РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(19) **RU** (11) **2 409 002** (13) **C2**

(51) МПК
H04N 7/167 (2011.01)
H04H 60/23 (2008.01)
H04L 9/00 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2007148552/09, 06.07.2006**

(24) Дата начала отсчета срока действия патента:
06.07.2006

Приоритет(ы):
(30) Конвенционный приоритет:
07.07.2005 EP 05106185.1

(43) Дата публикации заявки: **20.08.2009** Бюл. № 23

(45) Опубликовано: **10.01.2011** Бюл. № 1

(56) Список документов, цитированных в отчете о поиске: **US 2004215691 A1, 28.10.2004. WO 03069910 A1, 21.08.2003. WO 2004071091 A1, 19.08.2004. US 5461675 A, 24.10.1995. EP 1353511 A2, 15.10.2003. US 5349641 A, 20.09.1994. EP 0866613 A1, 23.09.1998. RU 2196389 C2, 10.01.2003. RU 2199832 C2, 27.02.2003. FRANCIS et al. Countermeasures for attacks on satellite TV cards using open receivers. AUSTRALASIAN** (см. прод.)

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **07.02.2008**

(86) Заявка PCT:
EP 2006/063988 (06.07.2006)

(87) Публикация заявки PCT:
WO 2007/006735 (18.01.2007)

Адрес для переписки:
191186, Санкт-Петербург, а/я 230, "АРС-ПАТЕНТ", пат.пов. В.М.Рыбакову, рег. № 90

(72) Автор(ы):
КЮДЕЛЬСКИ Анри (CH),
КОШАР Джимми (CH)

(73) Патентообладатель(и):
Награвисьон С.А. (CH)

RU 2409002 C2

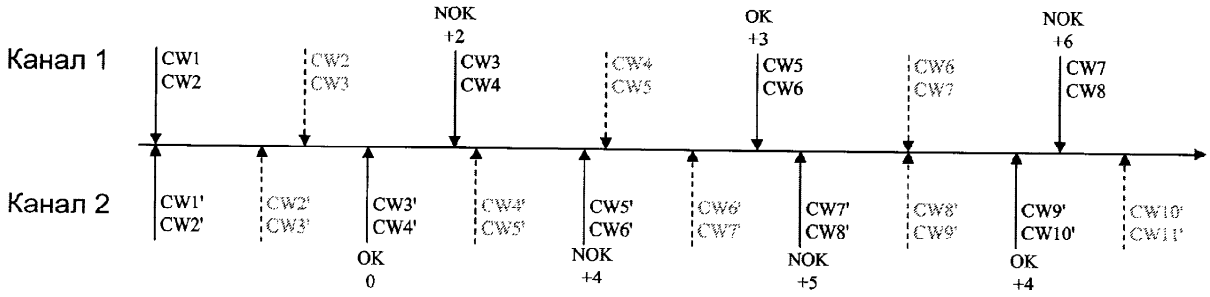
RU 2409002 C2

(54) СПОСОБ И УСТРОЙСТВО ДЛЯ УПРАВЛЕНИЯ ДОСТУПОМ К ЗАШИФРОВАННЫМ ДАННЫМ

(57) Реферат:

Изобретение относится к способу и устройству для управления доступом к данным, зашифрованным с использованием контрольных слов (CW), получаемых модулем защиты в сообщениях (ECM) управления и возвращаемых в модуль обработки (STB) зашифрованных данных. Техническим результатом является предотвращение доступа к зашифрованному содержанию при мошенническом использовании декодеров. Указанный результат достигается тем, что способ включает в себя следующие этапы: получение первого сообщения (ECM1)

управления, содержащего по меньшей мере одно контрольное слово (CW) и отметку (TS) времени; получение второго сообщения (ECM2) управления, следующего за первым сообщением (ECM1) управления, причем второе сообщение управления содержит по меньшей мере одно контрольное слово (CW) и отметку (TS) времени; определение продолжительности отрезка времени, соответствующего разности между отметками (TS) времени двух последовательных сообщений ECM1, ECM2; увеличение счетчика (CE) ошибок в случае, если указанная продолжительность отрезка времени меньше предварительно заданной продолжительности (CP); уменьшение счетчика (CE) ошибок в случае, если указанная продолжительность отрезка времени равняется или превышает указанную предварительно заданную продолжительность; возврат контрольного слова (CW) в модуль (STB) обработки по прошествии времени ожидания, которое зависит от значения счетчика (CE) ошибок. 2 н. и 14 з.п. ф-лы, 6 ил.



ФИГ. 6

(56) (продолжение):

INFORMATION SECURITY WORKSHOP. DIGITAL RIGHTS MANAGEMENT. 6 November 2004, с.1-6.

RU 2409002 C2

RU 2409002 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 409 002** (13) **C2**

(51) Int. Cl.
H04N 7/167 (2011.01)
H04H 60/23 (2008.01)
H04L 9/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2007148552/09, 06.07.2006**

(24) Effective date for property rights:
06.07.2006

Priority:
(30) Priority:
07.07.2005 EP 05106185.1

(43) Application published: **20.08.2009** Bull. 23

(45) Date of publication: **10.01.2011 Bull. 1**

(85) Commencement of national phase: **07.02.2008**

(86) PCT application:
EP 2006/063988 (06.07.2006)

(87) PCT publication:
WO 2007/006735 (18.01.2007)

Mail address:
191186, Sankt-Peterburg, a/ja 230, "ARS-PATENT", pat.pov. V.M.Rybakovu, reg. № 90

(72) Inventor(s):
KJuDEL'SKI Anri (CH),
KOShAR Dzhimmi (CH)

(73) Proprietor(s):
Nagravis'on S.A. (CH)

RU 2409002 C2

RU 2409002 C2

(54) METHOD AND DEVICE TO CONTROL ACCESS TO CODED DATA

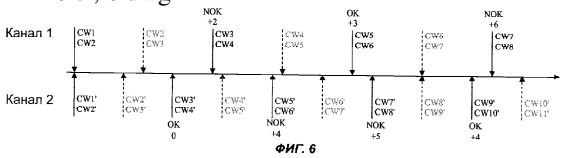
(57) Abstract:

FIELD: information technologies.

SUBSTANCE: method includes the following stages: receipt of the first control message (ECM1), containing at least one control word (CW) and time score (TS); receipt of the second control message (ECM2), following the first control message (ECM1), besides, the second control message contains at least one control word (CW) and time score (TS); detection of duration of time period, corresponding to difference between time scores (TS) of two serial messages ECM1, ECM2; increasing counter of errors (CE) in case specified duration of time period is less than previously set duration (CP); reducing counter of errors (CE) in case specified duration of time period equals or exceeds specified previously set duration; return of control word (CW) into module of processing (STB) as waiting time expires, which depends on value of counter of errors (CE).

EFFECT: prevention of access to coded content in case of fraudulent use of decoders.

16 cl, 6 dwg



ФИГ. 6

Область техники, к которой относится изобретение

Настоящее изобретение относится к способу и устройству для управления доступом к данным, зашифрованным посредством контрольных слов, которые модуль защиты получает в управляющих сообщениях и возвращает модулю обработки зашифрованных данных.

Настоящий способ и устройство применяются, в частности, в сфере платного телевидения.

Уровень техники

Известный способ в области платного телевидения состоит в том, что данные шифруются поставщиком данных посредством ключей шифрования, которые называются контрольными словами. Эти данные передаются в мультимедийные модули пользователей или абонентов. Параллельно с этим контрольные слова передаются в указанные мультимедийные модули в виде потока сообщений управления.

Мультимедийные модули обычно состоят из модуля обработки, который в случае платного телевидения представляет собой декодер, получающий вышеуказанный поток, и из модуля защиты, отвечающего за криптографические операции, связанные с использованием таких потоков.

