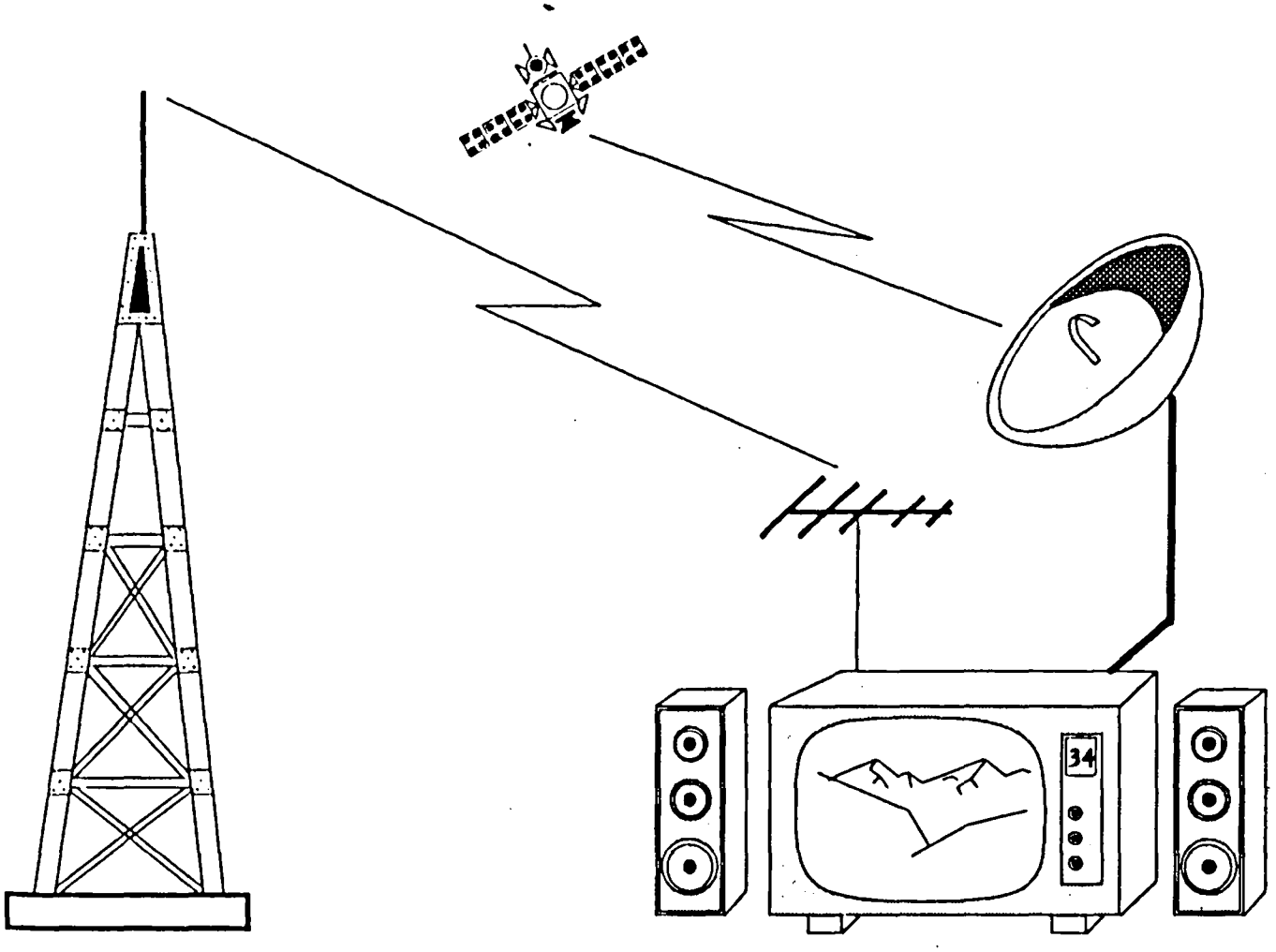
МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

РЕКОМЕНДАЦИИ МККР, 1992 г.

