



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: 2004119436/09, 14.11.2002

(24) Дата начала отсчета срока действия патента:
14.11.2002(30) Конвенционный приоритет:
27.11.2001 ЕР 01204668.6

(43) Дата публикации заявки: 10.11.2005

(45) Опубликовано: 10.08.2007 Бюл. № 22

(56) Список документов, цитированных в отчете о поиске: WO 0186393 A, 15.11.2001. RU 2160965 C2, 20.12.2000. RU 2160924 C1, 20.12.2000. US 6125118 A, 26.09.2000.

(85) Дата перевода заявки РСТ на национальную фазу:
28.06.2004(86) Заявка РСТ:
IB 02/04803 (14.11.2002)(87) Публикация РСТ:
WO 03/047204 (05.06.2003)Адрес для переписки:
129010, Москва, ул. Б. Спасская, 25, стр.3,
ООО "Юридическая фирма Городисский и
Партнеры", пат.пов. Ю.Д.Кузнецовой, рег.№ 595

(72) Автор(ы):

ВАН ДЕН ХЕФЕЛ Себастиан А.Ф.А. (NL),
ЛЕНУАР Петрус Й. (NL),
КАМПЕРМАН Франсискус Л.А.Й. (NL)

(73) Патентообладатель(и):

КОНИКЛЕЙКЕ ФИЛИПС ЭЛЕКТРОНИКС Н.В.
(NL)

RU 2304354 C2

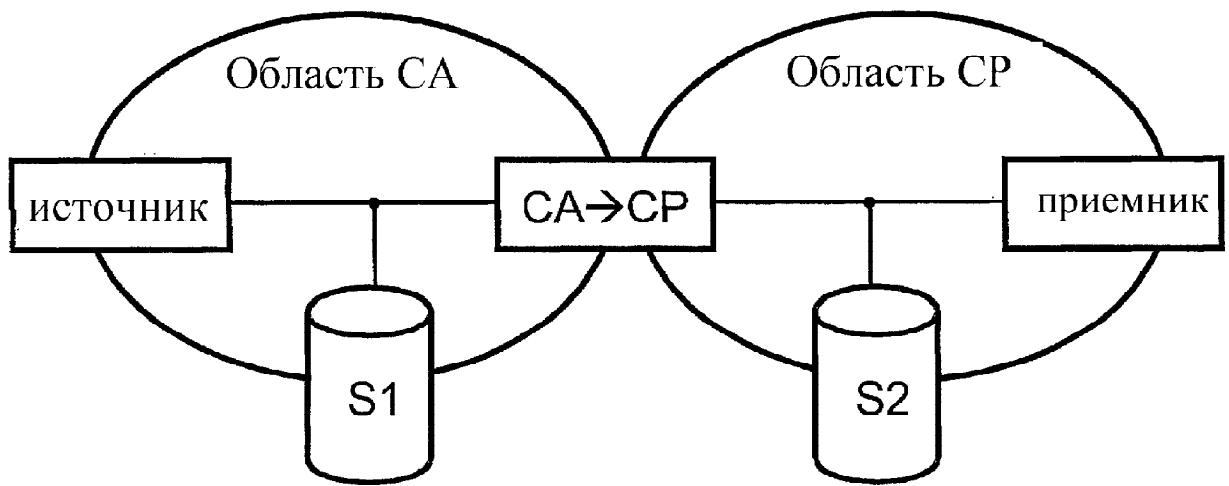
RU 2304354 C2

(54) СИСТЕМА УСЛОВНОГО ДОСТУПА

(57) Реферат:

Изобретение относится к цифровой, например домашней сети, которая может включать в себя ряд устройств, например радиоприемник, тюнер/декодер, проигрыватель компакт-дисков, пару громкоговорителей, телевизор, видеомагнитофон и т.д. Система условного доступа содержит множество таких устройств, связанных между собой в сеть, при этом эти устройства сгруппированы в первую группу и во вторую группу. Устройства первой группы работают в соответствии с первой инфраструктурой безопасности, а устройства второй группы работают в соответствии со второй инфраструктурой безопасности. Каждое устройство

работает с использованием конкретного слоя связующего программного обеспечения, при этом упомянутый слой связующего программного обеспечения сконфигурирован для аутентификации другого слоя связующего программного обеспечения другого устройства, причем аутентификацию упомянутого слоя связующего программного обеспечения выполняет инфраструктура безопасности, в соответствии с которой работает устройство. Техническим результатом является обеспечение передачи контента через систему при поддержании сквозного управления и без большого усложнения. 2 н. и 8 з.п. ф-лы. 6 ил.



ФИГ.1

R U 2 3 0 4 3 5 4 C 2

R U 2 3 0 4 3 5 4 C 2



(51) Int. Cl.
H04L 12/28 (2006.01)
H04L 29/06 (2006.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: 2004119436/09, 14.11.2002

(24) Effective date for property rights: 14.11.2002

(30) Priority:
27.11.2001 EP 01204668.6

(43) Application published: 10.11.2005

(45) Date of publication: 10.08.2007 Bull. 22

(85) Commencement of national phase: 28.06.2004

(86) PCT application:
IB 02/04803 (14.11.2002)

(87) PCT publication:
WO 03/047204 (05.06.2003)

Mail address:

129010, Moskva, ul. B. Spasskaja, 25, str.3,
ООО "Juridicheskaja firma Gorodisskij i
Partnery", pat.pov. Ju.D.Kuznetsov, reg.№ 595

(72) Inventor(s):

VAN DEN KhEFEL Sebastian A.F.A. (NL),
LENUAR Petrus J. (NL),
KAMPERMAN Fransiskus L.A.J. (NL)

(73) Proprietor(s):

KONINKLEJKE FILIPS EhLEKTRONIKS N.V. (NL)

C 2

C 4

5 4

3 5

2 3

0 4

R U

R U
2 3 0 4 3 5 4

C 2

(54) CONDITIONAL ACCESS SYSTEM

(57) Abstract:

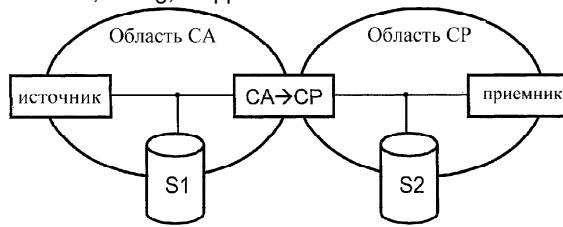
FIELD: digital networks such as domestic one that has radio receiver, tuner/decoder, compact-disk recorder, pair of loudspeakers, videorecorder, and the like.

SUBSTANCE: proposed conditional access system has plurality of devices intercoupled to form network and assembled in first and second groups. Devices of first-group operate in compliance with first safety infrastructure and those of second group, in compliance with second safety infrastructure. Each device uses in operation definite layer of linkage software; mentioned linkage software layer is configured for authenticating other layer of other-device

linkage software; mentioned linkage software layer is authenticated by safety infrastructure controlling device operation.

EFFECT: facilitated transfer of content through system to maintain throughput control.

10 cl, 6 dwg, 5 app



ФИГ.1

Область техники, к которой относится изобретение

Типичная цифровая домашняя сеть включает в себя ряд устройств, например радиоприемник, тюнер/декодер, проигрыватель компакт-дисков (CD-плеер), пару громкоговорителей, телевизор, видеомагнитофон, деку и т.д. Эти устройства обычно соединены между собой, чтобы позволить одному устройству, например телевизору, управлять другим, например видеомагнитофоном. Одно устройство, такое как, например, тюнер/декодер или телевизионная приставка, является обычно центральным устройством, обеспечивающим центральное управление другими устройствами. Кнопки и переключатели управления обычно располагаются на передней части тюнера, а также на переносном устройстве дистанционного управления. Пользователь может управлять всеми устройствами посредством центрального устройства или устройства дистанционного управления.

Так как эти устройства становятся более универсальными и более сложными, простое ручное управление не является достаточным. Более того, так как все более и более

устройств становятся доступными, возможность к взаимодействию становится проблематичной. Многие поставщики используют свои собственные протоколы связи, чтобы позволить их устройствам взаимодействовать, но при этом устройства от различных поставщиков не взаимодействуют. Для преодоления этих проблем определены несколько стандартов взаимодействия, которые позволяют различным устройствам обмениваться сообщениями и информацией и управлять друг другом. Одним из общеизвестных стандартов является стандарт Home Audio/Video Interoperability (HAVi) (стандарт на взаимодействие бытовой аудио/видео аппаратуры), версия 1.0 которого опубликована в январе 2000, и который доступен в сети Интернет по адресу <http://www.havi.org/>. Другими общеизвестными стандартами являются стандарт domestic digital bus (D2B) (стандарт на домашнюю цифровую шину), протокол связи, описанный в IEC 1030, и стандарт Universal Plug and Play (универсальный стандарт на распознавание и настройку устройств без последующего конфигурирования пользователем) (<http://www.upnp.org/>).

В системе, согласно такому стандарту, устройства соединены между собой в сеть с помощью стандартной шины, например последовательной коммуникационной шины IEEE 1394, и обмениваются информацией, такой как сообщения, данные и команды, через эту сеть согласно этому стандарту. Стандарты, такие как HAVi, определяют протокол для такого обмена, позволяя взаимодействовать устройствам от различных поставщиков. Пользователи могут добавить новые устройства в сеть, и они незамедлительно становятся доступными для других устройств. Протокол для «обнаружения» такого нового устройства также стандартизован.

Некоторые устройства в домашней цифровой сети (IHDN) могут иметь внешнее соединение. С помощью этого соединения контент (информационно значимое содержимое) может поступать в сеть, используя широкополосную передачу или загрузку из сети Интернет. Контент может также поступать в сеть путем считывания его с носителя данных, такого как Цифровой Универсальный Диск (DVD) или жесткий диск.

Задача, на которую направлено решение, представленное в этом документе, состоит в том, как реализовать передачу контента через такую систему, при поддержании сквозного управления и без большого усложнения.