Как хорошо известно специалистам в данной области, модуль защиты такого типа может быть представлен в четырех различных разновидностях. Первая из них представляет собой микропроцессорную карту, смарт-карту или, в более общем смысле, электронный модуль (в виде ключа, электронного пропуска, и т.д.). Модуль такого типа, как правило, является съемным и может быть подключен к декодеру. Наиболее широко распространена разновидность с электрическими контактами, однако не исключается использование бесконтактного соединения, например соединения типа ISO 14443.

Вторая известная разновидность модуля защиты представляет собой модуль интегральных схем, который, как правило, размещается определенным несъемным способом в модуле декодера. В одном из вариантов схема установлена на основании или разъеме, таком как разъем для SIM модуля.

В третьей разновидности модуль защиты интегрирован в модуль интегральных схем, имеющий также другую функцию, например в модуль дешифратора в декодере или в микропроцессор декодера.

В четвертом варианте осуществления модуль защиты физически не изготавливается, а его функции реализуются с помощью программного обеспечения. Учитывая то, что функция модуля защиты в этих четырех случаях аналогична, хотя уровень защиты и отличается, можно говорить о модуле защиты независимо от того, как он функционирует, или в каком качестве он выполнен.

После того как мультимедийный модуль получил поток, содержащий контрольные слова, в первую очередь проверяется, обладает ли пользователь правами на дешифровку заданных данных. Если это так, то производится дешифровка сообщений управления для того, чтобы извлечь контрольные слова. Эти контрольные слова в свою очередь используются для дешифровки данных.

Также известно, что каждое контрольное слово, как правило, позволяет дешифровать небольшую часть передаваемых данных. Обычно одно контрольное слово позволяет дешифровать 10 секунд программы платного телевидения. По прошествии этого периода времени, называемого криптопериодом, контрольное слово изменяется по соображениям защиты.

Один из возможных способов использования доступа к зашифрованным данным без авторизации заключается в использовании подлинного мультимедийного модуля вместе с настоящим модулем защиты и в распределении контрольных слов между несколькими декодерами. Это можно осуществить с помощью сервера или разделительного устройства, известного как «сплиттер» (splitter). Таким образом, сумма, соответствующая приобретению прав доступа к зашифрованным данным, уплачивается за один мультимедийный модуль, в то время как программы доступны нескольким мультимедийным модулям.

В европейской заявке EP 1575293 описывается способ, предназначенный для того, чтобы предотвратить совместное использование модуля защиты несколькими пользователями. Для реализации этого способа модуль защиты располагает памятью, предназначенной для запоминания последовательностей сообщений управления. Модуль защиты также располагает средствами анализа отклоняющихся от нормы последовательностей сообщений управления. Эти средства работают, сравнивая сообщения управления, помещенные в память. При обнаружении отклоняющейся от нормы последовательности происходит увеличение счетчика ошибок. В соответствии со значением счетчика ошибок в обработку контрольных слов вносится временная задержка.

В способе, описанном в указанной заявке, отклоняющееся от нормы поведение определяется на основании анализа используемых каналов. Например, если идентификатор канала поочередно имеет значение A и B, то средства анализа определяют, что это случай отклоняющейся от нормы последовательности, связанный с совместным использованием модуля защиты. При этом счетчик ошибок увеличивается. Наоборот, если идентификатор канала имеет значение A в течение нескольких криптопериодов, а затем принимает значение B на несколько криптопериодов, это не будет рассматриваться как отклоняющееся от нормы поведение, и счетчик ошибок не будет увеличен.

Изобретение, описанное в заявке US 2004/0215691, предназначено для предотвращения такого мошеннического использования. Для того чтобы достичь этого, каждый раз, когда мультимедийный модуль получает сообщение управления, этот модуль или модуль защиты, которому он соответствует, определяет то, к какому каналу относится данное сообщение управления. Идентификаторы каналов запоминаются вместе с информацией о времени. Сообщения сравниваются, для того чтобы определить, относятся ли они к разным каналам или к одному и тому же каналу. Если они относятся к разным каналам, то счетчик увеличивается на определенное значение. Если сообщения управления относятся к одному и тому же каналу, счетчик уменьшается. Если счетчик достигает установленного порогового значения, то это означает, что произошло большое количество изменений канала и расшифровка контрольных слов прекращается.

Два процесса, описанные в документах EP 1575293 и US 2004/0215691, влекут за собой необходимость иметь в распоряжении идентификатор соответствующего канала для каждого сообщения управления. В некоторых вариантах дело обстоит не так. Используя сообщения управления в частности так, как это определено стандартом Eurocrypt № EN 50094 от декабря 1992 года, можно идентифицировать класс каналов, а не каждый канал по отдельности. В этом случае с помощью изобретения, описанного выше, невозможно заблокировать использование нескольких мультимедийных модулей, которые используют только один модуль защиты и сплиттер.

Документ «Меры противодействия атакам на карты спутникового телевидения, использующие открытые приемники» XP-002333719, Фрэнсис и др. в общих чертах описывает различные средства для того, чтобы исключить мошенническое использование модулей защиты. В соответствии с одним частным аспектом этот документ предлагает проверку того, находится ли отметка времени сообщения в будущем относительно отметки времени сообщения, полученного ранее. Однако в этом документе не упоминается о каком-либо конкретном решении. В частности, нет информации, позволяющей различить нелегальное использование модуля защиты несколькими пользователями и легальное переключение каналов только одним пользователем.

Раскрытие изобретения

Изобретение предлагает реализовать решение, альтернативное известным в области техники, не использующее идентификатор канала, и, в то же время, предотвращающее использование разделительного устройства, которое позволяет получить доступ к зашифрованному содержательному материалу от одного модуля защиты нескольким декодерам. Более того, в соответствии с данным решением идентификатор соответствующего канала не нужен, поскольку решение также работает в случае, когда сообщения управления не содержат такой идентификатор канала, а каналы, например, сгруппированы по классу.

Цель изобретения достигается посредством способа управления доступом к данным, зашифрованным посредством контрольных слов, получаемых модулем защиты в сообщениях управления и возвращаемых в модуль обработки зашифрованных данных, содержащего следующие шаги:

получение первого сообщения управления, содержащего по меньшей мере одно контрольное слово и отметку времени,

получение второго сообщения управления, следующего за первым сообщением управления, причем второе сообщение управления содержит по меньшей мере одно контрольное слово и отметку времени,

определение продолжительности отрезка времени, соответствующего разности между отметками времени двух последовательных сообщений управления,

увеличение значения счетчика ошибок в случае, если указанная продолжительность отрезка времени меньше предварительно заданной продолжительности,

уменьшение значения счетчика ошибок в случае, если указанная продолжительность отрезка времени равняется или превышает указанную предварительно заданную продолжительность.

Цель изобретения достигается также посредством устройства для управления доступом к данным, зашифрованным посредством контрольных слов, получаемых модулем защиты в сообщениях управления и возвращаемых в модуль обработки зашифрованных данных, содержащего

средства получения первого сообщения управления, содержащего по меньшей мере одно контрольное слово,

средства получения второго сообщения управления, следующего за первым сообщением управления, причем второе сообщение управления содержит по меньшей мере одно контрольное слово,

средства определения продолжительности отрезка времени, отделяющего два последовательных сообщения управления,

средства увеличения значения счетчика ошибок в случае, если указанная продолжительность отрезка времени меньше предварительно заданной

продолжительности,

средства уменьшения значения счетчика ошибок в случае, если указанная продолжительность равняется или превышает указанную предварительно заданную продолжительность.