(Новые и пересмотренные на 15 сентября 1992 г.)



Серия RBT

ВЕЩАТЕЛЬНАЯ СЛУЖБА (ТЕЛЕВИДЕНИЕ)

МККР МЕЖДУНАРОДНЫЙ КОНСУЛЬТАТИВНЫЙ КОМИТЕТ ПО РАДИО

ISBN 92-61-04589-8

Женева, 1992 г.

Recommendation 810 (1992)

Conditional-access broadcasting systems [Russian version]

Extract from the publication:
CCIR Recommendations: RBT series: Broadcasting Service (Television)
(Geneva: ITU, 1992), pp. 153-165

РЕКОМЕНДАЦИЯ 810

РАДИОВЕЩАТЕЛЬНЫЕ СИСТЕМЫ С УСЛОВНЫМ ДОСТУПОМ

(Вопрос 37/11)

(1992)

МККР,

учитывая,

a) что в некоторых странах растет потребность в защите программ радиовещания от неразрешенного приема;

b) что одним из эффективных путей обеспечения такой защиты является реализация условного доступа к радиовещательным системам;

c) что образцы радиовещательных систем с условным доступом уже разработаны и эксплуатируются в наземном, кабельном и спутниковом телевидении, а также в службах телетекст и передачи данных;

d) что было бы желательно ограничить число различных систем с условным доступом, учитывая, тем не менее, различные требования разнообразных радиовещательных служб и систем передачи;

e) что применение в приемниках как можно больше общих элементов условного доступа в конечном счете предоставит самые широкие возможности населению в отношении доступа к защищенным службам при меньшей стоимости оборудования;

f) что владельцы авторских прав, изготовители программ и поставщики услуг служб желают обеспечить высокую степень защиты сетей распределения и вещания для того, чтобы иметь возможность защитить свои программы с помощью условного доступа,

рекомендует,

чтобы системы условного доступа в радиовещательных службах:

— обеспечивали высокую степень защиты;

— обладали максимально возможным количеством общих элементов в приемниках, и

— разрабатывались в соответствии с основными принципами, содержащимися в приложении 1.

ПРИЛОЖЕНИЕ 1

Основные принципы условного доступа в радиовещательных системах

1. Введение

Изложенные ниже принципы, в общем, применимы и к современным, и будущим телевизионным службам, службам звукового радиовещания, а также к службам телетекст и радиовещательной передачи данных. Эти принципы применимы к вещанию/распределению для пользователей по наземным, кабельным, спутниковым и другим средствам передачи, в том числе с предварительной записью*.

2. Элементы системы условного доступа

Имеются два различных, и во многих случаях независимых, элемента системы условного доступа, причем каждый из них связан с различными информационными процессами. Оба эти элемента описываются ниже и определяются в дополнении 1.

---

* Примеры реализации систем условного доступа, специально разработанных для спутникового телевизионного вещания во Франции, Соединенном Королевстве и в Японии, приведены в дополнении 2.

2.1 Скремблирование

Это — процесс обработки содержания сигнала в службе таким образом, чтобы он не представлял никакой ценности для неразрешенного пользователя. Процесс заключается в изменении некоторых характеристик сигнала с помощью системы условного доступа на передающем конце линии. Содержание сигнала в службе может быть в виде радиовещательной программы или в другом виде, например в виде данных.

2.2 Управление доступом

Это передача такой информации, которая позволяет разрешенному пользователю дескремблировать сигналы данной службы. Предоставление такой информации управляется системой условного доступа.

При передаче сигналов между передатчиком и приемником(ами) эта информация вводится в виде сигналов засекречивания, уплотняемых совместно с собственно основным сигналом.

На приемном(ых) конце(ах) линии передачи эти сигналы обрабатываются системой условного доступа, чтобы управлять процессом дескремблирования сигнала в разрешенном(ых) приемнике(ах).

3. Требования, которым должна удовлетворять система управления условным доступом

3.1 Качество

Процессы скремблирования и дескремблирования не должны влиять на восприятие качества принимаемого изображения, сигналов звукового сопровождения и данных.