Сущность изобретения

Согласно аспекту изобретения обеспечивается система условного доступа, содержащая множество устройств, соединенных между собой в сеть, при этом устройства сгруппированы в первую группу и во вторую группу, устройства первой группы работают в соответствии с первой инфраструктурой безопасности, а устройства второй группы работают в соответствии со второй инфраструктурой безопасности, причем каждое устройство работает с использованием конкретного слоя связующего программного обеспечения, при этом упомянутый слой связующего программного обеспечения сконфигурирован для аутентификации (установления подлинности) другого слоя связующего программного обеспечения другого устройства, и аутентификация упомянутого

слоя связующего программного обеспечения выполняется инфраструктурой безопасности, в соответствии с которой работает устройство.

Все устройства в сети реализуют инфраструктуру безопасности. Используя эту инфраструктуру, эти устройства могут выполнять аутентификацию в отношении друг

- 5 друга и безопасным образом распространять контент, а управление доступом к контенту выполняется системой безопасности. Это предохраняет незащищенный контент от «бегства» в неавторизованные (неуполномоченные) устройства. Для того, чтобы это работало, устройства должны быть способны доверять слоям связующего программного обеспечения друг друга и собственному слою связующего программного обеспечения, а
- 10 также и инфраструктуре безопасности других устройств. Изобретение предотвращает то, что инфраструктура безопасности должна выполнять аутентификацию каждого слоя связующего программного обеспечения в системе и должна поддерживать все виды специфических особенностей связующего программного обеспечения для всех различных слоев связующего программного обеспечения.

- 15 В варианте выполнения устройство из первой группы может выполнять функцию второй инфраструктуры безопасности, выполняя вызов удаленной процедуры (RPC) для слоя связующего программного обеспечения устройства из второй группы. Этот вариант выполнения позволяет инфраструктурам безопасности обнаруживать друг друга и осуществлять связь, и является независимым от связующего программного обеспечения
- 20 домашней сети (HN-MW) и сетевой технологии.

В еще одном варианте выполнения RPC передается к устройству из второй группы через защищенный аутентифицированный канал (SAC). Это позволяет инфраструктурам безопасности, которые намереваются сообщаться друг с другом, выполнять это безопасным образом. Когда несколько устройств безопасности присутствуют в сети, набор

- 25 каналов SAC между ними может рассматриваться как виртуальная частная сеть (VPN).

В еще одном варианте выполнения устройствам выдается разрешение на доступ к контенту в соответствии с конкретным классом целей, причем определен набор таких классов, и каждый класс содержит ряд операций или целей условного доступа. Связующее программное обеспечение рассматривает контент в отношении этого доступа к контенту в

- 30 рамках упомянутого класса.

Предпочтительно первый класс из упомянутого набора включает в себя операции ВОСПРОИЗВЕСТИ (RENDER), ПЕРЕМЕСТИТЬ (MOVE) и КОПИРОВАТЬ (COPY). Далее предпочтительно, второй класс из упомянутого набора включает в себя операции СОХРАНИТЬ (STORE), ВОСПРОИЗВЕСТИ (RENDER), РЕДАКТИРОВАТЬ (EDIT), УДАЛИТЬ (DELETE) и ОБРАБОТАТЬ (PROCESS). В другом варианте выполнения операция ОБРАБОТАТЬ предпочтительно санкционируется независимо от любых ограничений на права, связанные с контентом. Операция "обработать" позволяет совместимым устройствам в сети выполнять доступ к защищенному контенту для выполнения операций, которые не изменяют права на этот контент, без изменения этих прав. Примерами таких

- 40 операций являются транскодирование контента и битовой скорости, обработка, требуемая для поддержания спецэффектов, улучшение изображения.

Согласно второму аспекту изобретения обеспечивается способ, позволяющий устройству выполнять условный доступ к части контента, при этом устройству выдано разрешение на доступ к контенту в соответствии с конкретным классом целей, причем определен набор таких классов, и каждый класс включает в себя ряд операций или целей условного доступа.

В варианте выполнения первый класс из набора включает в себя операции СОХРАНИТЬ, ВОСПРОИЗВЕСТИ, РЕДАКТИРОВАТЬ, УДАЛИТЬ и ОБРАБОТАТЬ. В другом варианте выполнения операцию ОБРАБОТАТЬ санкционируют независимо от любых

- 50 ограничений на права, связанные с контентом.

Перечень фигур чертежей

Эти и другие аспекты изобретения будут очевидны и пояснены со ссылками на иллюстративные варианты выполнения, показанные на чертежах, на которых:

Фиг.1 - схематическая иллюстрация предпочтительной схемы домашней цифровой сети в соответствии с изобретением, содержащей источник, приемник и два носителя данных.

Фиг.2 - иллюстрация базовой структуры предпочтительной инфраструктуры безопасности для управления правами и их защиты (RMP).

5 Фиг.3 - описание сообщения, отправленного от одной инфраструктуры безопасности к другой.

Фиг.4 - иллюстрация того, как выполняются вызовы с помощью вызовов RPC на открытом интерфейсе виртуальных машин OPIMA.

Фиг.5 - иллюстрация того, как реализуется распределенный доступ к контенту.

10 Фиг.6 - иллюстрация того, как предпочтительно осуществляется управление вызовами RPC.

На всех чертежах одинаковые ссылочные позиции указывают сходные или соответствующие признаки. Некоторые из признаков, указанных на чертежах, обычно воплощаются в программном обеспечении, и как таковые представляют объекты

15 программного обеспечения, такие как программные модули и объекты.

Архитектура домашней сети

Фиг.1 схематически иллюстрирует предпочтительную схему домашней цифровой сети в соответствии с изобретением, содержащую источник, приемник и два носителя S1 и S2 данных. Сеть делится концептуально на область условного доступа (СА) и область защиты

20 от копирования (СР).

Большая часть контента, который обычно содержит, например, музыку, песни, фильмы, ТВ программы, изображения и т.д. входит в состав домашней сети в области СА. Источник может быть соединением с широкополосной кабельной сетью, Интернет-соединением, спутниковой нисходящей линией связи и т.д. Контент, принятый таким образом, может

25 быть сохранен в носителе S1 данных, так что он может быть считан и воспроизведен позднее на приемнике. Носителем S1 данных может быть персональное цифровое устройство записи (PDR) некоторого вида, например, устройство записи на перезаписываемые универсальные цифровые диски формата DVD+RW. Источник может также быть DVD-плеером, в который вставляется DVD-диск, так что контент может быть

30 считан с диска.

Точный способ, которым воспроизводится элемент контента, обусловлен типом приемника и типом контента. Например, в радиоприемнике воспроизведение включает в себя генерирование аудиосигналов и подачу их на громкоговорители. Для телевизионного приемника воспроизведение включает в себя генерирование аудио и видеосигналов и подачу их на экран дисплея и громкоговорители. Для других типов контента должно быть сделано подобное соответствующее действие. Воспроизведение может также включать в себя такие операции, как дешифрование или декремблирование принимаемого сигнала, синхронизацию аудио и видеосигналов и т.д.

40 Приемник может быть, например, телевизионной системой или устройством аудиовоспроизведения. Как правило, приемник располагается в области СР. Это гарантирует, что когда контент подается на приемник, нельзя сделать несанкционированные копии этого контента, потому что в области СР расположена схема защиты от копирования. Область СР содержит носитель S2 информации, на котором (временные) копии контента могут храниться в соответствии с правилами защиты от

45 копирования.

Все устройства во внутренней сети, которые реализуют инфраструктуру безопасности, делают это в соответствии с требованиями, предъявляемыми к конкретному варианту реализации. Используя эту инфраструктуру, эти устройства могут выполнять аутентификацию друг друга и распространять контент безопасным образом, а управление 50 доступом к контенту выполняется системой безопасности. Это предохраняет незащищенный контент от «бегства» в неавторизованные устройства.

Инфраструктура безопасности

Базовую структуру предпочтительной инфраструктуры безопасности для управления

правами и их защиты (RPM) иллюстрирует фиг.2. Эта инфраструктура безопасности определена в Призывае к Содействию (CFC) в рамках стандарта TV Anytime (TVA, «ТВ в любое время»), смотри web-сайт TV Anytime на <http://www.tv-anytime.org/cfcs/>. На фиг.2 описаны следующие элементы.

- 5 - Интерфейс Прикладного Программирования (API) приложений: Разрешает приложениям связываться с системой RMP способом, обеспечивающим возможность взаимодействия.
 - Приложение: Программы и/или службы, разрешающие пользователю доступ к контенту и Функциональным возможностям PDR в соответствии с условиями RMP.
 - 10 - Базовая система RMP: Функциональные возможности, согласующиеся с базовой спецификацией RMP TV Anytime (TVA).
 - Частные системы RMP: Частные системы защиты контента, непосредственно взаимодействующие с базовой системой RMP TVA через API служб RMP.
 - Менеджер (средство управления) информации RMP: Принимает решение о том, какие виды действий разрешены для контента, например проигрывание, копирование, перемещение и т.д., и может передавать криптографические ключи инструментальным средствам безопасности.
 - API служб RMP: Разрешает системе RMP осуществлять связь с базовыми функциями безопасности RMP способом, обеспечивающим возможность взаимодействия.
 - 15 20 - Функциональный слой системы RMP: Набор функций, реализующих Базовую систему.
 - Менеджер системы RMP: Управляет работой базовой системы.
 - Инструментальные средства Безопасности, возможно, содержат: средство дескремблирования, средство обнаружения/встраивания водяных знаков, средство проверки подлинности подписи и т.д.
 - 25 - Стандартизованные усовершенствования для базовой системы RMP TVA: необязательные стандартизованные TVA-расширения для базовой системы RMP TVA.
 - Интерфейс базового устройства RMP TVAF (инфраструктуры TVA): Слой безопасной связи между устройствами, совместимыми с TVA.

