number	Номер виртуального канала в списке каналов	Опционально
	channel_icon	Ссылка на иконку виртуального канала	Опционально
	banner	Ссылка на баннер технологического перерыва виртуального канала	Обязательно
metadata	subversion	Номер сборки файла метаданных	Обязательно
	version	Минорная версия файла метаданных	Обязательно
	build	Мажорная версия файла метаданных	Обязательно

В результате генерации основные метаданные представляют собой файл в формате JSON, дополнительные метаданные - архив, содержащий все необходимые файлы графических данных.

При изменении данных виртуальных каналов на EPG сервере, например, при актуализации расписания, изменения баннеров и пр., инициируют повторное генерирование необходимых данных с последующей передачей компонентам передающей стороны в CAS и на вход мультиплексора.

Сгенерированные метаданные формируют известным из уровня техники способом, посредством соответствующих предустановленных программно-аппаратных средств EPG сервера, в потоки и передают на вход мультиплексирующего устройства. Файл, содержащий основные метаданные сервиса виртуальных каналов, передается в виде

потока карусели данных (Data carousel, ETSI TR 101 202). Архив, содержащий дополнительные метаданные формируют и передают в виде потока объектной карусели (Object carousel, ETSI TR 101 202). Метод каруселей является обязательным способом вещания данных в транспортном потоке для обеспечения гарантии доставки данных на клиентское устройство, с учетом циклического повторения данных в потоке.

На следующем этапе осуществляют передачу сформированного расписания виртуальных каналов от EPG сервера в подсистему условного доступа CAS.

Для последующего дескремблирования линейных каналов в составе виртуальных каналов, посредством предустановленного на EPG сервере программно-аппаратным образом алгоритма, передают в подсистему удаленного доступа, на CAS сервер, основные метаданные (сгенерированное расписание виртуальных каналов) одновременно с передачей основных метаданных на вход мультиплексора. Основные метаданные, как было указано ранее, в обязательном порядке содержат следующую информацию: параметры канала (в том числе параметры SNT линейных каналов, используемых в составе виртуальных каналов сервиса), дата/время начала и окончания событий линейных каналов.

На основании полученных от подсистемы CAS данных и поступающего на вход подсистемы головного оборудования аудио-видео контента, посредством скремблера SCR осуществляют шифрование контента и генерирование данных вещаемых каналов и контента в подсистеме условного доступа CAS (фиг3) соответствующей DVB-Simulcrypt стандартам (ETSI TS 103 197), согласно алгоритму DVB CSA (Digital Video Broadcasting Common Scrambling Algorithm).

Рассмотренный выше в соответствии с заявленным решением процесс шифрования/расшифрования (скремблирования/дескремблирования) в общем процессе организации сервиса виртуальных каналов осуществляют следующим образом.

На вход шифрующего устройства (скремблера, SCR) подают открытый (нешифрованный) транспортный поток (TS), в составе которого, помимо дополнительной информации, имеется аудио и видео контент линейных спутниковых каналов вещания. Скремблер посредством генератора управляющих слов (на схемах фиг.3 не показан), выполненного программно-аппаратным образом, генерирует управляющие слова (CW), используемые для шифрования транспортного потока. Функциональный компонент CAS сервера - генератор EMM сообщений (EMMG) (фиг.3) передает сгенерированный сессионный ключ (OpKey, на схеме фиг.3 - sk), используемый для шифрования/расшифровывания CW. Скремблер передает CW функциональному компоненту CAS сервера, в генератор ECM сообщений (ECMG) (фиг.3) для последующей генерации ECM сообщения, содержащего шифрованные управляющие слова CW. В свою очередь, управляющие слова CW шифруют с использованием сессионных ключей для последующей генерации ECM сообщения, содержащего шифрованные управляющие слова CW. Контент транспортного потока шифруют с использованием управляющих слов CW и добавлением ECM сообщений. Таким образом, шифрование одного и того же события, транслируемого различными каналами, осуществляют общим управляющим словом, шифрованным различными сессионными ключами для каждого линейного и виртуального канала или их группы, и передают файлы метаданных сервиса виртуальных каналов на вход мультиплексора. EMMG генерирует EMM сообщения, содержащие служебные данные, информацию о правах доступа и специализированные команды. Сгенерированные EMM сообщения также передаются на вход мультиплексора, где формируют транспортный поток встраиванием метаданных сервиса в транспортный поток контента линейных каналов вещания. В итоге на выходе мультиплексора в контексте передающей части подсистемы условного доступа получают шифрованный транспортный поток, содержащий ECM и EMM сообщения согласно стандарту DVB (ETSI TS 102 470-1), которые передают на вход клиентского устройства для принятия и расшифровки защищенного транспортного потока на приемной части системы спутникового вещания при условии наличия действующей подписки. Таким образом, CAS совместно с головным оборудованием позволяет управлять доступом абонентов к своим сервисам для реализации услуг платного телевидения.

На клиентском устройстве расшифровку кодированного контента осуществляют посредством криптомодуля и смарт-карты. На смарт-карте хранятся сессионные ключи и права доступа, записанные посредством криптомодуля после получения EMM из транспортного потока. По запросу системы криптомодуль осуществляет проверку сохраненного на смарт-карте сессионного ключа с определенным ECM сообщением. Положительный результат сравнения подтверждает актуальность сессионного ключа и последующее его использование для вычисления CW и, как следствие, расшифровки кодированного контента.

Согласно заявленному изобретению, для обеспечения доступа к шифрованному контенту только в рамках сервиса виртуального канала, вышеупомянутая система условного доступа заявленного решения обеспечивает выполнение следующих действий:

- обработку списка виртуальных каналов и их расписания;
- генерирование и хранение отдельного набора сессионных ключей для доступа к кодированному контенту виртуальных каналов;
- шифрование управляющих слов CW дополнительным сессионным ключом виртуального канала;
- генерирование и рассылку EMM с сессионными ключами виртуального канала.

Ограничение доступа к контенту, как линейного, так и виртуального каналов может осуществляться не только временными рамками вещания события, транслируемого по данным каналам, но и, как было указано ранее, наличием прав допуска к просмотру контента, определяемых подпиской пользователя сервиса виртуальных каналов. Для учета данного обстоятельства, согласно заявленному решению, дополнительно осуществляют на передающей части CAS сервера генерирование EMM сообщений с командами управления доступом и сессионными ключами для технологических пакетов виртуальных каналов с обеспечением управления доступа абонентов к контенту сервиса виртуальных каналов в режимах в соответствии с данными о действующих подписках, полученными от биллинговой системы. Под технологическим пакетом виртуальных каналов понимают группу каналов объединяемых оператором в пакеты с разными правами доступа, например, пакет «Детский», «Спортивный» и т.д. Такое пакетное объединение возможно как для линейных, так и для виртуальных каналов. Соответственно права доступа к виртуальным каналам в рамках технологического пакета могут быть настроены как на уровне канала как такового, так и на уровне пакета.