В целом способ и устройство в соответствии с изобретением дают возможность на основании информации о времени, относящейся к сообщениям управления, посланным центром управления, определить то, каким образом эти сообщения управления посылаются и обрабатываются - мошенническим или обычным путем. Счетчик ошибок позволяет принять меры, когда обнаружено отклоняющееся от нормы использование. Существуют различные виды мер, такие как кратковременный перерыв обслуживания, задержка возврата контрольных слов или даже блокировка модуля защиты, в случае которой разблокировка может производиться либо автоматически, либо по запросу посредством телефонной связи. В случае обычного использования пользователь не заметит никаких изменений, связанных с применением данного способа. Под обычным использованием подразумевается как доступ к зашифрованному содержательному материалу на определенном канале, так и переключение каналов («бегство от рекламы») в течение «разумного» отрезка времени. И наоборот, в случае мошеннического использования разделительного устройства, которое обслуживает несколько декодеров только от одного модуля защиты, доступ к зашифрованному содержательному материалу быстро становится невозможным. Как только использование снова становится корректным, доступ к данным может быть снова разрешен.

Краткое описание чертежей

Изобретение и его преимущества может быть лучше понято со ссылками на прилагаемые чертежи и подробное описание отдельного примерного варианта осуществления, не вносящего каких-либо ограничений.

На фиг.1 представлен пример структуры сообщения управления, используемой в настоящем изобретении.

На фиг.2 представлена конфигурация, в которой два декодера используются только с одним модулем защиты и разделительным устройством.

На фиг.3 схематично представлен вариант осуществления процесса дешифрования в соответствии с данным изобретением.

На фиг.4 представлено получение сообщения ECM управления в зависимости от времени.

На фиг.5 представлены значение счетчика ошибок в зависимости от времени, и управляющие сообщения, получаемые, как представлено на фиг.4.

На фиг.6 представлен вариант изобретения, в котором для различных каналов используются разные криптопериоды.

Осуществление изобретения

На фиг.1 схематично представлены содержание и структура сообщения ECM управления (Entitlement Control Message), которое используется в настоящем изобретении. Это сообщение ECM управления содержит поля, в которых, в частности, могут находиться отметка времени, отражающая дату и время, длительность криптопериода CP, условия CA доступа к аудио- и/или видеоматериалу и два контрольных слова CW1, CW2 разной четности. Сообщение управления может также содержать другие поля, которые здесь подробно не описываются. Данные, содержащиеся в полях сообщения управления, обычно шифруются посредством ключа TK передачи. Это сообщение может также содержать один или более заголовков,

которые не обязательно зашифрованы. В частности, такое сообщение включает в себя заголовок H, который позволяет мультимедийному модулю идентифицировать его как сообщение ECM управления, указанный заголовок не должен быть зашифрован. Следует отметить, что криптопериод не обязательно содержится в таком сообщении управления. В действительности, если криптопериоды различных каналов одинаковы и остаются постоянными в течение некоторого периода времени, то криптопериод может быть передан в сообщении EMM авторизации (Entitlement Management Message).

Согласно первому варианту осуществления изобретение функционирует следующим образом. Стандартным образом сообщение ECM управления посылается в мультимедийный модуль, содержащий декодер STB и модуль SC защиты. При получении этого сообщения управления условия CA доступа, требуемые для доступа к определенному содержательному материалу, в дальнейшем также называемому аудио- и/или видеоматериалом, извлекаются из этого сообщения управления модулем защиты. Затем модуль защиты проверяет, обладает ли он правами на возврат контрольного слова. В случае, если это не так, модуль защиты не возвращает контрольное слово. Если права на дешифрование присутствуют, то контрольное слово передается в декодер.

Значение криптопериода CP также извлекается из сообщения управления или определяется другим путем. Это значение CP запоминается в памяти, соединенной с модулем защиты. Соответствующее контрольное слово возвращается в декодер, как правило, зашифрованным посредством сеансового ключа. Сеансовый ключ обычно основан на паре асимметричных ключей, причем в этой паре один из ключей запоминается в модуле защиты, а другой запоминается в декодере. Ключи этой пары называются спаренными ключами (pairing keys) и, вообще говоря, различны и уникальны для каждого мультимедийного модуля. Зашифрованный содержательный материал может затем быть расшифрован с помощью этого контрольного слова и отображен на экране пользователя. Механизм формирования пары подробно описан в европейском патенте № EP 1078524.

Когда мультимедийный модуль получает следующее сообщение управления, оно расшифровывается таким образом, чтобы среди прочего извлечь отметку TS времени.

Эта отметка времени сравнивается с отметкой времени, которая была запомнена во время обработки предыдущего сообщения управления. Разность между этими двумя отметками времени сравнивается с криптопериодом, который также был запомнен во время обработки предыдущего сообщения управления. Если эта разность меньше, чем значение криптопериода, то это означает, что мультимедийный модуль получил более чем одно сообщение за криптопериод, и значение счетчика увеличивается. Этот счетчик, в последующем описании называемый счетчиком CE ошибок, размещается, как правило, в модуле защиты. Увеличение этого счетчика, таким образом, производится тогда, когда от модуля защиты требуется возвращать контрольные слова с частотой, большей, чем криптопериод, либо из-за переключения каналов пользователем, либо из-за работы более чем одного мультимедийного модуля с одним и тем же модулем защиты.

На фиг.2 представлена конфигурация, для борьбы с которой предназначено данное изобретение. В этой конфигурации на два устройства обработки данных или два декодера STB1, STB2 подаются контрольные слова только одним модулем защиты и разделительным устройством. В этой конфигурации, при получении одним из декодеров сообщения ECM управления, тот передает его в разделительное устройство SP, которое, в свою очередь, посылает сообщение управления обратно в

модуль SC защиты. Последний расшифровывает это сообщение, если имеет на это права, а затем передает контрольное слово одному из декодеров STB1 или STB2 посредством разделительного устройства SP.

На фиг.2 представлены только два декодера. Теоретически можно снабжать контрольными словами большее число декодеров посредством одного модуля защиты и разделительного устройства.

Следует отметить, что способ контролирует только отрезки времени, связанные с сообщениями ECM управления. Если сообщения других типов, например сообщения EMM авторизации, посылаются между двумя сообщениями управления, то они не принимаются в расчет и не нарушают функционирования процесса.

Использование данных счетчика ошибок

Ниже описан отдельный пример варианта осуществления со ссылкой на фиг.3. В этом варианте осуществления значение счетчика CE ошибок используется для внесения временной задержки возврата контрольных слов CW, извлекаемых из сообщений ECM управления. В примере на фиг.3 используется предположение, что криптопериод равняется 10 секундам. При получении первого сообщения ECM1 управления оно обрабатывается таким образом, что из него извлекаются содержащиеся в нем контрольные слова, называемые, соответственно, CW1(C1) и CW2(C1). Следует отметить, что на фиг.3 верхняя часть соответствует каналу C1, а нижняя часть соответствует каналу C2. Для того чтобы избежать слишком большого количества деталей на этой фигуре, контрольное слово CW1(C1), соответствующее каналу C1, обозначается просто как CW1. Аналогично контрольное слово CW1(C2), соответствующее каналу C2, на фиг.3 также обозначается как CW1. Вследствие их расположения на фигуре, различие между этими двумя контрольными словами очевидно. В описании идентификатор канала указывается в скобках.

Обработка сообщения ECM1 управления обычно продолжается в течение нескольких десятков миллисекунд. Пока используется одно из контрольных слов, например контрольное слово CW1(C1), запоминается другое контрольное слово CW2(C1), содержащееся в том же сообщении ECM1 управления. Сообщение управления, соответствующее тому же самому каналу, как правило, будет содержать контрольное слово, запомненное во время обработки предыдущего сообщения, а также дополнительное контрольное слово, которое предоставляется для использования во время следующего криптопериода. Таким образом, каждое контрольное слово посылается дважды. Данный способ работы дает преимущество, состоящее в том, что контрольные слова, за исключением тех, которые были получены сразу после переключения канала, запоминаются до того, как будут использованы, и поэтому при необходимости сразу доступны.