Этот документ обеспечивает решение для следующих элементов системы:
 - 30 - API приложений
 - API служб RMP
 - Связь между устройствами.

API приложений

Стандартизованный API необходим, когда должно быть разработано программное обеспечение от третьей стороны. Таким образом, стандартизованный API приложений требуется только на платформах с этим требованием. Примерами таких платформ являются платформы, которые поддерживают загружаемые приложения. Только на таких устройствах требуется API приложений.
 - 35 40 - В качестве API приложений предлагается API DAVIC CA, разработанный Советом по Цифровой и Визуальной Информации (DAVIC (DIGITAL Audio-Visual Council), 1998, спецификации DAVIC 1.4, <http://www.davic.org/>). API DAVIC CA охватывает большую часть функциональных возможностей, требуемых для использования защищенного контента из приложения. Тем не менее, по всей видимости, потребуются некоторые расширения для решения некоторых вопросов, относящихся к хранению данных или сетям.
 - 45 - API служб RMP
 - 50 - API служб RMP разрешает системе RMP осуществлять связь с функциями безопасности базовой системы RMP способом, обеспечивающим возможность взаимодействия. API служб RMP должен состоять из поднабора методов стандарта OPIMA (инициатива в рамках открытой платформы для доступа к мультимедиа), как дано в этом разделе. В последующих разделах методы OPIMA для API RMP сгруппированы согласно функциональным возможностям. В отношении OPIMA, см. спецификацию OPIMA версии 1.1, 2000, включенную в настоящее описание посредством ссылки. <http://www.cselt.it/opima/>.
- Доступ к контенту

Эта часть отражает определение интерфейса «Абстрактный доступ к контенту», раздел 3.3.4.7 стандарта OPIMA. Через этот интерфейс приложение может показывать требуемое действие в отношении контента.

В соответствии с OPIMA система RMP имеет слабый контроль над приостановкой

- 5 действий в отношении контента, когда RMP решает, что доступ к контенту больше не разрешен (например, потому, что правило, относящееся к контенту, изменяет права доступа). Единственный механизм, который доступен для системы RMP, состоит в посылке неправильного ключа дешифрования виртуальной машине OPIMA (OVM). То, приведет ли это действие к крушению системы, зависит от реализации OVM. Для более изящного
- 10 прекращения доступа к контенту требуется дополнительный метод.

Следующие методы используются для доступа к контенту:

- installCallbackContentAccess
- AbstractContentAccess
- replyToContentAccess

- 15 В необязательном порядке можно использовать следующий дополнительный метод:

- stopContent(ContentId)

Доступ к правилам/ключам

Эта часть отражает определение интерфейса для интерфейса «Абстрактный Доступ к Содержимому», раздел 3.3.4.8 стандарта OPIMA. Через этот интерфейс приложение может

- 20 показывать, какие данные о правилах/правах оно желает принять.

Следующие методы используются для взаимодействия с пользователем:

- obtainUserRules
- obtainContentRules
- newRules

- 25 - updateContentRules

В необязательном порядке опционально можно использовать следующий дополнительный метод:

- addContentRules

Интеллектуальные карты (смарткарты)

- 30 Эта часть отражает определение интерфейса для интерфейса «Интеллектуальные карты», раздел 3.3.4.6 стандарта OPIMA. Система RMP может осуществлять доступ к интеллектуальным картам через эту систему и модули данных протокола прикладного уровня (APDU) стандарта ISO 7816 на передачу/прием.

Следующие методы должны быть использованы для взаимодействия с

- 35 интеллектуальными картами:

- addCTListener
- removeCTListener
- cardInserted
- cardRemoved
- 40 - getSlotId
- isCardPresent
- openSlotChannel
- closeSlotChannel
- getATR
- 45 - reset
- sendAPDU

Шифрование/Дешифрирование

Эта часть отражает определение интерфейса для интерфейса «Средства шифрования и дешифрирования», раздел 3.3.4.3 стандарта OPIMA. Система RMP может управлять через

- 50 этот интерфейс как криптографией контента, так и криптографическими действиями в отношении смешанной информации.

Следующие методы используются для шифрования и дешифрирования:

- queryEncryptionAlgorithms

- encrypt
- initEncryption
- updateEncryptionKeys
- stopEncryption
- 5 - decrypt
- initDecryption
- updateDecryptionKeys
- stopDecryption

Подписи

10 Эта часть отражает определение интерфейса для интерфейса «Средства для Подписей», раздел 3.3.4.4 стандарта OPIMA. Через этот интерфейс система RMP может проверять и генерировать как подписи для контента, так и подписи для смешанной информации.

Следующие методы используются для подписей:

- 15 - querySignatureAlgorithms
- verifySignature
- verifyContentSignature
- generateSignature
- generateContentSignature

Водяные знаки

20 Эта часть отражает определение интерфейса для интерфейса «Средство для Водяных Знаков», раздел 3.3.4.5 стандарта OPIMA. Через этот интерфейс система RMP может обнаруживать и встраивать водяные знаки в контент.

Следующие методы используются для водяных знаков:

- 25 - queryWatermarkAlgorithms
- extractWatermark
- stopWatermarkExtraction
- insertWatermark
- stopWatermarkInsertion

Доступ к RMP

30 Эта часть отражает определение интерфейса для интерфейса «Абстрактный Доступ к Одноранговым элементам OPIMA», раздел 3.3.4.9 стандарта OPIMA. Через этот интерфейс базовые системы могут взаимодействовать друг с другом.

Следующие методы используются для взаимодействия между системами RMP:

- 35 - openConnection
- closeConnection
- addConnectionListener
- sendMessage
- newConnection
- receiveMessageFromPeer

Взаимодействие с пользователем

40 Эта часть отражает определение интерфейса для интерфейса «Взаимодействие с пользователем», раздел 3.3.4.1 стандарта OPIMA. Через этот интерфейс пользователь может обмениваться информацией с системой RMP.

45 Следующие методы используются для взаимодействия с пользователем:

- sendMessageToUser
- receiveMessageFromUser

Метод receiveMessageFromUser разрешает лишь перенос строк символов между системой RMP и пользователем. Система RMP не контролирует форматирование и

50 представление информации. Для поддержки такого форматирования в методе receiveMessageFromUser, значение(я) MessageText должно(ы) соответствовать сообщениям высокого уровня интерфейса взаимодействия человека с аппаратурой (MMI), соответствующего Общему Интерфейсу, как стандартизовано в CENELEC EN 50221: 1997,

Common Interface for Conditional Access and other Digital Video Decoder Applications; и в CENELEC R 206-001: 1997, Guidelines for the Implementation and Use of the Common Interface for DVB 15 Decoder Applications.

Взаимодействие с приложениями

- 5 Эта часть отражает определение интерфейса «Абстрактный Доступ к Приложениям», раздел 3.3.4.10 стандарта OPIMA. Этот интерфейс определяет прозрачный битовый канал между приложением и системой RMP.

В инфраструктуре DVB (цифрового видеовещания) может быть представлено множество приложений и множество систем RMP. Таким образом, этот интерфейс 10 будет усовершенствован с помощью некоторых специальных методов для обеспечения взаимодействия между приложениями и системами RMP в отношении некоторых базовых функциональных возможностей.

Следующие методы должны быть использованы для взаимодействия с приложениями:

- installCallbackApplication
- 15 - replyMessage
- receiveMessageFromApplication

Нижеследующее расширение является необязательным.

Метод receiveMessageFromApplication должен содержать дополнительный тип сообщения (Message Type) «QUERY ENTITLEMENT». В ответ на этот тип сообщения 20 система RMP возвращает список доступных вариантов доступа для текущего пользователя через стандартный метод «replyMessage».

Управление жизненным циклом

Эта часть отражает определение интерфейса для интерфейса «Управление жизненным циклом», раздел 3.3.4.11 стандарта OPIMA.

- 25 Следующие методы используются для управления жизненным циклом:

- initialize
- terminate
- update
- remove

Базовый Интерфейс Устройства RMP TVAF

Интерфейс Устройства должен обеспечивать безопасный уровень связи между устройствами, совместимыми с TVA. Элементы, относящиеся к этому интерфейсу, включают взаимосвязь инфраструктуры безопасности с другими элементами системы, такими как сетевое связующее программное обеспечение (например, UPnP, NAVi и Jini).

35 Более того, аутентификация совместимых устройств и безопасная связь между этими устройствами обеспечивается Базовым Интерфейсом Устройства. Интерфейс устройства определен как расширение OPIMA для домашних сетей.

Базовая Система RMP

Базовая Система RMP обеспечивает систему TVA стандартизированной копией системы 40 защиты. Так как она стандартизована и обязательна в каждом устройстве, реализующем упомянутую инфраструктуру, любое устройство, реализующее Базовую Систему RMP, может осуществлять доступ к контенту, защищенному этой Системой RMP. Далее, очень важно, что базовая система проста для реализации. Это особенно важно, так как базовая система должна также поддерживаться компактными недорогими мобильными 45 устройствами.

Базовая Система RMP, как и любая Система RMP, состоит из двух частей: управление ключами и шифрование контента. Использование системы, описанной в следующем разделе, позволяет частной системе RMP, которая использует базовую схему шифрования контента, осуществлять сквозное управление. Хотя Базовая система RMP не предложена, 50 любая предлагаемая система RMP должна быть совместима с API служб RMP, соответствующим OPIMA.

Простая базовая система должна поддерживать по меньшей мере следующие правила, относящиеся к контенту: copy free (свободное копирование), copy_one_generation

- (копировать одно поколение), copy_no_more (больше не копировать). Поскольку эта Базовая система RMP будет присутствовать в каждом совместимом устройстве, алгоритм шифрования контента должен быть дешев, легко доступен и надежен. Так как Усовершенствованный Стандарт Шифрования (AES) удовлетворяет всем этим
- 5 требованиям, предпочтительно использовать AES в качестве базовой схемы шифрования контента.