Однако, возможна реализация и другого варианта осуществления заявленного решения, например, при осуществлении маркетинговых акций, когда обеспечивается свободный доступ абонентов, имеющих авторизированное оборудование и активацию функциональности виртуальных каналов по предустановленным в системе параметрам акций, осуществляемых с использованием виртуальных каналов.

Таким образом, заявленное решение позволяет обеспечить в рамках сформированного на передающей стороне, без участия пользователей, виртуального канала локальный доступ к выбранным событиям линейного канала вещания при наличии подписки или иного авторизованного доступа к виртуальному каналу вне зависимости от наличия или отсутствия прав доступа к линейному калу или группе линейных каналов, события которого вошли в состав виртуального канала.

После обработки полученного расписания генератор сообщений EMM осуществляет генерацию набора сессионных ключей для доступа к событиям виртуальных каналов, отличных от сессионных ключей для доступа к линейным каналам вещания. Управляющие слова дополнительно шифруют сгенерированными сессионными ключами виртуального канала. Таким образом, один и тот же контент скремблируется (шифруется) посредством нескольких сессионных ключей: один из которых используется для дескремблирования контента вне сервиса, другой используется для дескремблирования того же контента при его воспроизведении в рамках виртуального канала сервиса.

Далее осуществляют передачу шифрованного потока данных для дескремблирования от подсистемы CAS на вход мультиплексора, где передача EMM сообщений от CAS сервера, необходимых для дескремблирования заданных в

расписании событий в рамках виртуального канала, последовательно проверяется на двух уровнях:

а) наличие доступа к виртуальному каналу в соответствии с подпиской. Управляется EMM с командой установки прав и сессионного ключа для доступа к виртуальному каналу по подписке в соответствии с ее установленной длительностью;

б) наличии доступа к заданным вещаемым передачам, которые включены в виртуальный канал. Управляется вставкой в ECM данного канала копии CW, шифрованной сессионным ключом виртуального канала только на время вещания передачи, включённой в виртуальный канал. Рассылка команд приостановки доступа к передаче не требуется.

На мультиплексоре настраивают встраивание данных, полученных от EPG сервера и подсистемы CAS, в транспортный поток TS. Для метаданных, полученных от EPG сервера задают вручную или автоматически программно-аппаратным образом, например, посредством интерфейса подсистемы CAS, параметры вещания сервиса - SNT. Для вещания метаданных выделяют отдельный сервис в составе транспортного потока: для основных метаданных и для дополнительных метаданных выделяют отдельный пакет (PID) для упрощения поиска нужной составляющей метаданных.

Поскольку в рамках предоставляемого сервиса для формирования виртуального канала не требуется копирование контента линейного канала вещания и/или какая-либо запись отдельных событий, включенных в состав виртуального канала в блок памяти аппаратной части передающей и/или принимающей стороны, а трансляция событий виртуального канала осуществляется путем организации ограниченного доступа к линейному каналу вещания на период его трансляции и не имеет распространения на доступ к линейному каналу вне рамок события, транслируемого одновременно по линейному и виртуальному каналам, вещание метаданных в одном сервисе, согласно рассматриваемому примеру осуществления, осуществляют только на одном транспондере, что позволяет экономить транспондеру ёмкость, используемую для вещания метаданных.

Для обнаружения сервиса с метаданными в этом случае используется служебная информация с ссылкой на сервис с метаданными, являющийся Linkage дескриптором (Linkage descriptor, ETSI EN 300 468 V1.14.1). Linkage дескриптор добавляют в графическом интерфейсе мультиплексирующего устройства в таблицу сетевой информации потока - NIT (Network Information Table, ETSI EN 300 468). Расположение дескриптора в потоке обуславливается тем, что NIT таблицы на всех транспондерах оператора содержит один и тот же набор данных.

Среди служебной информации, содержащейся в Linkage дескрипторе, присутствуют параметры вещания метаданных (SNT), идентификатор сервиса и версия формата метаданных.

Представление структуры Linkage дескриптора на примере приведено ниже в таблице 2.

Таблица 2

Original Network ID	263
Transport Stream ID	601
Service ID	123
Linkage type	0x82
Data Bytes	56 5f 43 68 00 00 00 01

В Linkage дескрипторе задаются следующие параметры, доступные для редактирования:

1. Transport Stream ID, Original Network ID, Service ID - параметры вещания файла метаданных (SNT).

2. Data Bytes - строка шестнадцатеричных данных, содержащая:

1) signature (четыре байта) - идентификатор сервиса (используется непосредственно для сопоставления дескриптора с сервисом),

2) json_format_version - версия формата файла метаданных (для возможности обновления сервиса без обратной совместимости).

Использование Linkage дескриптора позволяет сформировать сервис виртуальных каналов без обратной связи пользователя, что обеспечивает дополнительную защиту контента при реализации возможности его просмотра в составе виртуальных каналов.

Сформированный в соответствии с заявленным изобретением на выходе мультиплексора MPEG-2 транспортный поток, содержит, по меньшей мере:

- линейные каналы, аудио-видео контент которых будет использован в составе виртуальных каналов;
- сервис с метаданными виртуальных каналов (основные и дополнительные метаданные);
- Linkage дескриптор для обнаружения сервиса с метаданными виртуальных каналов;
- служебные таблицы MPEG-2 транспортного потока (согласно стандарту EN 300 468) среди которых обязательно присутствуют:
- PMT(Program Map Table) - таблица структуры программ. Включается в поток для каждой телепрограммы и содержит PID компонентов телепрограммы - видео, звука, синхронизации. Кроме того, PMT содержит PID сообщения ECM системы условного доступа, если в программе присутствуют зашифрованные элементарные потоки.
- CAT (Condition Access Table) - таблица условного доступа. Содержит отдельные PID всех EMM сообщений.
- NIT (Network Information Table) - таблица сетевой информации. Содержит параметры системы передачи данных.
- TDT (Time Data Table) - таблица даты и времени. Является источником достоверного времени для клиентского устройства, позволяя составить расписание виртуальных каналов.
- BAT (Bouquet Association Table) - таблица групп программ. Содержит информацию, позволяющую в настоящем решении клиентскому устройству находить соответствующие каналы оператора и сопутствующую им служебную информацию.

Далее транспортный поток TS поступает на клиентское устройство (фиг.4) приемной части сервиса. Обработка транспортного потока TS и метаданных сервиса виртуальных каналов клиентским устройством осуществляется следующим образом.