3.2 Скрытность

Скрытность системы определяется как степень затруднения, с которым встречается неразрешенный пользователь при попытке осуществить доступ к службе. Скрытность может определяться двумя аспектами, представляющими два различных характера затруднений при рассекречивании:

— *дескремблирование сигнала при незнании характера процесса управления доступом.* Возможность дескремблирования в этом случае зависит от характера службы и метода скремблирования. Будущие службы вещательной передачи телевидения, звука и данных будут, по-видимому, в основном иметь цифровой характер, что позволит обеспечить высокую скрытность процесса скремблирования;

— *получение ключа управления доступом* недозволенным способом.* Это зависит от степени скрытности используемых алгоритмов и от способа распределения ключа.

3.3 Универсальный условный доступ

Доступ возможен для любого разрешенного пользователя, соблюдающего правила доступа, с помощью общего или универсального алгоритма скремблирования. Универсальный условный доступ попросту означает, что для удовлетворения требованиям, устанавливаемым изготовителем программ, поставщиком или распределителем услуг, любой пользователь получает доступ к службе с помощью общего для всех процесса и оборудования, выполняя общие для всех и удобные для пользователя правила и процедуры. Такой подход будет способствовать более широкому применению систем условного доступа, использующих простые, недорогостоящие и гибкие абонентские устройства. Универсальный условный доступ означает, что дескремблирование будет одинаковым для всех приемников и будет основано на применении стандартного алгоритма скремблирования, независимо от используемых средств передачи сигналов, при этом сохраняется возможность конкуренции в конкретном применении систем различных фирм.

3.4 Защита содержания информации на всем протяжении ее передачи (защита от начала до конца)

Защита информации от начала до конца в службах радиовещательного распределения телевидения, звука и данных заключается в защите содержания (программ и т.п.), а также информации, относящейся к управлению доступом (управление или данные) от самого начала сигнала до самого конца на всех участках распределения. Защита начинается в точке возникновения сигнала и поддерживается вплоть до точки его воспроизведения пользователю*. Это позволяет избежать раскрытия сигналов систем передачи с высокой скрытностью с помощью очень легко осуществимой записи содержания программ в домашних условиях.

. Таким образом, независимо от точки возникновения сигнала, система защиты от начала до конца обеспечивает такие условия, что информация, закрытая в самом начале, остается таковой на всех промежуточных участках распределительной системы до тех пор, пока она не достигнет приемника, в котором доступ зависит от удовлетворения пользователем условий, устанавливаемых изготовителем программ или распределителем службы. На транзитных участках и в накопительных (запоминающих) устройствах закрытое содержание или прочая информация никогда не появляются в открытой форме в какой-либо точке или в какой-либо момент времени до тех пор, пока доступ к ним не будет осуществлен разрешенным пользователем. Таким образом, любая передача и запоминание содержания будут осуществляться «целиком». Это не накладывает никаких ограничений на возмож-

* Определение см. в дополнении 1.

ность применения любыми промежуточными пользователями своих собственных средств защиты в дополнение к уже имеющемуся закрытию информации при условии, что при этом сохраняется ее целостность как таковой. Поскольку содержание информации, поступающей из какой-либо точки ее возникновения, может быть скремблировано только один раз, то такое скремблированное содержание передается как нечто целое. При этом ключ скремблирования, посылаемый в соответствии с правилами распределения ключа, обычно подвергается засекречиванию ключом распределения и направляется в приемник пользователя для хранения в нем в засекреченной форме совместно с ключами скремблирования для различных источников информации.

3.5 Виды доступа

Система условного доступа будет более эффективна, если будет иметься достаточное количество видов доступа.

Например:

— доступ в интервале времени — разрешение на пользование начинается в начале какой-либо передачи и заканчивается при ее окончании;

— доступ к программе или к элементу службы — доступ к какому-либо конкретному элементу службы, независимо от того, используется ли он полностью или нет;

— доступ с оплатой за службу (обычно называемой «платой за просмотр») — оплата или использование кредита пропорционально длительности использования и/или стоимости соответствующей службы.