Базовый Интерфейс устройства

- В предыдущем разделе была введена система OPIMA. OPIMA обеспечивает инфраструктуру безопасности для приложений и систем Цифрового Управления Правами (DRM) для взаимодействия между собой. В этом разделе система OPIMA усовершенствована для работы в домашней сети. Для введения в использование DRM в домашних сетях см. F.L.A.J. Kamperman, S.A.F.A. van den Heuvel, M.H. Verberkt, Digital Rights Management in Home Networks, Philips Research, The Netheklands, IBC 2001 conference publication vol. I, стр.70-77.

- 15 Домашняя сеть может быть определена как набор устройств, которые соединены между собой с помощью некоторого вида сетевой технологии (например, Ethernet, IEEE 1394, BlueTooth, 802.11b, и т.п.). Хотя сетевая технология позволяет сообщаться различным устройствам, этого недостаточно, чтобы разрешить устройствам взаимодействовать. Чтобы быть способными к взаимодействию, устройствам необходимо обнаруживать функции, 20 присутствующие в других устройствах в сети, и обращаться к ним. Такое взаимодействие обеспечивается связующим программным обеспечением домашней сети (HN-MW). Например связующим программным обеспечением домашней сети являются Jini, HAVi, UPnP, AVC.

- Использование сетевой технологии и HN-MW заменяет набор отдельных устройств на 25 одно большое виртуальное устройство. С точки зрения HN-MW, сеть может рассматриваться, как набор функций, которые можно использовать и соединять. Такая система обеспечивает пользователя возможностями обращаться к любому контенту или услуге из любой точки домашней сети.

- HN-MW может быть определено как система, которая обеспечивает две услуги. Оно 30 позволяет приложению в сети находить устройства и функции в сети. Более того, некоторый механизм вызова удаленных процедур (RPC) определяет, как использовать эти функции. С точки зрения HN-MW, системы, относящиеся к обработке безопасного контента, реализуются несколькими путями. Определенные функции в сети требуют доступа к защищенному контенту. Другие функции в сети обеспечивают функциональные 35 возможности, которые могут быть использованы элементами в сети, обрабатывающими безопасность контента. Более того, инфраструктуры безопасности, такие как OPIMA, могут использовать HN-MW для нахождения друг друга и осуществления связи способом, обеспечивающим возможность взаимодействия.

Инфраструктуры безопасности и домашние сети

- 40 Этот подраздел обсуждает этот последний вариант: как использовать связующее программное обеспечение домашней сети инфраструктурами безопасности для нахождения друг друга и осуществления связи между собой. В этом случае инфраструктура безопасности может быть представлена как функция в домашней сети. Это позволяет функциям безопасности находить другие функции безопасности в сети и обращаться к ним.

- 45 Используя этот подход, можно находить другие инфраструктуры безопасности и использовать их функциональные возможности. Этого достаточно для обычных приложений. В случае, когда приложения обращаются к защищенному контенту, требуется, чтобы этот контент оставался защищенным, и секреты, которые защищают контент, не могли быть перехвачены. Более того, требуется подтверждение того, что другим 50 устройствам безопасности можно доверять.

Такие функциональные возможности предпочтительно обеспечиваются защищенным аутентифицированным каналом (SAC). Когда SAC создан, обе стороны выполняют аутентификацию друг друга и создают защищенный канал шифрованных сообщений. Это

позволяет инфраструктурам безопасности, которые намереваются осуществлять связь друг с другом, выполнять это безопасным способом. Когда несколько устройств безопасности присутствуют в сети, набор каналов SAC между ними может рассматриваться как виртуальная частная сеть (VPN).

5 В такой VPN, опять-таки, устройства и функции необходимо находить и обращаться к ним. Поэтому для работы в VPN необходимо связующее программное обеспечение домашней сети (HN-MW). Поскольку подобные функциональные возможности уже присутствуют в системе (HN-MW, используемое для нахождения устройства безопасности), они могут быть повторно использованы в рамках VPN.

10 Для выполнения этого, инфраструктура безопасности должна иметь возможность посылать и принимать сообщения и реализовать способ, который позволяет посыпать ей сообщения, используя методики HN-MW (см. Приложение Д).

15 Для пояснения этого более подробно фиг.3 описывает сообщение, посланное от одной инфраструктуры безопасности к другой. На этом чертеже серые блоки слева показывают заголовок сообщения, а белые блоки показывают тело сообщения. Сетевое сообщение содержит сообщение HN-MW, которое является вызовом удаленных процедур (RPC) в отношении функции безопасности.

20 Данные вызова удаленных процедур являются телом сообщения, подлежащего обработке SAC. Хотя SAC может быть определен для каждого стандарта HN-MW, предлагается использовать один SAC, предпочтительно SSL (протокол защищенных сокетов) (RFC 2246) для всех стандартов HN-MW. Элемент данных SAC опять же является вызовом удаленной процедуры, но на этот раз в отношении функций: функции безопасности. В этом случае он является функциональным вызовом OPIMA. Сообщение HN-MW затем встраивается в сетевое сообщение и передается по домашней сети.

25 Это решение позволяет инфраструктурам безопасности находить друг друга и осуществлять связь между собой, и не зависеть от HN-MW и сетевой технологии. Конечно, SAC можно также встраивать в HN-MW или сетевую технологию. В этом случае картина немного изменится, но функциональные возможности при этом должны остаться.

Аутентификация и доверие

30 Для того, чтобы устройство использовало защищенный контент безопасным образом, системы RMP и инфраструктуры безопасности в сети должны доверять друг другу. От доверенного устройства можно ожидать, что оно будет работать в пределах параметров, установленных стандартом. Для того, чтобы реализовать это, доверенной третьей стороне необходимо проверить устройство перед предоставлением ключей, необходимых для аутентификации.

35 Это осуществляется с помощью двухшагового подхода: система RMP выполняет аутентификацию TVAF, а затем инфраструктуры TVAF выполняют аутентификацию друг друга. Это предотвращает то, что система RMP должна выполнить аутентификацию каждой TVAF в системе и должна поддерживать все виды специфических особенностей HN-MW.

40 Когда система RMP встроена в устройство, аутентификация инфраструктуры безопасности может не требоваться, так как они могут доверять друг другу. Это имеет то преимущество, что (отнимающая много времени) аутентификация инфраструктуры безопасности системой RMP может быть пропущена.

Использование удаленных инструментальных средств

45 Как объясняено выше в разделе, относящемся к инфраструктурам безопасности и внутренним сетям, между инфраструктурами TVAF создается VPN. Это может рассматриваться как одна большая TVAF. VPN может быть использована для локального предоставления инструментальных средств удаленной TVAF. В этом случае вызовы выполняются с помощью вызовов RPC открытого интерфейса другой TVAF. Пример такого 50 вызова в контексте виртуальных машин OPIMA (VMO) (которые могут быть использованы как инфраструктуры TVAF) показан на фиг.4. В устройстве 2 вызов функции и возвращаемое ей значение маршрутизируются через OVM, чтобы символизировать, что RPC с SAC извлечен и вызван.

Другой вариант инфраструктур TVAF для предоставления инструментальных средств, реализованных где-либо в сети, состоит в предоставлении инструментальных средств, непосредственно доступных в HN-MW. Вероятно, лучшим примером таких инструментальных средств является средство считывания интеллектуальных карт. Связь с 5 интеллектуальными картами уже защищена системой RMP, и к ней можно осуществить доступ по незащищенному каналу.

Эта конфигурация позволяет инфраструктурам TVAF предоставлять инструментальные средства HN-MW и инструментальные средства, доступные на других TVAF в VPN. С точки зрения эффективности желательно использовать локальные инструментальные средства, 10 когда они доступны. Сетевые инструментальные средства представляются с помощью обычного API OPIMA. Конечно, в реализации TVAF можно выбрать предоставление сетевых инструментальных средств, что подчеркивает, что использование локальных инструментальных средств не является жестким предписанием.

Декодирование контента, преобразование его в поток и HN-MW

15 При доступе к контенту в сетевой среде может потребоваться преобразование в поток/перенос этого контента от источника к другим устройствам. В большинстве случаев это требует некоторой поддержки QoS (качества обслуживания) из сети. Способ установки соединения в сети и управления QoS сильно зависит от сетевой технологии. Обычно такие потоки создают и останавливают с помощью механизмов, определенных в HN-MW.

20 Так как контент всегда может быть перехвачен на интерфейсе устройства, любой контент, отправляемый из TVAF, должен быть защищен. Как правило, это делается с помощью какого-либо вида шифрования. Система RMP поддерживает управление контентом, контролируя доступ к ключам, которые позволяют дешифровать этот контент. Контент должен лишь покинуть область устройств TVA, защищенных каким-либо видом 25 системы RMP. Более того, управление каждым переносом контента из одной системы RMP в другую осуществляется системой RMP. В этом случае система RMP остается в состоянии контроля того, что случается с контентом.

Распределенный доступ к контенту

Другой путь для использования связующего программного обеспечения домашней сети 30 состоит в осуществлении доступа к контенту с помощью элементов, реализованных в других устройствах. Пример того, как реализовать такой распределенный доступ к контенту, можно увидеть на фиг.5. В этом примере можно выделить следующие роли.

- Источник - источник контента.
- Приемник - приемник контента.
- Обработка - одна или более функций обработки могут быть представлены в тракте потока. Функция обработки является функцией, в которой некая операция выполняется в отношении контента.
- Приложение - приложение, соединяющее различные функции HN-MW и инициирующее доступ к контенту. Заметим, что это "приложение" является в действительности 40 реализацией API стандарта DVB-MHP (DVB - домашняя платформа мультимедиа) (или любого другого подобного API).
- RMP, система RMP, управляющая контентом.

При распределенном доступе к контенту каждая из этих ролей может быть размещена на отличающемся от других устройств.