В роли клиентского устройства, как было ранее отмечено, выступает цифровой спутниковый приемник STB 8, оснащенный по меньшей мере тюнером/ демодулятором 18, принимающим входной сигнал MPEG-2 транспортный поток, криптомодулем 19 CAS модуля 20, отвечающим за дескремблирование входящего шифрованного потока и основным процессором CPU 23, осуществляющим обработку данных и передающий аудио-видео сигнал, предоставляющийся конечному пользователю пользовательским интерфейсом и контентом каналов, на аудио-видео выход («HDMI»). Так же в приемник установлена смарт-карта 22 или встроенный эмулятор смарт-карты 21 в составе криптомодуля 19, далее просто «смарт-карта», содержащая ключи и права доступа к контенту. При этом, в криптомодуле 19 реализован секционный фильтр (на схеме фиг.4 не показан) на команды установки прав виртуального канала, обработчик типа EMM сообщений, соответствующий виртуальному каналу и отправка на смарт-карту команду на установку прав и сессионный ключ виртуального канала. При отсутствии ошибок работа сервиса виртуальных каналов на STB осуществляется CPU следующим образом, где осуществляют:

- обнаружение в транспортном потоке сервиса с метаданными виртуальных каналов;
- фильтрацию и обработку ECM и EMM сообщений с командами установки прав и сессионных ключей для доступа к событиям, включённым в виртуальные каналы, а также расшифровки управляющих слов для расшифровки событий контента, включённых в состав виртуальных каналов;
- получение метаданных виртуальных каналов и добавление виртуальных каналов в пользовательском интерфейсе STB на основе их параметров в списке линейных

каналов;

- формирование расписания виртуальных каналов и его отображения в соответствующем модуле пользовательского интерфейса;
- воспроизведение контента виртуального канала путем автоматического переключения на линейный канал вещания, осуществляющий трансляцию контента текущего события согласно расписанию выбранного виртуального канала, расшифровку контента линейного канала вещания, транслируемого в составе выбранного виртуального канала при помощи управляющих слов в случае их успешной расшифровки;
- обработку установки прав и ключей виртуального канала из потока;
- отображение баннера-заглушки в технологических перерывах на виртуальном канале.

Обнаружение метаданных сервиса в транспортном потоке (фиг.6) осуществляется первостепенно CPU STB посредством обработки соответствующей таблицы во входящем транспортном потоке (NIT) с обнаружением linkage дескриптора и проверкой его валидности. По имеющимся в linkage дескрипторе параметров SNT сервиса в TS происходит загрузка соответствующих метаданных.

Благодаря вещанию метаданных сервиса на каждом из транспондеров входящего сигнала, достаточно наличие спутникового сигнала на антенном входе STB для формирования виртуального канала.

После загрузки CPU метаданных в пользовательском интерфейсе отображается виртуальный канал с названием, позицией и логотипом, определенным в метаданных и отображаемого в соответствующе модуле пользовательского интерфейса наравне с названием виртуального канала. В дополнительном модуле пользовательского интерфейса, наравне с линейными каналами, реализуется отображение расписания виртуального канала, для ознакомления и с поддержкой функциональности, реализованной для линейных каналов.

При определении CPU во входящем транспортном потоке новой версии метаданных осуществляется обновление метаданных и на STB, начиная с загрузки метаданных.

Работа сервиса виртуальных каналов на клиентском устройстве при взаимодействии с пользователем (фиг.7, 8) осуществляется следующим образом.

Работа сервиса после выбора пользователем просмотра виртуального канала, например, посредством выбора канала в списке по нажатию кнопки пульта ,дистанционного управления, по большей части состоит в отображении контента выбранного виртуального канала (автоматическое переключение согласно расписанию) с дескремблированием соответствующего контента.

При выборе просмотра виртуального канала CPU STB осуществляет автоматическое включение контента согласно расписанию: переключение на линейный канал по параметрам SNT, если текущее событие транслируется на линейном канале, или отображение баннера, полученного в составе метаданных, если текущее событие является технологическим перерывом. Последующая работа сервиса виртуального канала осуществляется согласно полученному расписанию: по завершении текущего события осуществляется переключение на SNT другого линейный канал, если следующее событие транслируется на линейном канале, или отображение баннера, полученного в составе дополнительных метаданных, в случае если следующее событие является технологическим перерывом.

После автоматического переключения (фиг.7) на определенный линейный канал в составе виртуального, основной процессор осуществляет запрос к криптомодулю на дескремблирование соответствующего контента. Криптомодуль инициирует обращение к смарт-карте для расшифровки управляющего слова для дескремблирования контента виртуального канала, производит настройку элементарных потоков для дескремблера в соответствии с информацией служебной таблицы PMT (служебная таблица Program Map Table) для получения ECM сообщений и устанавливает в дескремблер управляющие слова CW, полученные от смарт-карты, либо посредством основного процессора, выполненного с обеспечением возможности расшифровки входящего шифрованного потока посредством встроенной системы безопасности.

Согласно заявленному решению в режиме просмотра виртуального канала CPU цифрового спутникового приемника может осуществлять автоматическое включение трансляции контента линейного канала вещания согласно расписанию путем переключения на линейный канал вещания по параметрам SNT, если текущее событие транслируется на линейном канале вещания, или отображение баннера, полученного в составе метаданных виртуального канала, если текущее событие является технологическим событием.

Таким образом, происходит дескремблирование линейного канала на время вещания события при его воспроизведении в рамках сервиса виртуального канала, при этом контент линейного канала вне сервиса виртуального канала остается кодированным.

Для поддержки данной модели виртуальных каналов CAS предоставляет доступ только для заданных телепрограмм в режиме работы виртуального канала. При этом:

1. Доступ к телепрограммам виртуального канала при просмотре канала-источника остаётся закрыт (при отсутствии действующей подписки). То есть, все телепрограммы при просмотре обычного канала остаются недоступны, если нет подписки.

2. Наличие подписок на каналы-источники не влияют на список телепрограмм доступных в виртуальном канале. В виртуальном канале остаются доступны только заданные в расписании канала телепередачи (независимо от наличия подписок на каналы-источники).

3. Изменение настроек телепрограммы через виртуальный канал автоматически влияет на логику управления доступом CAS:

- при добавлении телепрограммы в виртуальный канал - доступ предоставляется в соответствии с расписанием вещания телепрограммы (на время вещания в потоке). Для этого ECMG на время вещания телепрограммы в виртуальном канале шифрует копию CW вещаемого канала при помощи сессионного ключа данного виртуального канала (фиг.5). В результате STB абонентов с действующей подпиской на данный виртуальный канал имеют техническую возможность расшифровать CW и открыть канал во время вещания телепрограммы.

- при удалении телепрограммы из виртуального канала - доступ блокируется за счёт того что ECMG перестаёт использовать сессионный ключ виртуального канал при шифровании CW.

- при изменении расписания вещания телепрограммы из виртуального канала - время доступности контента канала смещается в соответствии с новым временем начала/окончания. Это так же контролируется ECMG применением сессионного ключа виртуального канала строго в соответствии с актуальным расписанием вещания виртуального канала.

4. Реализуется поддержка управления доступом одновременно нескольких виртуальных каналов с возможностями:

- включать один и тот же вещаемый канал в несколько виртуальных каналов.

2- добавлять в виртуальный канал несколько телепрограмм, вещаемых в одно и то же время (имеющих пересечение).

Заявленная группа изобретений также позволяет:

1) Расширить список пакетов каналов без вещания нескольких копий каналов (которые включены в несколько пакетов каналов).

2) Гибко и безопасно ограничить доступ к отдельным телепередачам (по условиям правообладателей, правилам распределения контента в услугах, и другим ограничениям).