Счетчик CE ошибок вносит временную задержку в возврат контрольных слов модуля защиты в декодер. Это означает, что вместо обработки сообщения ECM управления и возврата контрольных слов, как только они были извлечены, передача указанных контрольных слов в декодер задерживается на период времени, который зависит от значения, которое запомнено в этом счетчике.

На фиг.3 представлен пример, в котором нелегально используется разделительное устройство (сплиттер) между модулем защиты и двумя декодерами STB1 и STB2. В простейшем случае, когда криптопериоды одинаковы, и когда пользователи не переключают каналы, при описанной выше конфигурации за каждый криптопериод будут получены два управляющих сообщения. Поэтому за каждый криптопериод значение счетчика CE ошибок будет увеличиваться. Это увеличение может быть

выполнено в соответствии с предварительно определенными значениями, например, на две единицы. В качестве примера можно представить, что временная задержка вносится в обработку сообщений управления из расчета 1 секунда на единицу счетчика ошибок, начиная с момента, когда это значение превышает пороговое значение, равное 10. Если счетчик еще не достиг этого порогового значения 10 или равен 10, временная задержка не вносится.

Если начальное значение счетчика равно нулю (CE=0), то при получении первого сообщения ECM1 управления значение криптопериода CP, например 10 секунд, будет запомнено. Расшифровываются контрольные слова CW1(C1) и CW2(C1). Контрольное слово CW1(C1) используется для расшифровки аудио- и/или видеоматериала, а контрольное слово CW2(C1) запоминается для последующего использования. Отметка TS времени, TS=T0, извлекается из сообщения управления и запоминается. Когда следующее сообщение ECM2 управления принимается мультимедийным модулем, мультимедийный модуль извлекает отметку T1 времени. Второе сообщение ECM2 управления обрабатывается для того, чтобы извлечь контрольные слова, использовать первое из них CW1(C2) и запомнить второе CW2(C2). Затем вычисляется разность между T0 и T1 и получается значение, равное, например, 6 секундам.

Это значение сравнивается с занесенным в память криптопериодом CP, который в нашем примере равен 10 секундам. Поскольку разность T1-T0 между отметками времени меньше, чем криптопериод CP, то значение счетчика CE ошибок увеличивается - в нашем примере на две единицы. Таким образом, это значение равно 2.

При получении следующего управляющего сообщения ECM3, соответствующего первому каналу C1, проверяется значение счетчика CE ошибок. Поскольку это значение равно 2 и, таким образом, меньше, чем ранее заданное пороговое значение 10, временная задержка не вносится. Модуль защиты обрабатывает сообщение, сначала извлекая отметку TS времени, TS=T2. Поскольку криптопериод равен 10 секундам, в результате получится T2-T0=10. Так как T1-T0=6 в данном примере, то T2-T1=4 секундам. Поскольку это значение меньше, чем криптопериод, значение счетчика ошибок увеличивается на две единицы и становится равным 4. Контрольные слова CW2(C1) и CW3(C1) извлекаются из сообщения. В течение этого времени аудио- и/или видеоматериал дешифруется посредством контрольного слова CW2(C1), полученного из предыдущего сообщения управления.

При получении следующего сообщения ECM4 управления модуль защиты также обрабатывает сообщение и возвращает контрольные слова без внесения временной задержки. В это время декодер STB2 использует для дешифрования аудио- и/или видеоматериала контрольное слово CW2(C2), полученное из предыдущего сообщения.

Разность между отметкой времени этого сообщения и предыдущего равна 6 секундам, что меньше, чем криптопериод. Значение счетчика CE ошибок увеличивается на две единицы и имеет, таким образом, значение 6. Контрольные слова CW2(C2) и CW3(C2) извлекаются из сообщения. Когда нужно использовать контрольное слово CW3(C2) для того, чтобы дешифровать аудио- и/или видеоматериал, это контрольное слово будет доступно, так как оно было дешифровано в полученном ранее сообщении ECM4 управления.

Мультимедийный модуль затем получит пятое сообщение ECM5 управления, содержащее контрольные слова CW3(C1) и CW4(C1). В это время контрольное слово CW3(C1) может быть использовано для дешифрования аудио- и/или видеоматериала, так как это контрольное слово было уже передано в предыдущем

сообщении ECM3 управления. Так как разность между отметками времени сообщений ECM4 и ECM5 управления меньше, чем криптопериод, значение счетчика ошибок увеличивается на две единицы и становится равным 8.

Аналогичным образом следующее сообщение ECM6 управления содержит контрольные слова CW3(C2) и CW4(C2), которые могут быть использованы для дешифрования аудио- и/или видеоматериала. Отметка времени, которая содержится в этом сообщении, означает, что счетчик ошибок увеличивается на две единицы и становится равным 10.

Следующее сообщение ECM7 управления содержит контрольные слова CW4(C1) и CW5(C1). Поскольку счетчик ошибок имеет значение 10, которое равно пороговому значению, но не превышает этого значения, сообщение ECM7 обрабатывается, чтобы немедленно возвратить контрольные слова. Это означает, что контрольное слово CW5(C1) будет доступно для аудио- и/или видеоматериала в необходимый момент. Счетчик ошибок будет снова увеличен на две единицы и станет равным 12, превышая, таким образом, пороговое значение.

Следующее сообщение ECM8 управления содержит контрольные слова CW4(C2) и CW5(C2). Это сообщение обрабатывается немедленно, но контрольные слова, которые оно содержит, не будут возвращаться до тех пор, пока не пройдет 12 секунд. Это означает, что при криптопериоде, равном 10 секундам, контрольные слова возвращаются через 2 секунды после окончания криптопериода. В течение этих двух секунд контрольным словом, необходимым для доступа к аудио- и/или видеоматериалу, является слово CW5(C2). Однако это контрольное слово недоступно прежде, чем будет возвращено в декодер. В результате в течение этих двух секунд аудио- и/или видеоматериал недоступен. Результатом на экране пользователя будет скремблированное изображение или равномерно черный или белый экран.

Процесс продолжается таким же образом посредством добавления двух единиц к счетчику ошибок и, соответственно, двух секунд к времени возврата контрольных слов. По этой причине во время обработки следующего сообщения ECM9 управления, аудио- и/или видеоматериал не будет доступен в течение 4 секунд. Для последующих сообщений ECM10, ECM11 и ECM12 время, в течение которого доступ к аудио- и/или видеоматериалу невозможен, равно 6 секундам, 8 секундам и 10 секундам, соответственно. Как легко заметить, когда временная задержка равна удвоенному криптопериоду, содержательный материал более недоступен.

Отметка TS времени, подобная описанной выше, в теории может иметь "разрешение" примерно в секунду или даже несколько секунд, например 4 секунды. Это означает, что разность между двумя значениями отметок времени будет также выражаться в секундах, а не в дробных частях секунд.

Следует отметить, что пример, описанный выше, использует время, заданное в отметках времени. Если мультимедийный модуль, то есть модуль защиты и/или декодер, содержит часовое устройство, то тогда, конечно, можно вычислять разность между двумя моментами времени, полученными от часового устройства, а не между отметками времени. В обоих случаях, однако, принцип изобретения остается тем же.

Использование буферной памяти

Система, как описано выше, содержит ограничение, в случае, когда для запоминания аудио- и/или видеоматериала используется буферная память для того, чтобы компенсировать задержку, вносимую модулем защиты, и делающую ее, таким образом, недействительной.