45 Секции HN-MW и OPIMA

Существует множество форматов контента и систем RMP. Чтобы избежать необходимости моделирования и поддержки каждого возможного варианта, OPIMA использует концепцию секций. Согласно OPIMA секция является классом устройств, поддерживающих OPIMA, которые совместно используют некоторые общие элементы в их 50 интерфейсах RMP и/или архитектурных компонентах. Например, DVB может рассматриваться как секция, которая, в свою очередь, содержит другие секции, определяемые конкретной системой RMP. Секции могут быть иерархическими. То есть секция может содержать подсекции.

Секция определяет различные системные элементы и инструментальные средства, доступные в этой секции. Так как система RMP работает в пределах секции, она знает, какие инструментальные средства и системы можно ожидать. Примерами элементов, определенных в пределах секций, являются алгоритмы шифрования и фильтры правил.

- 5 В пределах HN-MW секции используются для определения сетевых функций, которые должны быть доступны в IHDN, межсоединения в которой должны быть обеспечены с использованием HN-MW. Эти функции безопасности определены в секции и могут быть реализованы как отдельная функция в HN-MW, или же они могут быть встроены в другую функцию (например, тюнер может содержать фильтры правил, дисплей, средство 10 декремблирования). Используя секции, функции безопасности можно определить таким образом, что контент будет доступен только на интерфейсе устройства, защищенном некоторым видом системы RMP.

Защищенный контент и метаданные

- Для того, чтобы осуществить доступ к контенту, система RMP, защищающая этот контент, должна быть известна. При традиционной установке контент доступен в устройстве, которое также содержит компоненты безопасности. В сети это уже не является необходимым. Поэтому приложение требует средства для определения того, какая система RMP используется для защиты контента. Это является дополнительной информацией, которая необходима поверх всех существующих метаданных, таких как 20 формат контента.

- В идеальном случае контент должен обрабатываться только тогда, когда этот контент воспроизводится. Однако в некоторых случаях система RMP может требовать выполнения некоторых операций в отношении контента. Примерами таких операций являются замена ключей и пересифрование. Эти операции зависят от операций, которые требуются в 25 отношении контента, и должны быть известны приложению. Примером таких случаев является то, что при копировании правила, ассоциированные с контентом, могут измениться (copy_one_generation -> copy_no_more). Только когда приложение знает, что некоторые операции требуются для определенной операции, эти операции можно встроить 30 в тракт потока. Другие элементы, которые должны встраиваться в тракт потока, - это конкретные фильтры правил.

- Поэтому приложение должно знать, какие функции безопасности нужно включить в тракт потока. Приложение может узнавать об этих функциях из метаданных. Метаданные контента содержат список для каждого типа доступа к контенту для операций, которые должны быть включены.

- 35 Функции безопасности, которые необходимы, зависят от типа доступа, который требуется в отношении контента. Другими словами, они зависят от Цели (Purpose) доступа к контенту. В OPIMA определен набор целей. Этот набор расширен для соответствия полному набору вариантов доступа к контенту с точки зрения сети.

- Определены три основных класса целей. Полный список целейдается ниже в 40 Приложении Б.
- РАЗБЛОКИРОВКА (RELEASE), этот класс цели управляет переносом контента от одной системы RMP к другой. Следом за классом цели указывается цель контента в другой системе RMP.

- ПРИНЯТЬ (RECEIVE), этот класс цели указывает, что контент принят от другой 45 системы RMP.

- ОСУЩЕСТВИТЬ ДОСТУП (ACCESS), класс цели обрабатывает доступ к контенту в одной системе RMP. Вслед за классом цели, цель указывается более подробно.

- Разблокировка контента необходима, когда права, соответствующие контенту 50 переносятся из одной системы RMP в другую, обычно это требует изменения правил в отношении контента и, возможно также, пересифрования. Транскодирование (формата) контента как при доступе, спецэффекты и обработка изображения с целью его улучшения не изменяют контент и должны быть разрешены в пределах системы RMP. Такие функциональные возможности являются обычно частью функции обработки.

Поэтому метаданные, относящиеся к системам RMP, должны содержать следующую информацию:

- Определение секции (см. Приложение В).
- Определение RMP (см. Приложение В).
- 5 - Список целей, содержащий для каждой цепи URN (унифицированное имя ресурса) функции безопасности, которая требуется.
- Возможно, некоторую информацию, специфическую для секции.

Для того, чтобы распознать функции безопасности, присутствующие в функции в HN-MW, каждая соответствующая функция в HN-MW будет реализовать способы,

10 указывающие на это.

Функции и инфраструктуры безопасности

В этот момент можно создать график потока, содержащий все требуемые функции безопасности, поэтому можно начать сеанс, связанный с этим конкретным контентом. Один или более таких сеансов можно связать для включения всех элементов, необходимых для 15 доступа к контенту.

В OPIMA такой сеанс представлен так называемым Идентификатором_Контента (ContentId), который уникальным образом идентифицирует один из потоков в TVAF. В сетевой среде становится важной возможность определить этот ContentId посредством такого определения, которое делало бы каждый ContentId уникальным. Это реализуется 20 замещением ContentId OPIMA структурой, содержащей следующие значения:

- tvafId (идентификатор TVAF), Уникальный идентификатор TVAF;
- contentAccessId (идентификатор доступа к контенту), уникальный идентификатор, идентифицирующий этот сеанс в пределах этой TVAF;
- streamId (идентификатор потока), число, служащее индикатором потока в этом

25 сеансе, на который делается ссылка.

В приложении B в B.1.5 эта структура представлена в контексте языка описания интерфейсов (IDL) ContentSessionId (идентификатор сеанса, связанного с контентом).

Комбинация tvafId и contentAccessId идентифицирует этот сеанс уникальным образом.

Используя эту информацию, инфраструктуры TVAF функций безопасности в сети могут 30 регистрироваться с помощью Главной TVAF для приема сообщений, относящегося к этому доступу к контенту. Поэтому сначала должен быть создан новый сеанс. Приложение А содержит пример определения внутренних методов, которые могут использоваться для создания сеанса.

Используя tvafId и ContentAccessId, функции безопасности, задействуемые при этом

35 доступе к контенту, могут регистрировать сами себя с помощью TVAF, в которой инициирован доступ к контенту (Главная TVAF). Это делается с помощью метода attachToContentAccess, соответствующего API HN-MW функции безопасности. Когда этот метод вызывается, TVAF функции безопасности будет регистрировать сама себя с помощью Главной TVAF.

40 После регистрации Главная TVAF будет вызывать зарегистрированную TVAF, подтверждать эту регистрацию и указывать цель, ассоцииированную с этим доступом к контенту. TVAF будет обрабатывать контент этого доступа к контенту в рамках этой Цели (Purpose).

Когда все функции безопасности зарегистрированы, сеанс может быть начат. Сеанс

45 начинается посредством инициирования потока в домашней сети, и последующей индикации того, что требуется доступ к контенту. Сначала должен быть инициирован поток, потому что для фильтров правил, расположенных в устройствах, отличающихся от устройства источника, требуется доступ к контенту. Это требует того, чтобы поток был инициирован. Для поддержки частных расширений, в любой момент времени приложение 50 может осуществлять связь напрямую с системой RMP (см. Приложение А в А.3 и А.4).

В этот момент времени сеанс может быть начат. TVAF будет сообщаться с системой RMP, правила будут фильтроваться, и доступ к контенту будут разрешен или запрещен.

Распределенный доступ к контенту и вызовы RPC

В системе RMP локальный и распределенный доступ к контенту должны обрабатываться одинаковым образом. Для того, чтобы использовать интерфейс API OPIMA безотносительно к сетевому доступу, требуются некоторые директивы в отношении обработки RPC. Управление вызовами RPC осуществляется согласно системе, показанной на фиг.6.

Все вызовы системы RMP, показанным как «Вызов», маршрутизируются Главной OVM на все OVM, зарегистрированные в сеансе. Ответы на все вызовы комбинируются, и возвращаемое значение указывается в обратном вызове в систему RMP.

Можно определить два типа вызовов (удаленных процедур), а именно: вызовы, которые 10 относятся к доступу к контенту, и вызовы, которые используют инструментальные средства. Вызовы, связанные с доступом к контенту, используют ContentId для соотнесения с доступом к контенту. Обычно, инструментальные средства, не относящиеся 15 к вызовам, связанным с доступом к контенту, вызываются локально, если они доступны, в противном случае - удаленно. Вызовы, связанные с доступом к контенту, обрабатываются с помощью следующих директив.

1. Если вызов является RPC, обработать его локально и возвратить результат.
2. Если вызов является локальным и если доступ к контенту, соответствующий этому вызову, локальный, то вызвать функцию на всех зарегистрированных TVAF (также локально, если эта TVAF является частью потока).
- 20 3. Если вызов является локальным, а доступ к контенту, соответствующий этому вызову - нет, то вызывается Главная TVAF, контролирующая доступ к контенту.

Сущность «главный-подчиненный» этого решения упрощает связь, так как различным TVAF не надо знать, какие функции располагаются на какой TVAF.

Приложение A. API служб приложений

25 API DAVIC CA служит как API приложений в пределах этого документа. Для того, чтобы реализовать этот API, внутренним образом в устройстве, в котором размещен этот API, некоторая специфическая информация должна быть передана в TVAF. Это делается с помощью частных внутренних API, которые не нуждаются в определении. Следующие (информационные) методы дают пример методов, которые используются для запуска, 30 остановки и управления доступом к контенту.

AttachToContentAccess

Этот способ регистрирует свою TVAF с помощью TVAF, управляющей указанным доступом к контенту так, что она будет принимать любые соответствующие вызовы RPC. Все значения указываются посредством TVAF, когда доступ к контенту начат.

35 А.1 Службы приложений

A.1.1 createContentRelease

Создать сеанс с TVAF с намерением разблокировать контент для другой системы RMP.