3) Предоставлять доступ к телепередачам только в рамках виртуального канала. CAS предоставляет доступ к телепередачам в рамках вещаемых каналов только при наличии действующей подписки на соответствующие пакеты каналов.

4) Управлять доступом к виртуальным каналам по подпискам от биллинговой системы, так и массово всем авторизированным устройствам при активации доступа к функции виртуальных каналов (всем либо только заданным устройствам).

Таким образом, для поддержания комплексных сценариев использования системы и способа шифрования дескремблирования контента сервиса виртуальных каналов,

подсистема CAS следующим образом участвует в следующих операциях организации сервиса виртуальных каналов:

- организация виртуального канала, включая: создание; активация; изменение параметров (названия); отключение (временная приостановка); удаление;
- формирование расписания виртуального канала, включая: создание; изменение параметров; удаление.

При создании виртуального канала сервер CAS принимает от сервера EPG запрос на создание нового виртуального канала и проверяет на корректность значения параметров виртуального канала (внешний идентификатор, статус, название и описание). А также, в некоторых случаях, осуществляет проверку корректности значения внешнего идентификатора услуги биллинговой системы, управляющей доступом к данному виртуальному каналу. В случае некорректных значений сервер CAS возвращает в сервер EPG ошибку (код и текстовое описание ошибки). При этом, информацию о новом виртуальном канале с привязкой к услуге, управляющей доступом (опционально) сервер CAS сохраняет в базе данных CAS, а также создаёт в ней новый технологический пакет для управления доступом к данному виртуальному каналу (фиг.5). Генерирует и сохраняет в базе данных CAS первый сессионный ключ для шифрования CW при управлении доступом к данному виртуальному каналу и возвращает в EPG сервер ответ со статусом успешного создания виртуального канала.

В результате успешного создания виртуального канала сервер CAS переходит в готовность к обработке команд от биллинговой системы на добавление, изменение (дат начала и окончания) и удаления подписок на данный виртуальный канал, а также обработке команд от сервера EPG на добавление, изменение и удаление расписания вещания виртуального канала и управлению доступом к виртуальному каналу для абонентов в соответствии с подписками биллинговой системы. Доступ индивидуально для абонентов по подпискам от биллинговой системы может быть реализован при помощи сессионных ключей технологического пакета, управляющего доступом к данному виртуальному каналу (фиг.5).

При переключении каналов сервиса на приёмной стороне:

- при переключении с линейного канала на виртуальный канал - приёмная часть CAS получает и обрабатывает от программного обеспечения приёмника запрос на дескремблирование события контента в режиме виртуального канала. При наличии у абонента действующих прав доступа к технологическому пакету CAS для виртуального канала (по подписке на уровне сессионных ключей), и глобальной доступности телепередачи для просмотра в виртуальном канале (на уровне CW), производится расшифровка CW и инициализацию процесса дескремблирования транспортного потока (фиг.5);
- при переключении с одного виртуального канала на другой виртуальный канал - выполняется логика аналогичная переключению линейного канала на виртуальный канал;
- при переключении с виртуального канала на обычный вещаемый (линейный) канал, на котором осуществляется вещание события контента добавленного в виртуальный канал, с которого осуществляется переключение - приёмная часть CAS получает и обрабатывает от программного обеспечения приёмника запрос на дескремблирование телепередачи в режиме обычного канала. При отсутствии у абонента действующих прав доступа к технологическому пакету CAS именно для обычного вещаемого канала выполняется отказ от дескремблирования, даже при наличии действующих прав для дескремблирования канала через виртуальный канал.

Таким образом, для поддержки функциональности виртуальных каналов передающая часть CAS реализует:

1. Получение, обработку и хранение подписок на виртуальные каналы от биллинговой системы.
2. Получение и обработку запросов на шифрование ключей скремблирования транспортного потока (CW) от головного оборудования станции вещания согласно стандартам DVB-Simulcrypt (ETSI TS 103 197).
3. Получение, обработку и хранение списка виртуальных каналов (и их параметров) от сервера EPG.

4. Получение, обработку и хранение расписаний вещания телепередач для виртуальных каналов от сервера EPG.

5. Генерирование, хранение, применение и автоматическую смену по расписанию сессионных ключей технологических пакетов CAS, используемых для управления доступом к вещаемым телепередачам через виртуальный канал.

6. Генерирование ECM сообщений с учётом расписания вещания телепередач для виртуальных каналов. Для управления принципиальной доступностью к отдельным телепередачам через виртуальные каналы (возможность расшифровать CW сессионным ключом, выданным для доступа через виртуальный канал).

7. Генерирование EMM сообщений с командами управления доступом и сессионными ключами для технологических пакетов виртуальных каналов. Для управления доступом абонентов к виртуальным каналам в двух режимах:

- индивидуально в соответствии с подписками, полученными от биллинговой системы. Для предоставления абонентам услуг на базе виртуальных каналов по платным подпискам;
- глобально для всех абонентов, имеющих авторизированное оборудование и активацию функциональности виртуальных каналов. Для оптимизации битрейта EMM при проведения массовых маркетинговых акций с использованием виртуальных каналов.

На приёмной части CAS в рамках сервиса виртуальных каналов осуществляется дескремблирование шифрованного транспортного потока и управление доступом к контенту следующим образом:

1. Посредством установленной программно-аппаратным образом Библиотеки CAS (программного обеспечения (алгоритма) CAS, интегрируемое в приёмное устройство (STB) для дескремблирования каналов в соответствии с подписками) реализует:

- фильтрацию и обработку EMM сообщений с командами установки прав и сессионных ключей для доступа к телепередачам, включённым в виртуальные каналы;
- получение и обработку запросов от программного обеспечения приёмника на дескремблирование телепередач виртуальных каналов;
- фильтрацию и обработку ECM сообщений - для получения и расшифровки ключей дескремблирования телепередач (CW), включённых в состав виртуальных каналов. При этом расшифровка CW и дескремблирование телепередачи производится только при включении запрошенной телепередачи в данный виртуальный канал. А также при наличии необходимых прав доступа и сессионных ключей (выданных по подписке). См. фиг.4;
- инициализацию дескремблирования заданного канала при помощи CW в случае их успешной расшифровки;
- передачу в программное обеспечение приёмника информации о подписках на услуги виртуальных каналов и текущем статусе доступа к ним.

2. Программное обеспечение встроенной или внешней смарт-карты реализует в безопасном аппаратном окружении:

- расшифровку и хранение прав абонента на доступ к пакету каналов, а также сессионных ключей при наличии действующих прав (подписок на пакет каналов);
- расшифровку и выдачу в библиотеку CW для дескремблирования заданного канала при наличии действующих прав на просмотр.

Модули, блоки и другие компоненты были описаны выше с точки зрения их особенностей и обеспечиваемых ими функций, вместе с необязательными и предпочтительными особенностями. С предоставленной информацией и приведенными характеристиками и описанием практическая реализация этих особенностей и конкретные детали реализации могут быть определены разработчиком. Например, определенные модули можно было бы реализовать с помощью программного обеспечения, а некоторые или все компоненты могут быть реализованы с помощью специализированных аппаратных средств.