Виды доступа должны быть различными в зависимости от нескольких переменных параметров, например:

— время;

— различные части службы;

— группы пользователей, для которых предназначена передача.

3.6 Стандартизация оборудования

Для обеспечения максимальной экономии при производстве приемного оборудования и упрощения управления и технического обслуживания:

— общее оборудование должно быть стандартизовано таким образом, чтобы имелась возможность осуществления как можно большего количества вариантов служб;

— схема построения приемника пользователя должна быть гибкой, для того чтобы имелась возможность применения устройств шифровки и дешифровки ключа распределения и ключа последовательности, а также устройств шифровки и дешифровки ключа рассекречивания в различных формах — от встроенных или отделяемых от приемника блоков процессоров до портативных персональных модулей (или персональных кодовых карточек) закрытой информации с встроенными секретными ключами последовательности и логическими кодовыми устройствами персонального опознавания.

3.7 Организация доступа

Определение условного доступа основано на формальной концепции *права* на доступ, которое может быть осуществлено в различных формах. Обладание таким правом дает его владельцу *разрешение* на доступ к соответствующей службе. Следует избегать неэкономного использования ресурсов из-за накладных расходов при передачах или управлении.

3.8 Исключение ухудшения качества службы

Следует указать на два наиболее значительных вида ухудшения качества службы:

— ухудшение качества полученной в конечном счете услуги за счет процесса скремблирования/дескремблирования;

— ухудшение качества за счет ошибок или недостоверного приема данных, относящихся к управлению доступом.

3.9 Взаимодействие с цифровой обработкой сигналов

Следует отметить, что процессы скремблирования могут существенно ограничить возможности дальнейшей обработки сигнала, в том числе уменьшить битовую скорость передачи.

3.10 Управление содержанием

Система должна обладать возможностью обеспечивать различные уровни разборчивости сигнала по выбору изготовителя программы в качестве одного из элементов его рыночной стратегии.

4. Общее описание системы условного доступа

4.1 Общие положения

Система условного доступа требует *скремблирования* информации до ее передачи. Этот процесс осуществляется с помощью скремблирующей последовательности, получаемой от *генератора псевдослучайных сигналов*.

Для восстановления первоначального сигнала процесс дескремблирования на приемном конце требует использования той же самой последовательности (в данном случае дескремблирующей последовательности).

Для обеспечения генерирования этой последовательности и сохранения синхронизма между процессами на передаче и на приеме производится включение генератора псевдослучайного потока битов с помощью *инициализирующего слова*.

Подробная диаграмма прохождения этого процесса представлена на рис. 1.

4.2 Инициализирующее слово

Условный доступ к какому-либо элементу службы, по сути дела, эквивалентен условному доступу к инициализирующему слову, которое имеет две составляющих: *управляющее слово* и *инициализирующий модификатор*.

4.3 Управляющее слово

Управляющее слово является основным элементом обеспечения скрытности. Форма его выбирается произвольно и может меняться во время работы службы для увеличения степени скрытности.

Управляющее слово передается приемнику следующим образом:

— на передающем конце: в соответствии с используемым видом доступа алгоритм шифрования выдает управляющее слово в зашифрованной форме, которое уплотняется с самим сигналом. Таким образом получается сообщение проверки права на доступ;

— на приемном конце: оборудование управления доступом с помощью обратного алгоритма восстанавливает управляющее слово, если выполнены все прочие условия доступа. Модуль(и) скрытности приемника(ов) может(гут) также производить криптографическую проверку суммированием и подтверждение для обеспечения полноты приема.