Один из способов сделать это запоминание бесполезным или по меньшей мере

неэффективным заключается в том, чтобы не фиксировать верхний предел задержки, вызываемой счетчиком ошибок, или фиксировать очень большой предел. Таким образом, поскольку счетчик ошибок увеличивается на два при каждом нестандартном сообщении управления, он будет практически всегда достигать значения, превышающего удвоенный криптопериод или даже большего, таким образом, превышая интервал, вносимый буферной памятью. С этого времени весь аудио- и/или видеоматериал более недоступен. Однако это может дать и отрицательный эффект. В действительности, если счетчик ошибок достигает значительной величины, то необходимо ждать в течение значительного времени после того, как сплиттер был остановлен, для того, чтобы уменьшение счетчика ошибок стало достаточным для корректной работы системы.

Другой способ сделать это запоминание неэффективным заключается в том, чтобы не возвращать контрольные слова, которые, принимая в расчет задержку, должны быть посланы в период, в течение которого содержательный материал больше не шифруется контрольными словами, предположительно посылаемыми модулем защиты. Например, сообщение управления, обозначенное как ECM8 на фиг.2, содержит контрольные слова CW4(C2) и CW5(C2). При значении счетчика ошибок, равном 12, эти контрольные слова должны быть возвращены по окончании криптопериода. В данном случае эти контрольные слова просто не возвращаются. Поскольку контрольное слово CW4(C2) содержится в сообщении ECM6, аудио- и/или видеоматериал может быть дешифрован вплоть до окончания криптопериода, использующего эти контрольные слова. Как только произведено следующее изменение, содержательный материал не будет больше доступен. Однако счетчик ошибок продолжает увеличиваться, поскольку частота отправления сообщений управления не была изменена.

Уменьшение счетчика

В режиме незаконного использования, описанном ранее, ясно, что если два пользователя одновременно имеют доступ к модулю защиты, для того чтобы дешифровывать данные, эти данные быстро станут недоступными. Если один из пользователей прекращает осуществлять доступ к модулю защиты, то для «легального» пользователя может быть снова предоставлен доступ к этому содержательному материалу. Ввиду этого предложенное решение заключается в уменьшении счетчика CE ошибок в соответствии с заранее установленными правилами.

На фиг.4 и 5 схематически проиллюстрированы уменьшение счетчика ошибок, а также его увеличение в соответствии с криптопериодом CP и разностью между отметками времени двух последовательных сообщений ECM управления. В соответствии с одним из возможных правил, каждый раз, когда сообщение ECM управления принято корректно, то есть когда разность между отметками времени данного сообщения и предыдущего сообщения равняется криптопериоду, счетчик ошибок уменьшается на единицу.

В качестве иллюстрации на фиг.4 представлены принятые сообщения ECM управления с зависимостью от времени, тогда как на фиг.5 показано значение счетчика CE ошибок также в зависимости от времени.

Следует отметить, что в данном примере начальное значение счетчика ошибок не равно нулю, а приравнено 2. В связи с тем, что не вносится никакой задержки, пока не превышено пороговое значение, данное начальное ненулевое значение не оказывает отрицательного эффекта на дешифрование. И наоборот, следствием этого будет то,

что в случае мошеннического использования пороговое значение, начиная с которого вносится задержка, достигается быстрее.

Возврат контрольных слов, содержащихся в первом сообщении управления, не задерживается, поскольку пороговое значение не достигнуто. Первое контрольное слово позволяет получить доступ к аудио- и/или видеоматериалу. Второе контрольное слово запоминается декодером. В конце криптопериода мультимедийный модуль получает новое сообщение ECM2 управления. После сравнения отметок времени двух сообщений с криптопериодом первого сообщения ECM1 управления оказывается, что криптопериод равняется разнице между отметками времени, содержащимися в сообщениях управления. В этот момент значение счетчика CE ошибок уменьшается в соответствии с заранее установленным правилом, в данное случае на одну единицу. Таким образом, он принимает значение 1.

Когда мультимедийный модуль принимает следующее сообщение управления, происходит проверка значения счетчика ошибок. Оно равняется 1. Соответственно, временная задержка не применяется. В течение этого времени запомненное ранее контрольное слово, полученное из предыдущего сообщения управления, используется для доступа к аудио/видео содержательному материалу. Значение счетчика уменьшается в соответствии с заранее установленным правилом и принимает теперь нулевое значение.

В проиллюстрированном примере мультимедийный модуль получает новое сообщение ECM4 управления, где разность между отметкой времени этого сообщения и предыдущего сообщения меньше, чем криптопериод. В этот момент значение счетчика увеличивается на две единицы и становится равным 2. Это увеличение может иметь место по двум различным причинам. В соответствии с одной из этих причин пользователь переключает канал (бегство от рекламы). В соответствии с другой причиной использован сплиттер. Как описано выше со ссылками на фиг.3, значение счетчика увеличивается, например, с шагом два.

В примере на фиг.4 и 5 разность между отметками времени двух последовательных сообщений ECM управления меньше, чем криптопериод, вплоть до сообщения управления, обозначенного как ECM8. Значение счетчика ошибок увеличивается каждый раз на два, пока не достигнет значения 12. Как показано на фиг.3, когда значение этого счетчика превышает 10, вносится временная задержка в возврат контрольных слов. Таким образом пользователь не будет иметь доступа ко всему аудио- и/или видеоматериалу. На фиг.4 и 5 во время получения сообщений управления, обозначенных от ECM9 до ECM12, разность между отметками времени равна криптопериоду, и значение счетчика CE ошибок, таким образом, уменьшается на 1 при каждом сообщении. Как только значение этого счетчика достигает 10, временная задержка на обработку отменяется и аудио- и/или видеоматериал становится полностью доступен пользователю.

На фиг.6 проиллюстрирован один из вариантов осуществления изобретения, в соответствии с которым криптопериоды разных каналов отличаются. На этой фигуре также предполагается, что устройство по изобретению используется мошеннически для обслуживания двух декодеров только от одного модуля защиты и что при этом каждый канал получает только одно сообщение управления из двух. Такое использование одного сообщения управления из двух возможно благодаря тому факту, что каждое из этих сообщений содержит два контрольных слова. Поэтому в данном случае все контрольные слова также будут доступны для двух каналов.

В качестве примера предполагается, что криптопериод канала 1, представленного в

верхней части фиг.6, имеет длину 7 секунд. Криптопериод канала 2, представленного на нижней части фиг.6, имеет длину 5 секунд. Будет рассматриваться случай, когда первые сообщения управления каждого канала C1 и C2 принимаются одновременно. Первое сообщение ECM1 (C1) управления канала 1 содержит указание на то, что криптопериод длится 7 секунд. Это сообщение содержит контрольные слова CW1(C1) и CW2(C1).

Первое сообщение управления канала 2 содержит значение криптопериода, равное 5 секундам, наряду с контрольными словами CW'1(C2) и CW'2(C2).

В примере, представленном на фиг.6, следующие сообщения управления каждого канала не используются. Следующее используемое сообщение - это сообщение управления, обозначенное как ECM2(C2). Это сообщение принимается через два криптопериода после первого сообщения ECM1(C2), так что оно рассматривается как допустимое. Значение счетчика ошибок, таким образом, остается на нулевом значении или, возможно, уменьшается.

Следующее сообщение, принимаемое модулем защиты, имеет обозначение ECM2(C1). Оно принимается через два криптопериода после первого сообщения ECM1(C1), а именно через 14 секунд в нашем примере. Это означает, что оно также принимается через 4 секунды после сообщения ECM2(C2), соответствующего каналу C2. Это значение в 4 секунды меньше, чем криптопериод, содержащийся в предыдущем сообщении управления. Значение счетчика ошибок, таким образом, увеличивается на 2 единицы, если применяется то же правило, что и в предыдущем примере. Это значение счетчика CE ошибок, таким образом, равно 2.