Описанные выше модули и компоненты являются не более чем иллюстративными примерами. Изобретение может быть реализовано разнообразными способами и, в частности, некоторые компоненты можно интегрировать с другими, выполняющими подобные функции, или некоторые компоненты можно опускать в упрощенных

реализациях. Аппаратные и программные реализации каждой из описанных функций могут комбинироваться в любых сочетаниях, как между несколькими компонентами, так и для каждого отдельного компонента.

Понятно, что функции, выполняемые аппаратным обеспечением, компьютерным программным обеспечением и тому подобным, выполняются на электрических и подобных сигналах или с их использованием. Программные реализации могут храниться в ПЗУ или могут быть "зашиты" во флэш-память.

Совершенно очевидно, что настоящее изобретение было описано выше и использованием исключительно иллюстративных примеров возможных вариантов его осуществления, и возможны различные изменения деталей реализации, не приводящие к выходу за рамки настоящего изобретения.

Каждый из признаков, раскрытых в описании и (в соответствующих случаях) в формуле изобретения и на графических фигурах, может реализовываться как независимо, так и в любом подходящем сочетании.

Заявленное решение группы изобретений обеспечивает простое решение расширения эксплуатационных возможностей системы спутникового вещания, за счет расширения возможностей трансляции контента без увеличения транспондерной емкости и объема памяти передающей и клиентской части с одновременным повышением уровня защиты контента путем формирования виртуальных каналов, трансляция контента которых не требует предварительной записи контента линейных каналов вещания, за счет формирования расписания трансляции виртуального канала путем формирования выборки событий контента линейных каналов вещания, отбираемых по предустановленным для каждого виртуального канала критериям и транслируемых в рамках виртуальных каналов сервиса последовательно по времени и обеспечения вещания контента виртуального канала путем защищенного переключения на транслируемый в соответствии с расписанием виртуального канала контент линейных каналов, транслируемый в указанное время.

Формула изобретения

1. Система шифрования контента сервиса виртуальных каналов и его дескремблирования, включающая по меньшей мере сформированные на передающей стороне, соединенные между собой и с мультиплексором линиями связи, сервер электронной программы телевизионных передач (EPG), снабженный средствами формирования расписания событий контента линейных каналов вещания, и подсистему условного доступа (CAS), включающую шифрующее устройство, снабженное средствами шифрования и контроля доступа к шифрованному контенту линейных каналов, а мультиплексор снабжен, по меньшей мере, средствами формирования транспортного потока вещания линейных каналов, отличающаяся тем, что

сервер EPG дополнительно снабжен средствами формирования метаданных виртуальных каналов и расписания виртуальных каналов на основе формирования тематической выборки событий контента линейных каналов вещания, отбираемых по предустановленным для каждого виртуального канала критериям, параметрам и транслируемых в рамках виртуальных каналов сервиса последовательно по времени, с установкой для каждого события контента выборки идентификатора каждого соответствующего виртуального канала, в расписание которого включено событие контента и отметки использования каждого события контента в составе каждого соответствующего виртуального канала;

а подсистема CAS содержит выполненные программно-аппаратным образом передающую и приемную части, где передающая часть включает систему управления подписками (SMS), соединенную с биллинговой системой, средствами генерирования управляющих слов (CW) с шифрованием их сессионными ключами, а также средствами генерирования сообщений ECM и EMM, их содержащих, для каждого линейного и виртуального канала сервиса или их группы, с установкой прав доступа к трансляции указанных виртуальных каналов сервиса и линейных каналов вещания, причем одно и то же событие контента, транслируемое различными каналами, выполнено шифрованным общим управляющим словом, шифрованным разными сессионными ключами для каждого линейного и виртуального канала или их группы,

а приемная часть снабжена средствами обработки EMM и ECM сообщений для установки прав доступа к каждому событию контента, получения и расшифровки ключей дескремблирования на основе CW каждого события контента, включенных в состав каждого виртуального канала сервиса соответственно, а также средства дескремблирования на основании CW.

2. Система по п. 1, отличающаяся тем, что подсистема условного доступа (CAS) снабжена средствами шифрования контента так, что одно и то же транслируемое событие шифруется общим управляющим словом, которое в свою очередь дополнительно шифруется разными сессионными ключами для каждого линейного и виртуального канала или их группы.

3. Система по п. 2, отличающаяся тем, что подсистема условного доступа (CAS) снабжена средствами шифрования контента согласно алгоритму DVB CSA.

4. Система по п. 1, отличающаяся тем, что транспортный поток на выходе мультиплексора является MPEG-2 транспортным потоком и включает, по меньшей мере: линейные каналы вещания, контент которых используют также в составе виртуальных каналов; основные и дополнительные метаданные сервиса виртуальных каналов; Linkage дескриптор; служебные таблицы MPEG-2 транспортного потока, включающие: таблицу структуры программ (PMT); таблицу условного доступа (CAT); таблицу сетевой информации (NIT); таблицу даты и времени (TDT); таблицу групп программ (BAT).

5. Система по п. 1, отличающаяся тем, что метаданные виртуальных каналов сформированы с возможностью вещания в одном сервисе на одном транспондере и снабжены служебной информацией со ссылкой на сервис с метаданными виртуальных каналов с возможностью обнаружения в транспортном потоке сервиса с метаданными.

6. Система по п. 4, отличающаяся тем, что служебная информация снабжена Linkage дескриптором, добавленным в таблицу сетевой информации (NIT) потока с обеспечением возможности предоставления сервиса виртуальных каналов конечному пользователю без канала обратной связи пользователя.

7. Система по п. 6, отличающаяся тем, что служебная информация Linkage дескриптора включает, по меньшей мере: параметры вещания метаданных виртуальных каналов (SNT), идентификатор сервиса с метаданными виртуальных каналов и версию формата метаданных виртуальных каналов.

8. Система по п. 1, отличающаяся тем, что приемная часть включает, по меньшей мере, тюнер/демодулятор, восстанавливающий входящий шифрованный транспортный поток в модулированном мультиплексором входном сигнале и передающий его на вход криптомодуля (CAS module), снабженного установленной программно-аппаратным образом библиотекой системы условного доступа, интегрируемой в приёмное устройство (STB) для дескремблирования линейных и виртуальных каналов в соответствии с подписками, с обеспечением возможности дескремблирования входящего шифрованного транспортного потока и его передачу на вход основного процессора (CPU), выполненного с обеспечением возможности расшифровки входящего шифрованного транспортного потока, посредством встроенной системы безопасности, реализованной программно-аппаратным образом, и осуществления на основе предустановленного программно-аппаратным образом алгоритма обработки данных, предоставление конечному пользователю на аудио-видео выход контента каналов в модуле пользовательского интерфейса, при этом CPU снабжен секционным фильтром команд установки прав виртуального канала, обработчиком типа EMM сообщений, соответствующих виртуальному каналу, и возможностью отправки команды на установку прав и сессионных ключей виртуального канала сервиса.