4.4 Инициализирующий модификатор

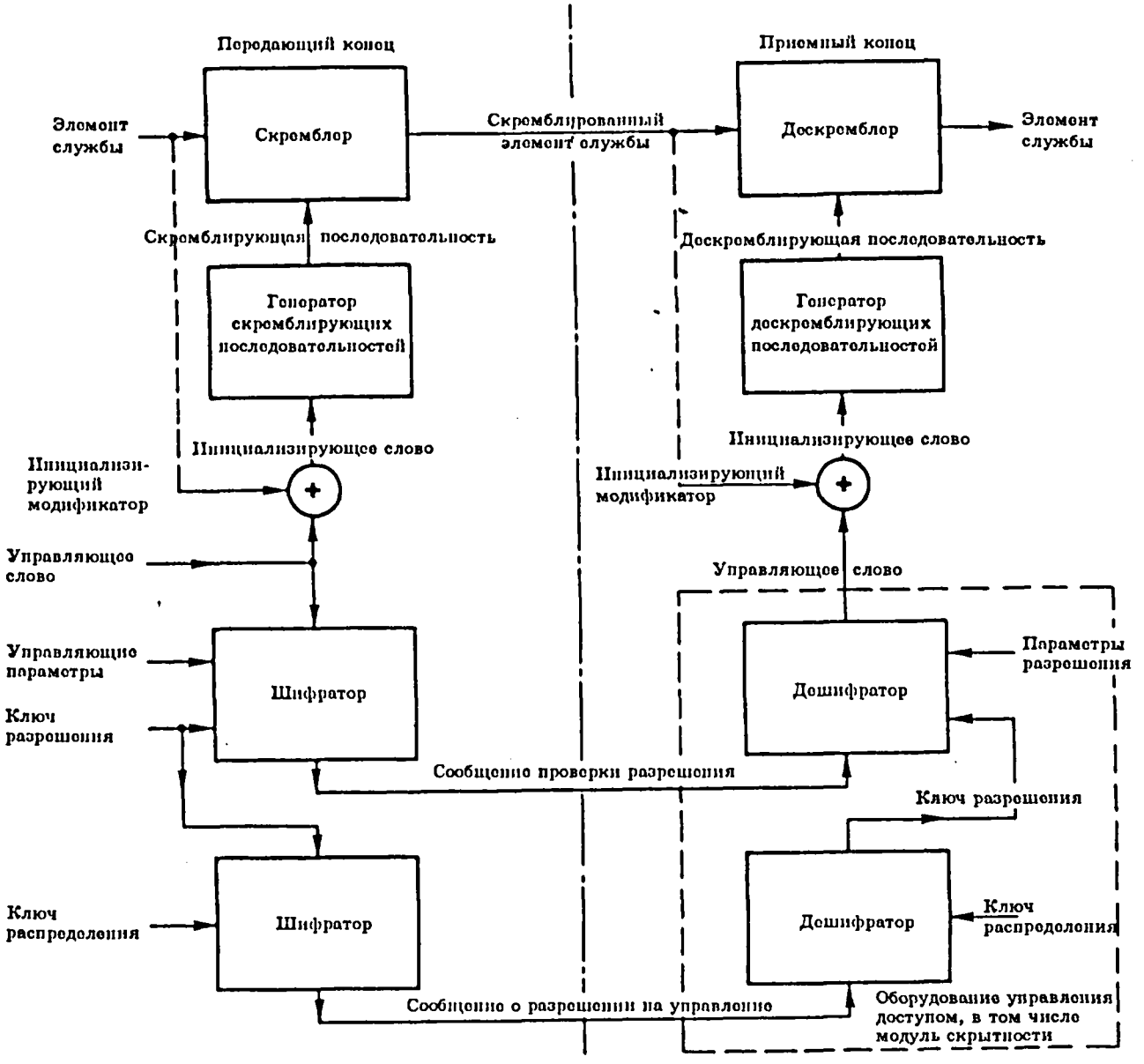
Инициализирующий модификатор предназначен, для того чтобы при обеспечении скрытности использовались довольно короткие скремблирующие последовательности при исключении необходимости в слишком частом определении управляющего слова. Следовательно, использование различных инициализирующих модификаторов для каждой структурной единицы скремблируемой информации требует довольно частой смены инициализирующего слова. Инициализирующий модификатор также передается пользователю в виде части вещательного сигнала.