	Входные параметры	Значения
40	SourseRMP URL (унифицированный указатель ресурса) для RMP, защищающей контент.	строка (URL TVAF системы RMP).
	TargetRMP URL для RMP, для которой контент будет разблокирован.	строка (URL TVAF системы RMP).
	Purpose Идентификатор цели для доступа к контенту.	
	Выходные параметры	Значения
45	ContentAccessId Уникальный идентификатор этого сеанса в этой TVAF.	Положительное целое значение
	Возвращаемая Переменная	Значения
	Result (результат) либо идентификатор соединения, либо код ошибки	Целое значение. Успешный, если Result=0. Неудачный, если Result<0

A.1.2 createContentAccess

Создает сеанс с TVAF с намерением доступа к контенту.

	Входные параметры	Значения
50	RMP URL для RMP, защищающей контент.	строка (URL TVAF системы RMP).
	Purpose Идентификатор цели для доступа к контенту.	
	Выходные параметры	Значения
	ContentAccessId Уникальный идентификатор этого сеанса в этой TVAF.	Положительное целое значение
	Возвращаемая Переменная	Значения

Result (результат) либо идентификатор соединения, либо код ошибки	Целое значение. Успешный, если Result=0. Неудачный, если Result<0
---	---

A.1.3 createContentReceive

Создает сеанс с TVAF с намерением приема контента из другой системы RMP.

5	Входные параметры	Значения
	SourceRMP URL для RMP, защищающей контент.	строка (URL TVAF системы RMP).
	TargetRMP URL для RMP, для которой контент будет разблокирован.	строка (URL TVAF системы RMP).
10	Purpose Идентификатор цели для доступа к контенту.	
	Выходные параметры	Значения
	ContentAccessId Уникальный идентификатор этого сеанса в этой TVAF.	Положительное целое значение
10	Возвращаемая Переменная	Значения
	Result (результат) Либо идентификатор соединения, либо код ошибки	Целое значение. Успешный, если Result=0 Неудачный, если Result<0

A.1.4 startContentSession

Начинает этот сеанс

15	Входные параметры	Значения
	ContentAccessId Уникальный идентификатор этого сеанса в этой TVAF.	Положительное целое значение
	Listener (принимающая сторона) Функция обратного вызова, которая доставляет ответ TVAF приложению	Адрес метода
20	Возвращаемая Переменная	Значения
	Result (результат) Либо идентификатор соединения, либо код ошибки	32-битное целое, которое может быть либо положительным, либо отрицательным. Положительное значение указывает идентификатор сеанса, который может быть использован приложением для сопоставления последующих асинхронных ответов от TVAF. Отрицательное значение указывает, что произошла ошибка, и причину неудачи.
	Асинхронные Ответы	Значения
25	startContentSessionResponse	Служит индикатором того, возможен ли этот сеанс, связанный с контентом.

A.1.5 stopContent

Прекращает доступ к контенту, разблокировку или прием.

30	Входные параметры	Значения
	Tvafid Уникальный идентификатор TVAF, вызывающей TVAF.	Положительное целое значение
	ContentAccessId Уникальный идентификатор сеанса, связанного с контентом к которому подсоединяется запрос вызывающий TVAF.	Положительное целое значение
35	Возвращаемая Переменная	Значения
	Result (результат) Либо идентификатор соединения, либо код ошибки	Целое значение. Успешный, если Result=0 Неудачный, если Result<0

A.2 Принимающая сторона служб приложений

A.2.1 startContentSessionResponse

Этот асинхронный ответ выдается TVAF приложению для извещения о том, что произошло некоторое событие; он может быть использован для целей синхронизации.

40	Входные параметры	Значения
	SessionID Идентификатор, предоставленный TVAF, который ссылается на действие, на которое выдан этот ответ	То же самое значение, которое ранее было возвращено (startContentSession)
	Статус показывает успех или неудачу, и причину неудачи	Успех, если статус=0 Код ошибки, если статус<0
45	Сообщение Специфическая для RMP строка, подлежащая интерпретации приложением	Специфическая для RMP строка, объясняющая статус.

A.3 Службы RMP приложений

A.3.1 queryRMPSystems

Этот метод позволяет приложениям посыпать сообщения системам RMP, установленным в TVAF, и принимать ответы.

50	Входные параметры	Значения
	Listener (принимающая сторона) Метод обратного вызова, который доставляет ответ TVAF приложению	Адрес метода
	Выходные параметры	Значения
50	Result (результат)	Целое значение. Успех, если Result=0 Неудача, если Result<0
	Возвращаемая переменная	Значения
	indicateRmpList Список систем RMP, известных этой TVAF.	Массив имен URN (строк).

A.3.2 sendMessageToRMP

Этот метод позволяет приложениям посыпать сообщения системам RMP, установленным в TVAF, и принимать ответы.

	Входные параметры	Значения
5	RMPsystemID Идентификационные данные системы RMP, которой адресовано сообщение.	Массив байтов, содержащих уникальный идентификатор, присвоенный органом регистрации.
10	MessageType (Тип Сообщения) Идентификационные данные типа сообщения	Запрос контента Владелец системы RMP Пустое сообщение (NULL) (позволяет приложению, зарегистрировать само себя в качестве приемника сообщений без фактической посылки какого-либо сообщения) Таблица значений дается в определении IDL.
15	Сообщение Listener (принимающая сторона) Метод обратного вызова, который доставляет ответ TVAF приложению	URL (в случае сообщения запроса контента) Данные, передаваемые компоненту RMP.
	Возвращаемые Переменные	Значения
20	Result (Результат)	32-битное целое, которое может быть либо положительным, либо отрицательным. Положительное значение показывает идентификатор сеанса, который может быть использован приложением для сопоставления асинхронных ответов от TVAF. Отрицательные значения показывают, что случилась ошибка, и причину этой неудачи.
25	Асинхронные ответы	Значения
30	Ответ на запрос контента	- Контент не доступен. - Страна для отображения конечному пользователю. - Данные.

A.4 Принимающая сторона служб RMP приложений

A.4.1. msgFromRMP

Этот асинхронный ответ выдается TVAF для приложения с целью уведомления о том, что произошло определенное событие; это может быть использовано для целей синхронизации.

	Входные параметры	Значения
25	SessionID Идентификатор, обеспечиваемый TVAF, который ссылается на действие, на которое выдан этот ответ	То же самое значение, которое было ранее возвращено любой из sendMessageToRMP.
30	Статус Показывает успех или неудачу, и причины неудачи	Успех, если статус=0 Код ошибки, если статус<0
35	Сообщение Специфическая для RMP строка, подлежащая интерпретации приложением	Любое из нижеследующего: - Специфическая для RMP строка (в ответ на запрос sendMessageToRMP) или - Список альтернативных наборов систем RMP, которые необходимы контенту для того, чтобы TVAF выполняла предназначенную "цель", связанную с индикацией их текущего статуса в TVAF (наличие/отсутствие). Системы RMP идентифицируются посредством идентификаторов систем RMP, как описано выше (в ответ на запрос queryTVAF).

A.4.2 indicateRmpList

Этот асинхронный ответ выдается TVAF для приложения с целью информирования о списке доступных систем RMP.

	Входные параметры	Значения
40	SessionID Идентификатор, обеспечиваемый TVAF, который ссылается на действие, на которое выдан этот ответ	То же самое значение, которое было ранее возвращено любой из createContentAccess, createContentRelease, createContentReceive, getRMPSystem, sendMessageToRMP или queryTVAF.
	RMPsystemList Список систем RMP, известных для этой TVAF.	Массив имен URN (строк).
	Статус Показывает успех или неудачу, и причины неудачи	Успех, если статус=0 Код ошибки, если статус<0

Приложение Б: Цели

Определены следующие цели.

Класс цели	Подкласс	Описание
РАЗБЛОКИРОВАТЬ	ВОСПРОИЗВЕСТИ	Разблокировать контент для другой системы RMP, позволяя только воспроизведение на устройстве (без сохранения).
	ПЕРЕМЕСТИТЬ	Переместить этот контент полностью в другую систему RMP.
	КОПИРОВАТЬ	Переместить копию этого контента в другую систему RMP.
ПРИНЯТЬ		Принять контент от другой системы RMP.
ОСУЩЕСТВИТЬ ДОСТУП	СОХРАНИТЬ	Сохранить этот контент на некотором устройстве хранения данных.
	ВОСПРОИЗВЕСТИ	Воспроизвести контент.

	РЕДАКТИРОВАТЬ	Создавать копию контента и редактировать ее.
	УДАЛить	Удалять контент.
	ОБРАБОТАТЬ	Обрабатывать контент без изменения прав (например, битовой скорости или транскодирования контента)
	ДРУГИЕ	Другие варианты доступа определены в секции.

5

Приложение В: API TVAF, относящийся к использованию HN-MW.

B.1 Сетевые службы TVAF

B.1.1 getTVAFId

Возвращает идентификатор TVAF этой TVAF.

10

Выходные параметры	Значения
tvafid Уникальный идентификатор этой TVAF.	Положительное целое значение
Возвращаемая Переменная	Значения
Result (результат) Либо идентификатор соединения, либо код ошибки	Целое значение. Успех, если Result=0 Неудача, если Result<0

15

B.1.2 registerWithContentSession

Регистрирует вызывающую TVAF с указанным сеансом, связанным с контентом.

20

Входные параметры	Значения
tvafid Уникальный идентификатор вызывающей TVAF.	Положительное целое значение
ContentSessionId Уникальный идентификатор связанного с контентом сеанса, который больше не интересует вызывающую TVAF.	Положительное целое значение
Возвращаемая Переменная	Значения
Result (результат) Либо идентификатор соединения, либо код ошибки	Целое значение. Успех, если Result=0 Неудача, если Result<0

25

B.1.3 unRegisterWithContentSession

Отменяет регистрацию вызывающей TVAF с указанным сеансом, связанным с контентом.