9. Система по п. 8, отличающаяся тем, что криптомодуль сопряжен со смарт-картой (SmartCard) или снабжен встроенным эмулятором смарт-карты (SmartCard emulator), содержащими ключи и права доступа к контенту.

10. Система по любому из пп. 1-9, отличающаяся тем, что передающая часть подсистемы CAS, по меньше мере, включает средства генерирования EMM и ECM сообщений, соединенные линиями обратной связи со средством шифрования управляющих слов (CW) сессионными ключами, причем один из входов средства

генерирования ECM сообщений соединен с выходом средства генерирования EMM сообщений, а два других входа соединены по линиям обратной связи с EPG сервером и синхронизатором SCS процессов генерации CW, выход которых соединен с мультиплексором (MUX), соединенным со средством шифрования транспортного потока с ключами CW, соединенным со средством модуляции транспортного потока и его передачи на приемную часть, при этом второй вход средства генерирования EMM сообщений соединен с системой управления подписками (SMS), соединенной с биллинговой системой.

11. Способ шифрования контента и генерирования данных для дескремблирования сервиса предоставления виртуальных каналов, включающий последовательно осуществляемые этапы, на которых, по меньшей мере:

- формируют по предустановленным критериям на EPG сервере передающей стороны справочник виртуальных каналов сервиса, содержащий, по меньшей мере, название каналов и номер их позиции в списке каналов вещания и расписание событий виртуальных каналов сервиса посредством компоновки выборки событий контента линейных каналов вещания, транслируемых в рамках виртуальных каналов сервиса последовательно по времени и одновременно с соответствующей трансляцией события линейного канала, с установкой для каждого события выборки идентификатора соответствующего виртуального канала и отметки использования события в его составе, с последующим формированием метаданных каждого виртуального канала;

- получают и шифруют управляющие слова, сгенерированные посредством скремблера подсистемы условного доступа, генерируют сессионные ключи и содержащие их ECM и EMM сообщения линейных каналов вещания и виртуальных каналов системы сервиса, причем шифрование одного и того же транслируемого в составе линейного и виртуального каналов события осуществляют общим управляющим словом, дополнительно шифрованным различными сессионными ключами для каждого линейного и виртуального канала или их группы, с установкой прав доступа к трансляции указанного в расписании события линейного канала в составе виртуального канала и его остановки по окончанию события, и передают файлы метаданных сервиса виртуальных каналов на вход мультиплексора, где формируют транспортный поток встраиванием метаданных сервиса в транспортный поток контента линейных каналов вещания и передают его на вход клиентского устройства.

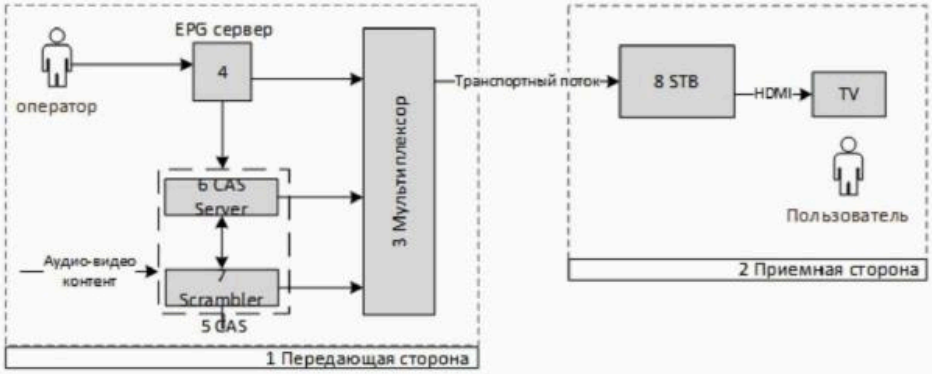
12. Способ по п. 11, отличающийся тем, что дополнительно осуществляют на передающей части CAS сервера генерирование, хранение, применение и автоматическое обновление по расписанию сессионных ключей технологических пакетов CAS, используемых для управления доступом к вещаемым событиям линейных каналов через виртуальный канал.

13. Способ по п. 11, отличающийся тем, что дополнительно осуществляют на передающей части CAS сервера генерирование EMM сообщений с командами управления доступом и сессионными ключами для технологических пакетов виртуальных каналов с обеспечением управления доступа абонентов к контенту сервиса виртуальных каналов в соответствии с данными о действующих подписках, полученными от биллинговой системы, и/или свободного доступа абонентов, имеющих авторизированное оборудование и активацию функциональности виртуальных каналов по предустановленным в системе параметрам.

14. Способ по п. 11, отличающийся тем, что при формировании MPEG-2 транспортного потока посредством мультиплексора встраивают в транспортный поток, передаваемый впоследствии на вход клиентского устройства, дополнительную служебную информацию, являющуюся Linkage дескриптором в таблице сетевой информации (NIT), обеспечивающим динамическое обнаружение клиентским устройством метаданных сервиса виртуальных каналов в транспортном потоке, и на клиентском устройстве осуществляют обнаружение сервиса с метаданными в транспортном потоке посредством упомянутого Linkage дескриптора без канала обратной связи пользователя.

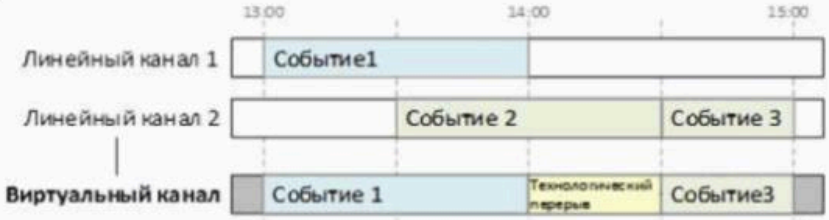
15. Способ по любому из пп. 11-14, отличающийся тем, что при генерировании расписания виртуальных каналов сервиса EPG сервером при пересечении по времени

транслируемых разными линейными каналами вещания событий выборки для виртуального канала в расписание добавляют событие с более ранним временем трансляции, а на время отсутствия отображения событий линейных каналов вещания в расписание виртуального канала добавляют предустановленное в системе сервиса технологическое событие.