Следующее сообщение будет получено через 4 криптопериода канала C2, то есть через (4×5)-(2×7)=6 секунд после последнего принятого сообщения ECM2(C1). Так как это сообщение содержало значение 7 секунд для криптопериода, то сообщение ECM3(C2) рассматривается как некорректное, и значение счетчика ошибок увеличивается на 2. Оно, таким образом, достигает значения 4.

Следующее сообщение ECM3(C1) принимается через (4×7)-(4×5)=8 секунд. Предыдущее сообщение содержало значение криптопериода, относящееся к криптопериоду канала C2, а именно 5 секунд. Промежуток времени в 8 секунд, прошедший после предыдущего сообщения, больше этого значения, равного 5 секундам. Сообщение, таким образом, считается корректным. Значение счетчика CE ошибок будет, таким образом, уменьшено на единицу. Продолжая описанным выше способом, можно показать, что счетчик ошибок будет попеременно увеличиваться и затем уменьшаться. Так как увеличение производится посредством шага величиной две единицы, а уменьшение производится посредством шага величиной единица, значение этого счетчика в случае мошеннического использования будет увеличиваться, как представлено на Фиг.6. Этот счетчик будет принимать значения 0, 2, 4, 3, 5, 4, 6, 5, 7, … до тех пор, пока не превысит порогового значения, начиная с которого создается задержка возврата контрольных слов.

Следует отметить, что случай, когда пользователи дешифруют только одно сообщение управления из двух, как описано со ссылкой на фиг.6, представляет наиболее неблагоприятный случай в отношении выявления мошеннического использования. Легко заметить, что когда мошенники расшифровывают все сообщения ECM управления, значение счетчика ошибок будет увеличиваться быстрее, и возврат контрольных слов модулем защиты будет, соответственно, задержан быстрее.

Модуль защиты и спаренные декодеры

Остальное описание применимо в частности, но не исключительно, в случае, когда модуль защиты и декодер, образующие мультимедийный модуль, спарены. В этом случае каждый из них содержит один ключ из пары ассиметричных ключей, причем эта пара различна и уникальна для каждого модуля вида декодер/модуль защиты. В данной конфигурации, когда активируется мультимедийный модуль, модуль защиты и декодер согласуют сеансовый ключ, который обычно является симметричным ключом. Этот сеансовый ключ используется для шифрования контрольных слов CW, которые были дешифрованы модулем защиты, прежде чем посылаться в декодер. Использование подобного сеансового ключа создает проблему для мошенника, использующего сплиттер. В действительности, поскольку сеансовый ключ для пары модуль защиты/декодер 1 отличается от сеансового ключа для пары модуль защиты/декодер 2, необходимо согласовывать сеансовый ключ для каждого приема сообщения ECM управления для различных каналов. В случае, проиллюстрированном на фиг.3, когда сообщения управления поочередно принимаются для канала C1 и другого канала C2, в соответствии с отдельными вариантами мультимедийного модуля, сеансовый ключ должен согласовываться между каждым получением сообщения ECM управления.

Для того, чтобы осуществить согласование такого сеансового ключа, необходимо выполнить сброс модуля защиты. Это производится с помощью посылки команды сброса в мультимедийный модуль. Такая команда, таким образом, может посылаться между каждым сообщением ECM управления. В данном случае важно, чтобы значение счетчика CE ошибок не сбрасывалось в ноль. Также желательно увеличивать значение счетчика в случае того, что сброс в ноль соответствует мошенническому использованию.

Чтобы осуществить это, модуль защиты запоминает самое последнее время, которое он получил, в энергозависимой памяти. Это время посылается, например, центром управления в виде сообщения управления. При получении команды сброса это время запоминается в энергонезависимой памяти.

Параллельно этому, как уже указывалось, сообщения ECM управления содержат отметку TS времени. Мультимедийный модуль или, точнее, модуль защиты также запоминает промежуток времени, называемый "время ожидания", который, в принципе, больше или равен криптопериоду.

При получении каждого сообщения ECM управления модуль защиты вычисляет разность между отметкой TS времени этого сообщения ECM и самым последним временем, принятым перед последним сбросом в ноль, которое запомнено в энергонезависимой памяти. Если эта разность больше, чем время ожидания, счетчик ошибок может быть сброшен в ноль или любое значение, для которого в возврате контрольных слов нет задержки. Если эта разность меньше, чем время ожидания, это означает, что модуль защиты дешифровал сообщение управления незадолго до сброса в ноль, что может соответствовать конфигурации, в которой используется сплиттер. Счетчик ошибок увеличивается в соответствии с заранее установленным правилом, например, на 3 единицы.

В соответствии с первым вариантом осуществления с момента, в который сообщение управления было обработано «незадолго» до сброса в ноль или последнего запомненного времени, то есть в промежуток времени меньший, чем время ожидания, вносится временная задержка. Это избавляет от запоминания значения счетчика ошибок в энергонезависимой памяти. Вместо этого в случае «легального» сброса в ноль по техническим причинам добросовестный пользователь должен ждать

пока пройдет временная задержка, прежде чем сможет получить доступ к аудио- и/или видеоматериалу. Более того, если в течение этого времени будет переключен канал, то значение счетчика будет увеличено.

В соответствии с другим вариантом осуществления значение счетчика ошибок хранится таким образом, что команда сброса не приводит к сбросу счетчика ошибок в ноль. Напротив, это значение сохраняется таким, каким оно было перед сбросом в ноль. Подобным образом команда сброса между каждым сообщением ECM управления быстро предотвратит доступ к аудио- и/или видеоматериалу. И наоборот, случайный сброс в ноль не будет предотвращать доступ к аудио- и/или видеоматериалу, пока достаточное число сообщений управления было обработано корректно между двумя последовательными сбросами в ноль. Для того чтобы предотвратить какой-либо накопительный эффект в нормальных условиях, если промежуток времени между первой обработкой сообщения управления (после сброса в ноль) и временем последней обработки перед сбросом в ноль достаточно большой (например, несколько часов), то счетчик ошибок будет сброшен в ноль. Время, необходимое для того, чтобы произвести сброс счетчика в ноль, может быть определено заблаговременно и называется временем бездействия.

Следует отметить, что существуют модули защиты, называемые мультисеансовыми, которые способны запомнить несколько сеансовых ключей. В случае стандартного использования для диалога с мультимедийным модулем, или даже с узлом дешифрования содержательного материала, который может размещаться в том же устройстве, может предусматриваться каждый сеансовый ключ.

При доступе к модулю защиты одним из блоков дешифрования будет добавлен опознавательный указатель. Модуль защиты будет обрабатывать это сообщение в среде, относящейся к этому блоку и содержащей сеансовые ключи (если функционирует спаривание), другие опознавательные данные (права, кредит) и данные, позволяющие выявить мошенническое использование, как это было описано выше. В частности это касается счетчика ошибок, отметки времени последней обработки сообщения управления и значения криптопериода.

Таким образом, один и тот же модуль защиты может работать с несколькими блоками дешифрования, проверяя, что общее число декодеров, связанных с этим модулем, не превышает установленного предела. Этот предел может быть установлен в соответствии с параметрами пользователя.