30

Входные параметры	Значения
tvafid Уникальный идентификатор вызывающей TVAF.	Положительное целое значение
ContentSessionId Уникальный идентификатор связанного с контентом сеанса, который больше не интересует вызывающую TVAF.	Положительное целое значение
Возвращаемая Переменная	Значения
Result (результат) Либо идентификатор соединения, либо код ошибки	Целое значение. Успех, если Result=0 Неудача, если Result<0

35

B.1.4 contentSessionRegistered

Подтверждение регистрации Главной TVAF. Цель указывает цель, относящуюся к этому доступу к контенту. TVAF будет обрабатывать контент в рамках этой цели.

40

Входные параметры	Значения
tvafid Уникальный идентификатор Главной TVAF.	Положительное целое значение
ContentSessionId Уникальный идентификатор сеанса, связанного с контентом Главной TVAF.	Положительное целое значение
Purpose Уникальный идентификатор сеанса, связанного с контентом, в Главной TVAF.	
Возвращаемая Переменная	Значения
Result (результат) Либо идентификатор соединения, либо код ошибки	Целое значение. Успех, если Result=0 Неудача, если Result<0

45

50

B.1.5 contentSessionStopped

Индикация для других TVAF, что связанный с контентом сеанс остановлен.

Входные параметры	Значения
tvafid Уникальный идентификатор Главной TVAF.	Положительное целое значение

ContentSessionId Уникальный идентификатор сеанса, связанного с контентом в Главной TVAF.	Положительное целое значение
Возвращаемая Переменная	Значения
Result (результат) Либо идентификатор соединения, либо код ошибки	Целое значение. Успех, если Result=0 Неудача, если Result<0

5

B.2 IDL

Код IDL предыдущих способов имеет:

```
// общие структуры
enum Purpose {RELEASE_RENDER, RELEASE_MOVE, RELEASE_COPY, RECEIVE,
10 ACCESS_STORE, ACCESS_RENDER, ACCESS_EDIT, ACCESS_DELETE,
ACCESS_PROCESS, OTHER};

typedef sequence<octet, 16>TVAFId;
struct ContentId
{TVAFId TVAFId;
15 long contentSessionId;
long streamId};
// интерфейсы TVAF, относящиеся к сети
interface TVAFNetworkServices
{long getTVAFId(out TVAFId TVAFId);
20 long registerWithContentSession(in TVAFId TVAFId, in long contentSessionId);
long unRegisterWithContentSession(in TVAFId TVAFId, in long contentSessionId);
long contentSessionRegistered(in TVAFId TVAFId, in long contentSessionId, Purpose p);}

Приложение Г: указатели URL и имена URN TVAF
```

Г.1 Определение Унифицированного Указателя Ресурса (URL)
25 Для использования в инфраструктурах TVAF, даются следующие определения URL:

- Системы RMP

tvaf://<network_adress>/<TVAFId>/ipmp/<rmp_id>

- Приложения

tvaf://<network_adress>/<TVAFId>/app/<app_id>

30 - Инструментальные средства

tvaf://<network_adress>/<TVAFId>/tool/<tool_id>

В этих указателях URL различные поля имеют следующие значения:

tvaf::, отображает сообщения, посылаемые через SAC.

35 <network_address> - адрес устройства, на котором размещена TVAF.
<TVAFId> - идентификатор TVAF.

<RMP_id> - идентификатор модуля RMP.

<app_id> - идентификатор приложения.

<tool_id> - идентификатор инструментального средства.

Например:

40 tvaf://130.130.120.4/34535/ipmp/1213

tvaf://130.130.120.4/34535/app/113

tvaf://130.130.120.4/34535/tool/12234

Г.2 Определение Унифицированного Имени Ресурса (URN)

Имена URN системы TVAF определяются как:

45 - Секции:

tvaf://<compartment_source>/compartment

- Функции безопасности:

tvaf://<compartment_source>/compartment/<function>

В этих именах URN различные поля имеют следующие значения:

50 <compartment_source> - имя (стиль Интернет) тела, которое определяет секцию.

<function> - имя этой специальной функции в этой секции.

Например:

tvaf://org.dvb/mpeg2

tvaf://org.dvb/mpeg2/sink
 tvaf://org.dvb/mpeg2/receive
 tvaf://org.dvb/mpeg2/source
 tvaf://org.dvb/mpeg2/processor

5 Приложение Д: Методы на методах HN-MW

Д.1 API TVAF

Инфраструктуры TVAF представлены в HN-MW, как отдельный метод. Последующие методы должны быть доступны на такой функции.

Д.1.1 newMessage

10 Новое сообщение для этой TVAF принято.

Входные параметры	Значения
Message Сообщение, которое посыпается к этой TVAF.	Массив байтов, содержащих сообщение SAC.
Возвращаемая Переменная	Значения
Result (результат) Либо идентификатор соединения, либо код ошибки	Целое значение. Успех, если Result=0 Неудача, если Result<0

Д.2 API функции безопасности

Последующие методы будут доступны на функциях в HN-MW, поддерживающем функции безопасности.

20 Д.2.1 getSecurityFunction

Этот метод показывает имена URN функций безопасности (Приложение Г), поддерживаемых этой функцией HN-MW

Выходные параметры	Значения
securityFunctionUrns имена URN функций безопасности секций, поддерживаемых этой функцией HN-MW.	Массив строк (имен URN).
Возвращаемая Переменная	Значения
Result (результат) Либо идентификатор соединения, либо код ошибки	Целое значение. Успех, если Result=0 Неудача, если Result<0

Д.2.2 attachToContentAccess

30 Этот метод регистрирует свою TVAF с помощью TVAF, управляющей указанным доступом к контенту, так что он будет принимать любые соответствующие вызовы RPC. Все значения указываются посредством TVAF, когда начинается доступ к контенту.

Входные параметры	Значения
tvaflId TVAF, управляющая этим доступом к контенту.	Целое значение
ContentAccessId Уникальный идентификатор этого доступа к контенту в TVAF, которая управляет этим доступом к контенту.	
Возвращаемая Переменная	Значения
Result (результат) Либо идентификатор соединения, либо код ошибки	Целое значение. Успех, если Result=0 Неудача, если Result<0

40

Приложение Е: Сокращения

Ниже приведен список сокращений, которые используются в этом документе, с их значениями.

AES	Усовершенствованный Стандарт Шифрования
APDU	Модуль Данных Протокола Прикладного Уровня
API	Интерфейс Прикладного Программирования
CFC	Призыв к Содействию
DAVIC	Совет по Цифровой Аудио и Визуальной Информации
DVB	Цифровое Видеовещание
HAVi	Взаимодействие Бытовой Аудио- и Видеоаппаратуры

50

	HN-MW Связующее программное обеспечение домашней сети
	ISO Международная Организация по Стандартизации
	MMI Интерфейс взаимодействия человека с аппаратурой
	MPEG Экспертная Группа По Вопросам движущихся изображений
	OVM Виртуальная Машина OPIMA
	QoS Качество Обслуживания
5	RMP Управление Правами и их Защита
	RPC Вызов Удаленных Процедур
	SAC Защищенный аутентифицированный Канал
	TLS Протокол Защиты Транспортного Уровня
	TTP Доверенная Третья Сторона
	TVA «ТВ в любое время»
	TVAF Инфраструктура TVA
10	UpnP Универсальные стандарт на распознавание и настройку оборудования без последующего конфигурирования пользователем
	VPN Виртуальная Частная Сеть

Следует отметить, что описанные выше варианты выполнения иллюстрируют, а не ограничивают изобретение, и что специалисты в данной области техники будут способны сконструировать множество альтернативных вариантов выполнения, не выходя за рамки объема, определяемого прилагаемой формулой изобретения. Например, хотя в вышеприведенном описании используется стандарт OPIMA, другие инфраструктуры безопасности могут быть, конечно же, использованы вместо него. Например, расширения IPMP (Управления и защиты интеллектуальной собственности) MPEG-4 могут быть использованы в подобных случаях.

20 В формуле изобретения любые ссылочные обозначения, расположенные в круглых скобках, не должны интерпретироваться как ограничения формулы изобретения. Слово "содержащий" не исключает наличия элементов или этапов, отличающихся от описанных в формуле изобретения. Употребление элемента в единственном числе не исключает наличия множества таких элементов. Изобретение может быть реализовано посредством аппаратного обеспечения, содержащего некоторое количество отдельных элементов, и посредством соответственно запрограммированного компьютера.

25 В пункте формулы изобретения, относящемуся к устройству и в котором перечислены некоторые средства, некоторые из этих средств могут быть воплощены одним и тем же элементом аппаратного обеспечения. Простой факт того, что определенные меры излагаются во взаимно отличающихся пунктах формулы изобретения, не свидетельствует 30 о том, что комбинация этих мер не может использоваться выгодным образом.

Формула изобретения

35 1. Система условного доступа, содержащая множество устройств, соединенных между собой в сеть, при этом на каждом из этих устройств установлено связующее программное обеспечение, обеспечивающее упомянутым устройствам возможность взаимодействия друг с другом, причем эти устройства сгруппированы в первую группу и во вторую группу, устройства первой группы работают в соответствии с первой инфраструктурой безопасности, а устройства второй группы работают в соответствии со второй 40 инфраструктурой безопасности, причем каждое устройство работает с использованием конкретного слоя связующего программного обеспечения, при этом упомянутый слой связующего программного обеспечения сконфигурирован для аутентификации другого слоя связующего программного обеспечения другого устройства, причем аутентификацию упомянутого слоя связующего программного обеспечения выполняет инфраструктура безопасности, в соответствии с которой работает устройство.

45 2. Система по п.1, в которой устройство из первой группы может выполнять функцию второй инфраструктуры безопасности, выполняя вызов удаленной процедуры (RPC) в отношении слоя связующего программного обеспечения устройства второй группы.

3. Система по п.2, в которой RPC передается устройству второй группы через защищенный аутентифицированный канал (SAC).

50 4. Система по п.1, в которой устройствам выдается разрешение на доступ к контенту в соответствии с конкретным классом операций, при этом определен набор таких классов, причем каждый класс содержит некоторое количество операций условного доступа.