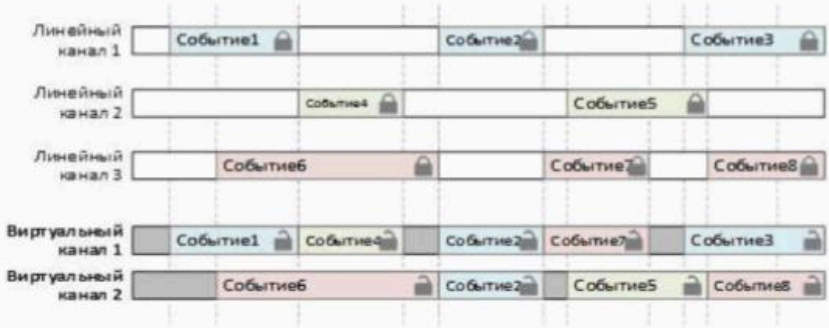

EPG сервер
4
оператор
6 CAS Server
Аудио-видео контент
7 Scrambler
5 CAS
3 Мультиплексор
Транспортный поток
8 STB
HDMI
TV
Пользователь
2 Приемная сторона
1 Передающая сторона

Фиг.1

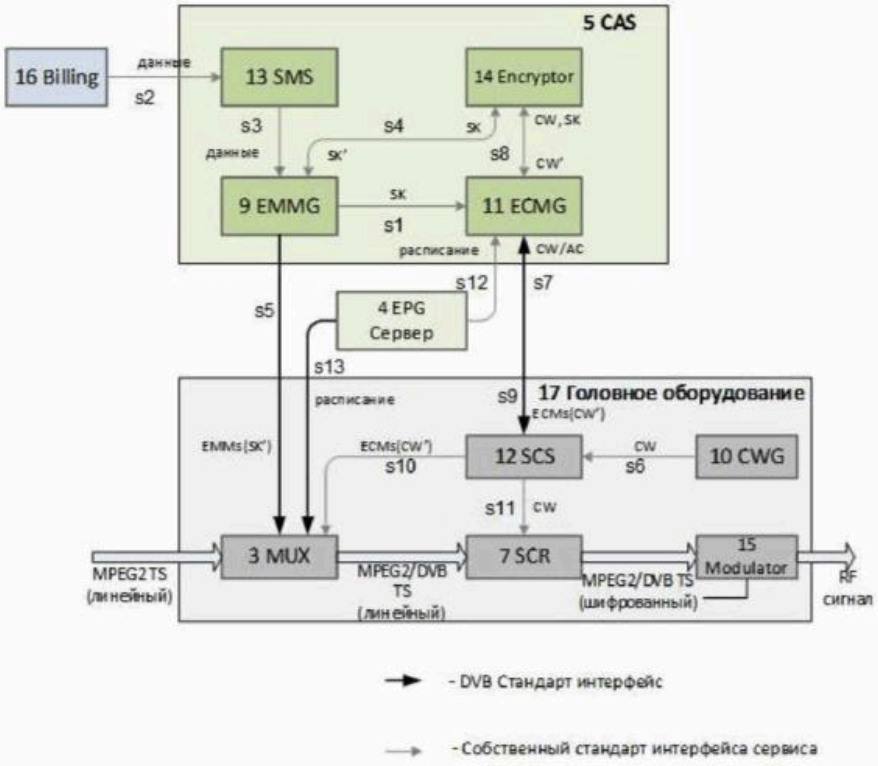
а)


13:00
14:00
15:00
Линейный канал 1
Событие1
Линейный канал 2
Событие 2
Событие 3
Виртуальный канал
Событие 1
Технологический перерыв
Событие3

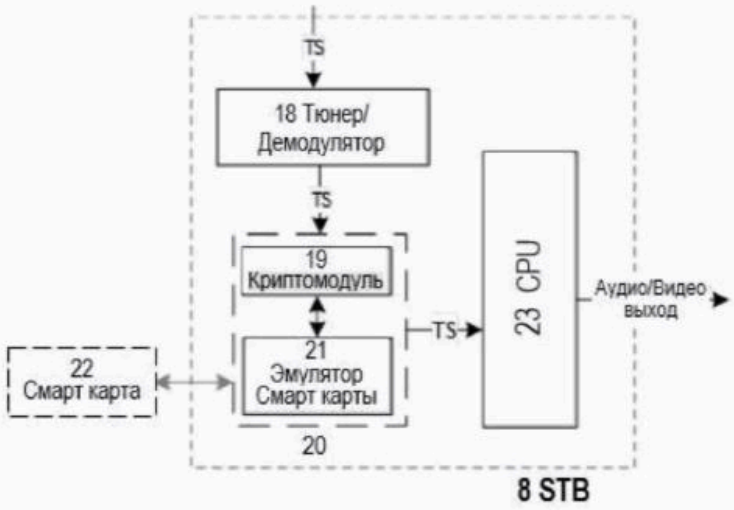
б)


Линейный канал 1
Событие1
Событие2
Событие3
Линейный канал 2
Событие4
Событие5
Линейный канал 3
Событие6
Событие7
Событие8
Виртуальный канал 1
Событие1
Событие4
Событие2
Событие7
Событие3
Виртуальный канал 2
Событие6
Событие2
Событие5
Событие8

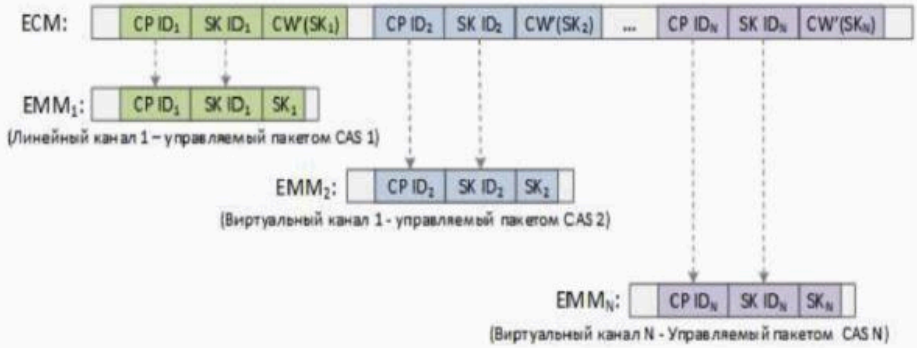
Фиг. 2


5 CAS
16 Billing
данные
s2
13 SMS
14 Encryptor
s3
данные
s4
sk
sk'
s8
CW, SK
CW'
9 EMMG
sk
s1
11 ECMG
расписание
CW/AC
s12
s7
s5
4 EPG
Сервер
s13
расписание
s9
17 Головное оборудование
ECMs(CW')
EMMs(SK')
ECMs(CW')
s10
12 SCS
CW
s6
10 CWG
s11
CW
3 MUX
7 SCR
15
Modulator
MPEG2 TS
(линейный)
MPEG2/DVB
TS
(линейный)
MPEG2/DVB TS
(шифрованный)
RF
сигнал
- DVB Стандарт интерфейс
- Собственный стандарт интерфейса сервиса