Увеличение/уменьшение с различными скоростями

В показанных примерах значение счетчика увеличивается быстрее, чем уменьшается. Оно увеличивается, например, на две единицы, когда разность между отметками времени двух последовательных сообщений управления меньше, чем криптопериод. Оно увеличивается на три единицы после каждого сброса в ноль, рассматриваемого как некорректный, в то время как уменьшается только на единицу после каждого корректного приема. Это делает возможным избежать отдельных случаев, в которых, используя сброс в ноль и корректную обработку сообщений управления, можно удерживать значение счетчика ошибок в диапазоне, в котором мошенники могут всегда или почти всегда иметь доступ к аудио- и/или видеоматериалу.

В соответствии с другим вариантом можно предусмотреть, чтобы уменьшение производилось быстрее, чем увеличение.

Длительность задержки

Как было показано ранее, обычно предусматривается внесение задержки, когда

значение счетчика ошибок достигает определенного порогового значения. Выше этого порогового значения задержка может быть пропорциональна содержимому счетчика, или может увеличиваться пошагово, или может быть фиксированной. Обычно эта задержка делается для того, чтобы предотвратить доступ к части аудио- и/или видеоматериала в течение некоторого времени мошеннического использования, а затем и ко всему аудио- и/или видеоматериалу после более продолжительного периода мошеннического использования.

В примерах, описанных выше, указано, что продолжительность криптопериода сообщения управления извлекается вместе с его отметкой времени, и затем во время получения следующего сообщения управления производится проверка для подтверждения того, равна разность между отметкой времени этого сообщения и отметкой времени предыдущего сообщения криптопериоду или меньше него. Это означает, что криптопериод и отметка времени первого сообщения должны быть запомнены.

В соответствии с одним из вариантов можно вычислять разность между отметками времени двух последовательных сообщений ECM1, ECM2 управления и проверять, является ли эта разность равной или меньшей, чем криптопериод, извлеченный из второго принятого сообщения ECM2. У такого подхода есть преимущество, заключающееся в том, что не требуется запоминать криптопериод и тем самым можно сберечь память.

В примерах, описанных выше, значение счетчика ошибок может заключаться между 0 и пороговым значением, например 10, или же может превышать это пороговое значение. Если это значение между 0 и пороговым значением, то временной задержки нет. Если пороговое значение превышается, то вносится задержка. Ясно, что можно ограничить максимальное значение счетчика, что позволит ввести ограничение на количество корректных последовательных сообщений, которые должны быть расшифрованы, для того чтобы значение счетчика снова стало меньше порогового значения.

В соответствии с одним из вариантов можно обратить направление счетчика, что означает, что после каждой корректной операции дешифрования счетчик увеличивается, в то время, как во время мошеннического использования счетчик уменьшается. В этом случае временная задержка вносится, когда счетчик содержит значение, заключенное между 0 и пороговым значением, а если значение счетчика превышает это пороговое значение, то временная задержка не вносится.

В описанных примерах упоминается использование двух декодеров с одним модулем защиты. При мошенническом использовании, конечно, можно подключить более чем два декодера к модулю защиты через сплиттер. Согласно изобретению это заблокирует доступ к аудио- и/или видеоматериалу даже еще быстрее, поскольку счетчик ошибок будет увеличиваться соответственно быстрее.

Формула изобретения

1. Способ управления доступом к данным, зашифрованным посредством контрольных слов (CW), получаемых модулем защиты в сообщениях (ECM) управления и возвращаемых в модуль (STB) обработки зашифрованных данных, содержащий следующие шаги:

получение первого сообщения (ECM1) управления, содержащего, по меньшей мере, одно контрольное слово (CW) и отметку (TS) времени;

получение второго сообщения (ECM2) управления, следующего за первым

сообщением (ECM1) управления, причем второе сообщение управления содержит, по меньшей мере, одно контрольное слово (CW) и отметку (TS) времени;

определение продолжительности отрезка времени, соответствующего разности между отметками (TS) времени двух последовательных сообщений (ECM1, ECM2) управления;

увеличение значения счетчика (CE) ошибок в случае, если продолжительность отрезка времени меньше предварительно заданной продолжительности (CP);

уменьшение значения счетчика (CE) ошибок в случае, если продолжительность отрезка времени равна или превышает предварительно заданную продолжительность;

возврат контрольного слова (CW) в модуль (STB) обработки по прошествии времени, которое зависит от значения счетчика (CE) ошибок.

2. Способ по п.1, отличающийся тем, что значение предварительно заданной продолжительности содержится, по меньшей мере, в одном сообщении (ECM1, ECM2) управления.

3. Способ по п.1, отличающийся тем, что значение предварительно заданной продолжительности содержится в сообщении (EMM) авторизации.

4. Способ по п.3, отличающийся тем, что значение предварительно заданной продолжительности является общим для нескольких устройств, на которые передают зашифрованные данные.

5. Способ по п.1, отличающийся тем, что значение предварительно заданной продолжительности равно продолжительности отрезка времени, в течение которого данные шифруют одним контрольным словом (CW).

6. Способ по любому из пп.1-5, отличающийся тем, что первое сообщение (ECM1) управления включает одну отметку (TS) времени, второе сообщение (ECM2) управления включает другую отметку (TS) времени, а отрезок времени, отделяющий два последовательных сообщения управления, соответствует разности между указанными отметками (TS) времени двух сообщений управления.

7. Способ по любому из пп.1-5, отличающийся тем, что модуль защиты и/или модуль обработки содержит часовое устройство, при этом отрезок времени, отделяющий два последовательных сообщения управления, соответствует разности между моментом получения первого сообщения (ECM1) управления и моментом получения второго сообщения (ECM2) управления, причем указанные моменты определяют посредством часового устройства.

8. Способ по п.1, отличающийся тем, что время ожидания равно нулю в случае, когда значение счетчика (CE) ошибок меньше предварительно заданного порогового значения.

9. Способ по п.1, отличающийся тем, что увеличение значения счетчика (CE) ошибок производят в соответствии с заранее установленными правилами.

10. Способ по п.1, отличающийся тем, что уменьшение значения счетчика (CE) ошибок производят в соответствии с заранее установленными правилами.

11. Способ по п.9 или 10, отличающийся тем, что заранее установленные правила для увеличения значения счетчика (CE) ошибок и уменьшения значения счетчика (CE) ошибок различны.

12. Способ по п.11, отличающийся тем, что увеличение значения счетчика (CE) ошибок производят быстрее, чем уменьшение.

13. Способ по п.1, отличающийся тем, что в случае перезапуска модуля защиты дополнительно содержит следующие шаги: определение времени, соответствующего последнему времени, полученному мультимедийным модулем; определение времени

получения нового сообщения (ECM) управления; вычисление разности между указанными двумя временами; увеличение значения счетчика (CE) ошибок в случае, если эта разность меньше предварительно заданного времени ожидания.

14. Способ по п.13 отличающийся тем, что в случае, если разность между двумя временами больше предварительно заданного времени бездействия, то перезапускают счетчик (CE) ошибок.