5. Система по п.4, в которой первый класс из набора включает в себя операции

ВОСПРОИЗВЕСТИ, ПЕРЕМЕСТИТЬ и КОПИРОВАТЬ.

6. Система по п.5, в которой второй класс из набора включает в себя операции СОХРАНИТЬ, ВОСПРОИЗВЕСТИ, РЕДАКТИРОВАТЬ, УДАЛИТЬ и ОБРАБОТАТЬ.

5 7. Система по п.6, в которой операция ОБРАБОТАТЬ санкционируется независимо от любых ограничений на права, связанные с контентом.

8. Способ разрешения сетевому устройству осуществлять условный доступ к части контента в сети, в котором устройству выдают разрешение на доступ к контенту в соответствии с конкретным классом операций, при этом определен набор таких классов, причем каждый класс содержит некоторое количество операций условного доступа.

10 9. Способ по п.8, в котором первый класс из набора включает в себя операции СОХРАНИТЬ, ВОСПРОИЗВЕСТИ, РЕДАКТИРОВАТЬ, УДАЛИТЬ и ОБРАБОТАТЬ.

10. Способ по п.9, в котором операцию ОБРАБОТАТЬ санкционируют независимо от любых ограничений на права, связанные с контентом.

15

20

25

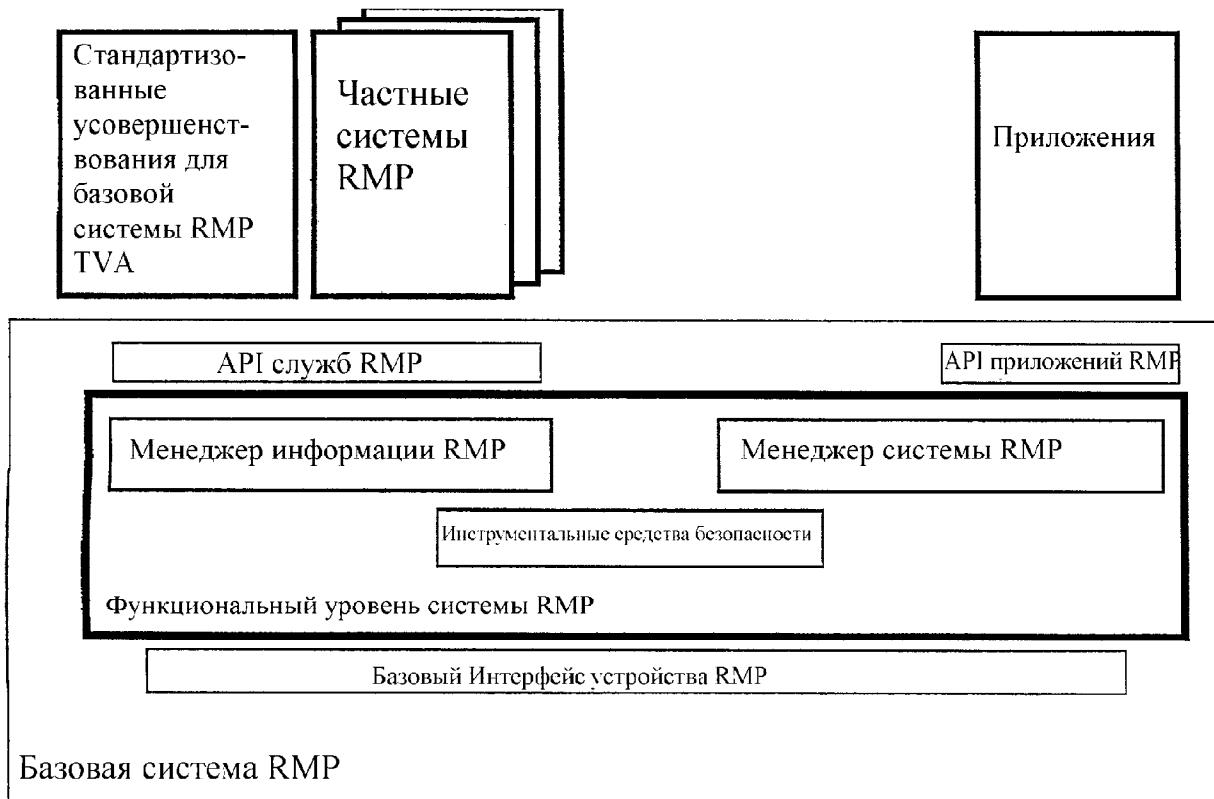
30

35

40

45

50



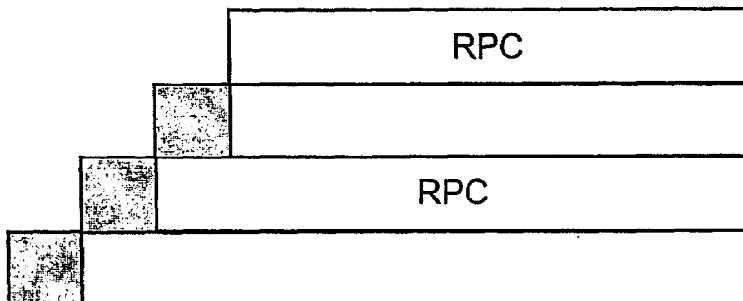
ФИГ.2

Инфраструктура безопасности

SAC

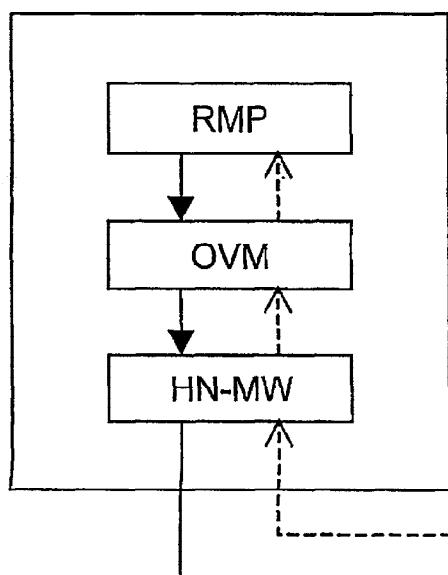
HN-MW

Сеть

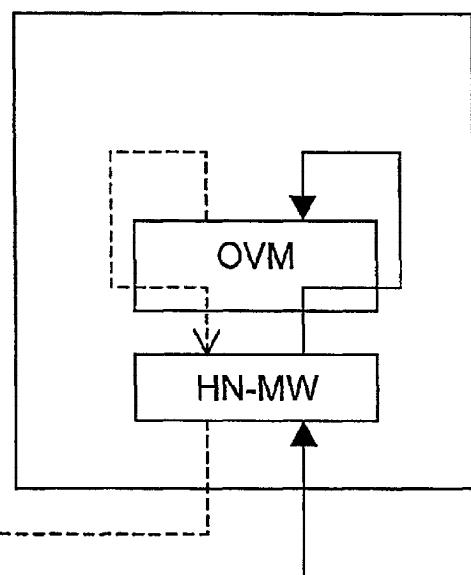


ФИГ. 3

Устройство 1

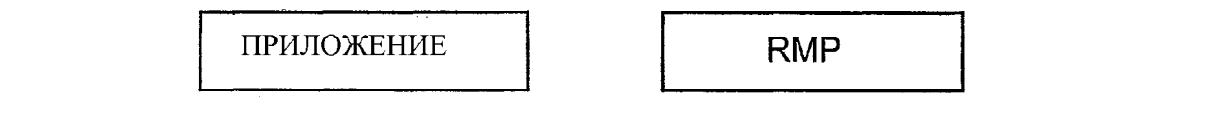


Устройство 2



-----→ Значение, возвращаемое
функцией → Вызов функции

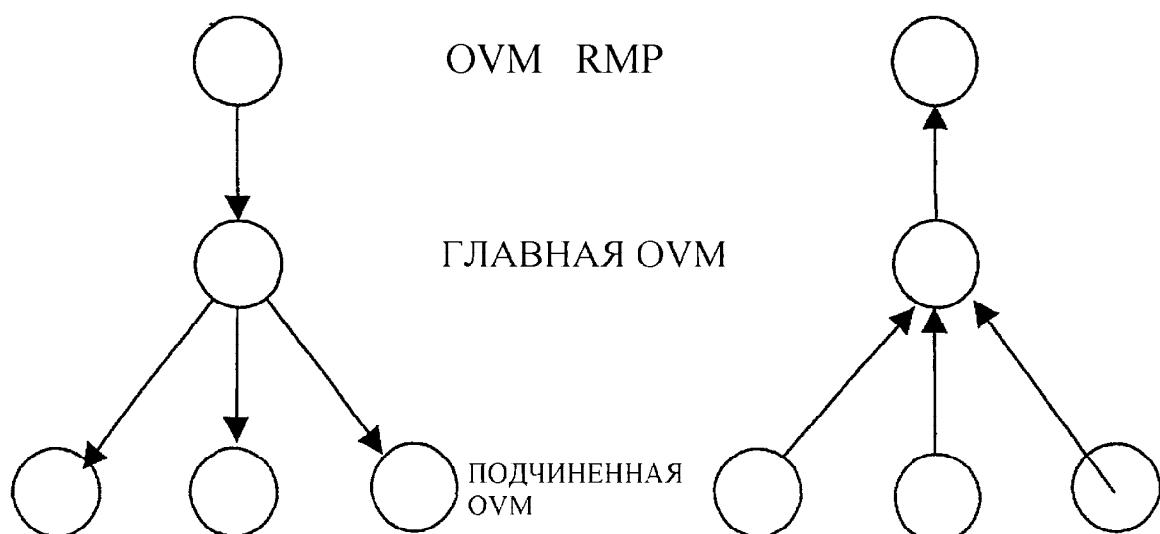
ФИГ. 4



ФИГ. 5

ВЫЗОВ

ОБРАТНЫЙ ВЫЗОВ



ФИГ. 6