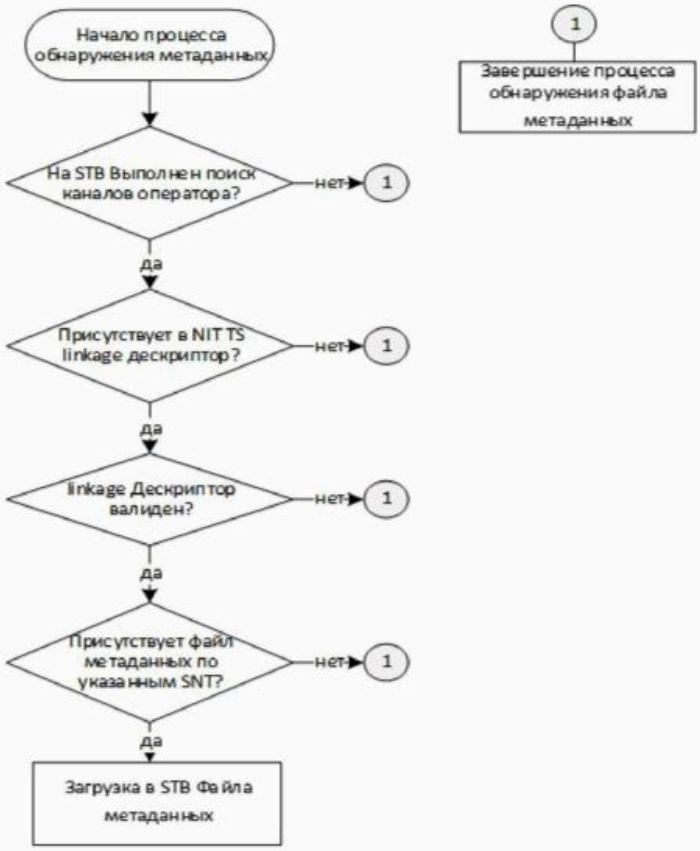
Фиг. 3


TS
18 Тюнер/
Демодулятор
TS
19
Криптомодуль
TS
21
Эмулятор
Смарт карты
20
22
Смарт карта
23 CPU
Аудио/Видео
выход
8 STB

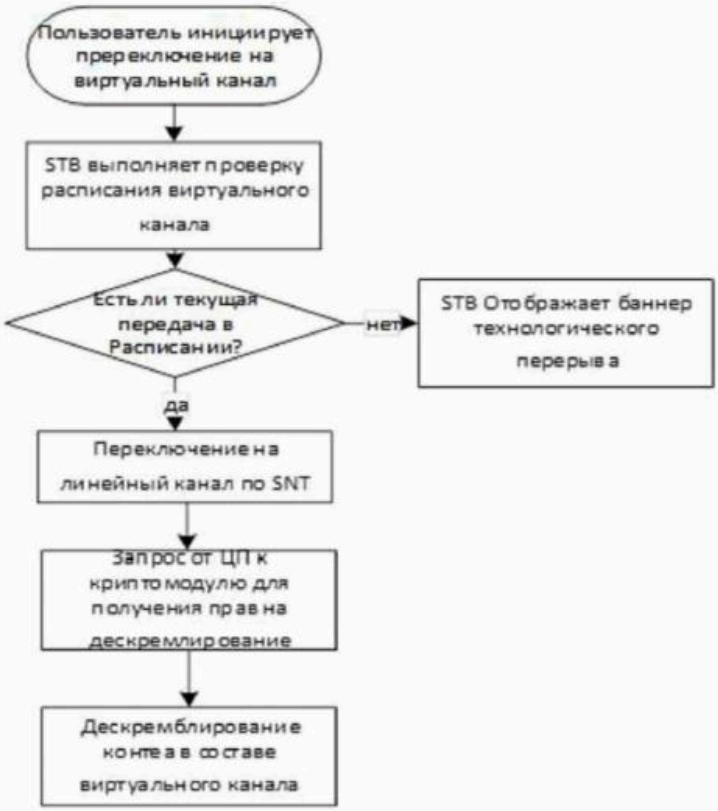
Фиг.4


ECM:
CP ID1
SK ID1
CW'(SK1)
CP ID2
SK ID2
CW'(SK2)
...
CP IDN
SK IDN
CW'(SKN)
EMM1:
CP ID1
SK ID1
SK1
(Линейный канал 1 – управляемый пакетом CAS 1)
EMM2:
CP ID2
SK ID2
SK1
(Виртуальный канал 1 - управляемый пакетом CAS 2)
EMMN:
CP IDN
SK IDN
SKN
(Виртуальный канал N - Управляемый пакетом CAS N)

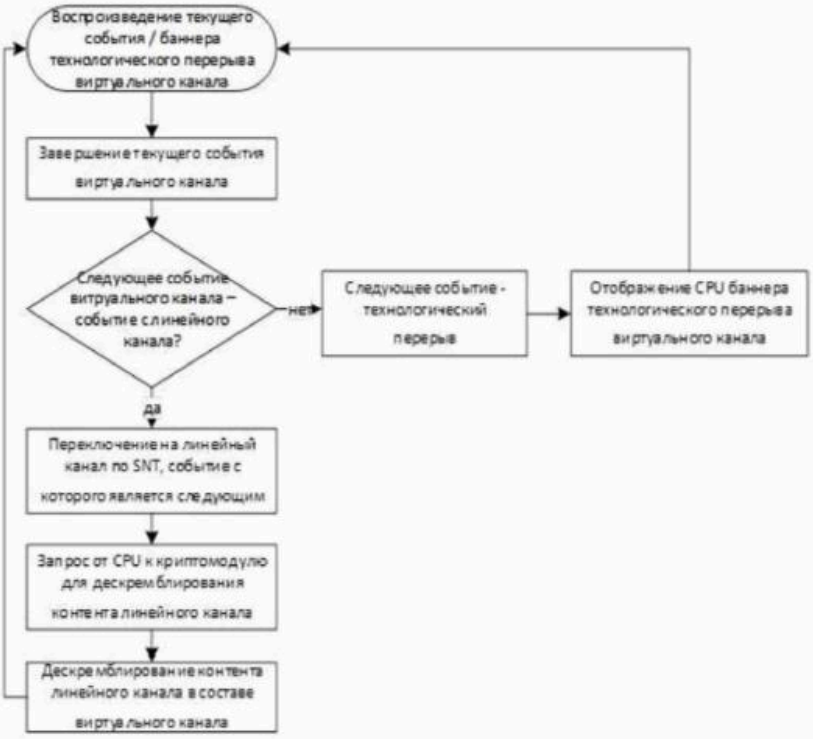
Фиг. 5


Начало процесса обнаружения метаданных
На STB Выполнен поиск каналов оператора?
нет
1
да
Присутствует в NIT TS linkage дескриптор?
нет
1
да
linkage Дескриптор валиден?
нет
1
да
Присутствует файл метаданных по указанным SNT?
нет
1
да
Загрузка в STB Файла метаданных
1
Завершение процесса обнаружения файла метаданных

Фиг. 6


Пользователь инициирует переключение на виртуальный канал
STB выполняет проверку расписания виртуального канала
Есть ли текущая передача в Расписании?
нет
STB Отображает баннер технологического перерыва
да
Переключение на линейный канал по SNT
Запрос от ЦП к криптомодулю для получения прав на дескремлирование
Дескремблирование контента в составе виртуального канала

Фиг. 7


Воспроизведение текущего события / баннера технологического перерыва виртуального канала
Завершение текущего события виртуального канала
Следующее событие витруального канала – событие с линейного канала?
нет
Следующее событие - технологический перерыв
Отображение CPU баннера технологического перерыва виртуального канала
да
Переключение на линейный канал по SNT, событие с которого является следующим
Запрос от CPU к криптомодулю для дескремблирования контента линейного канала
Дескремблирование контента линейного канала в составе виртуального канала

Фиг. 8