15. Устройство для управления доступом к данным, зашифрованным посредством контрольных слов (CW), получаемых модулем защиты в сообщениях (ECM) управления и возвращаемых в модуль (STB) обработки зашифрованных данных, содержащее

средства получения первого сообщения (ECM1) управления, содержащего, по меньшей мере, одно контрольное слово (CW);

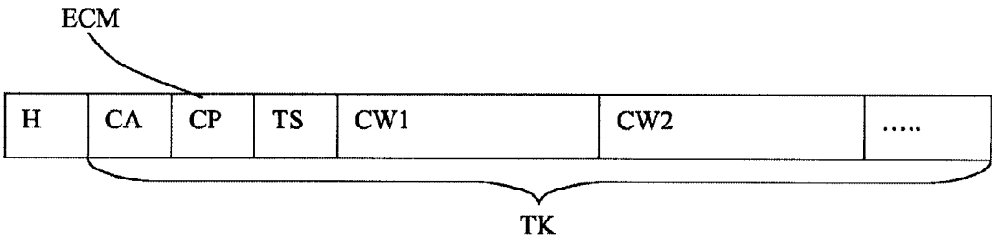
средства получения второго сообщения (ECM2) управления, следующего за первым сообщением (ECM1) управления, причем второе сообщение управления содержит, по меньшей мере, одно контрольное слово (CW);

средства определения продолжительности отрезка времени, отделяющего два последовательных сообщения (ECM1, ECM2) управления;

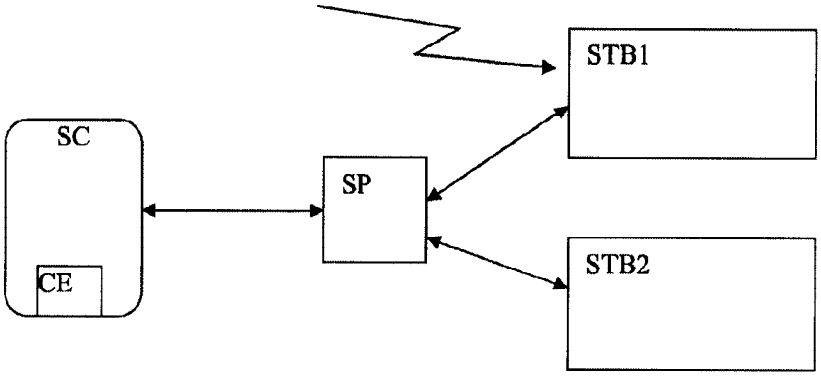
средства увеличения значения счетчика (CE) ошибок в случае, если продолжительность отрезка времени меньше предварительно заданной продолжительности (CP);

средства уменьшения значения счетчика (CE) ошибок в случае, если продолжительность отрезка времени равна или превышает предварительно заданную продолжительность.

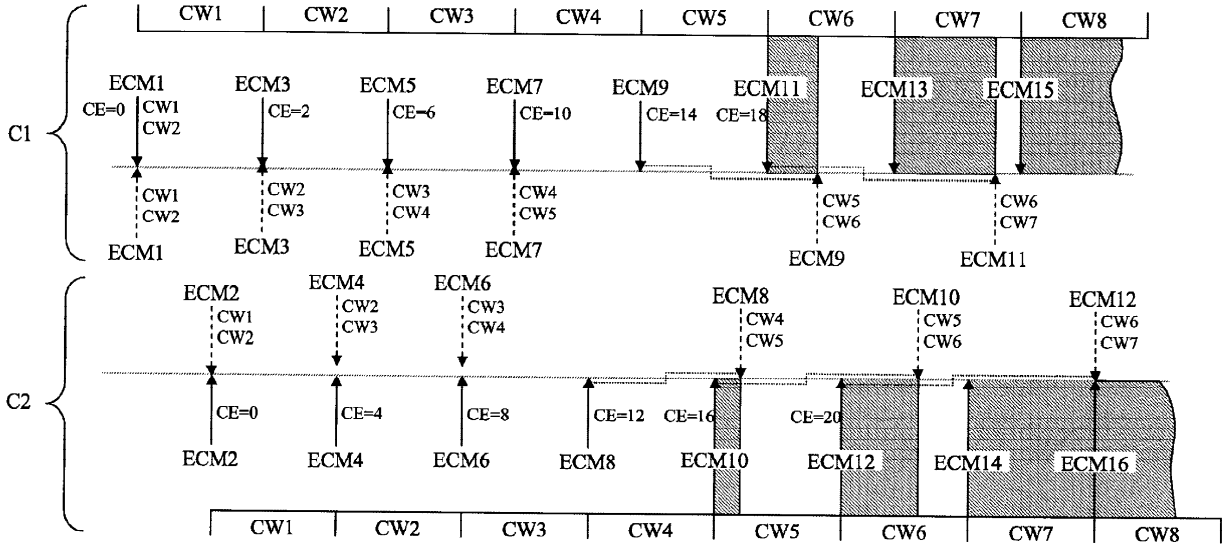
16. Устройство по п.15, отличающееся тем, что дополнительно содержит средства возврата контрольного слова (CW) в модуль (STB) обработки по прошествии времени, зависящего от значения счетчика (CE) ошибок.



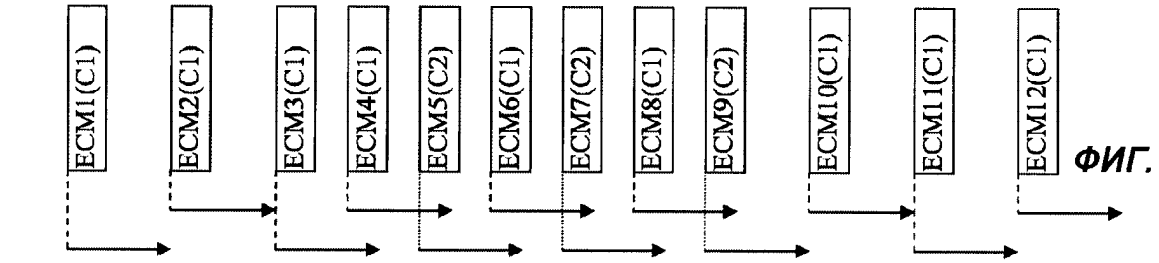
ФИГ. 1



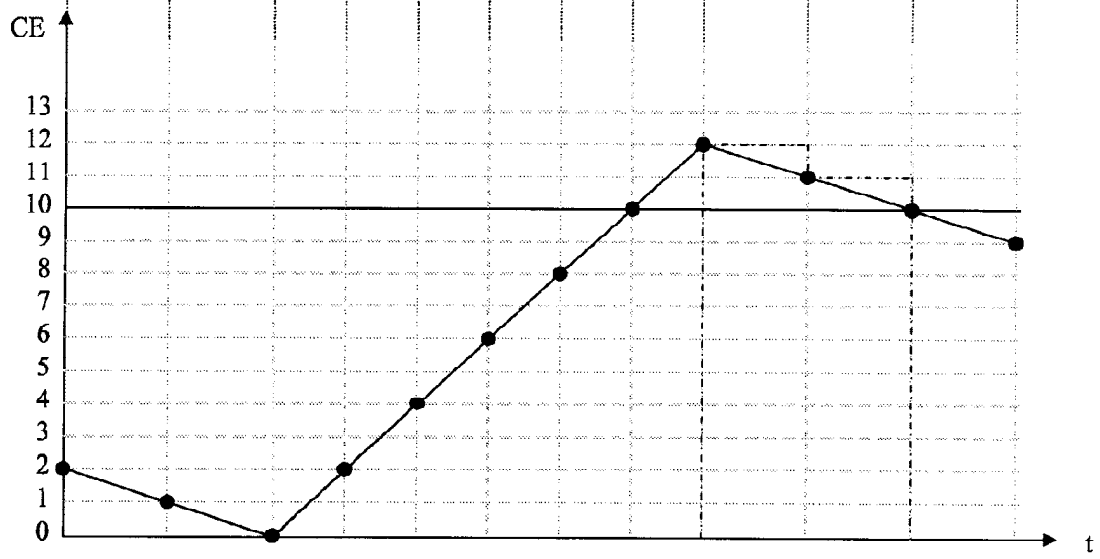
ФИГ. 2



ФИГ. 3


ECM1(C1)
ECM2(C1)
ECM3(C1)
ECM4(C1)
ECM5(C2)
ECM6(C1)
ECM7(C2)
ECM8(C1)
ECM9(C2)
ECM10(C1)
ECM11(C1)
ECM12(C1)
t

ФИГ. 4


CE
13
12
11
10
9
8
7
6
5
4
3
2
1
0
t

ФИГ. 5