4.5 Индекс управляющего слова

При работе службы с сегментной организацией необходимо обрабатывать несколько соответствующих управляющих слов. Они различаются друг от друга посредством *индексов*. Индекс управляющего слова, используемый для обеспечения доступа к единице скремблированной информации, должен выделяться из передаваемого сигнала.

РИСУНОК 1

Функциональное описание системы условного доступа



Примечание 1. — Для большей ясности на данном рисунке изображены два шифратора и два дешифратора. На практике, если алгоритмы шифрования, управляемые соответственно ключом разрешения и ключом распределения, одинаковы, то необходимы только один шифратор и один дешифратор.

Примечание 2. — На приемном конце операции скрытности осуществляются внутри модуля(лей) скрытности.

5. Сообщения проверки разрешения на доступ

Каждое из таких сообщений состоит из:

— индекса управляющего слова;

— указателя изменения управляющего слова: изменение состояния означает изменение значения управляющего слова;

— *указателя разрешения*, который определяет ключ разрешения, находящийся в приемном модуле скрытности, к которому адресуется данное сообщение;

— *управляющего параметра*, который указывает значение (например, даты, цены и т.п.) для сравнения со значениями границ, установленных для этих величин в приемном модуле скрытности, называемых *параметрами разрешения*;

— зашифрованного управляющего слова.

Для дескремблирования какой-либо единицы информации приемник должен прежде всего выделить управляющее слово из сообщения проверки разрешения на доступ, в котором указан и соответствующий индекс.

Для повышения эффективности сообщения проверки разрешения на доступ, относящиеся к одному и тому же управляющему слову, но соответствующие либо различным группам пользователей, либо различным типам оборудования управления доступом, должны группироваться под одним и тем же индексом. Система использования индексов, описанная выше, облегчает заблаговременную передачу проверочных сообщений о разрешении, хотя это и не является ее единственной задачей.

В оборудовании условного доступа создается таблица действующих управляющих слов, которая обновляется с помощью сообщений проверки разрешений, независимо от скремблированных данных. Для опознавания правильного управляющего слова устройство дескремблирования передает соответствующий индекс в оборудование управления доступом. Поддержание такой таблицы является одной из операций, производимых между устройством дескремблирования и оборудованием управления доступом.

6. Сообщение об управлении разрешением на доступ

В результате обработки сообщения об управлении разрешением на доступ получается подтверждение права или дается право на доступ. Эта обработка осуществляется в модуле скрытности и связана с проведением криптографических вычислений с использованием *ключа распределения*. Этот ключ распределения используется для шифровки и дешифровки сообщений и/или ключей разрешений, относящихся к отдельным приемникам. Соответствующая криптограмма представляет собой сигнал подтверждения и передается как часть сообщения об управлении разрешением на доступ.

В радиовещательных системах с условным доступом сообщение об управлении доступом может передаваться как радиовещательный сигнал. Такой способ передачи известен как «радиоадресование». Отрезок времени, отводимый на распределение ключей по радио, может быть значительно уменьшен путем применения принципов совместной шифровки ключей. Сообщения об управлении доступом могут передаваться также и другими средствами связи.

Пример работы системы может быть описан следующим образом. В случае оплаты доступа (за единицу времени или за программу) сообщение об управлении может нести в себе зашифрованный код стоимости, передаваемый как часть сигнала данной службы. Сведения о кредите могут содержаться в приемнике и могут иметь вид зашифрованных денежных обозначений, которые передаются как часть службы радиоадресования. В другом случае кредит может иметь форму занесенных в память денежных обозначений, распределяемых другими средствами. Оплата заключается в уменьшении кредита, находящегося в памяти, в соответствии с принятым кодовым сообщением о стоимости.

7. Оборудование управления доступом

Данное оборудование включает модуль скрытности, в который поступают сообщения проверки разрешения. Этот модуль может иметь вид встроенных или отделимых от оборудования устройств (причем в обоих случаях должна иметься возможность ввода алгоритмов дешифровки). В первом из этих вариантов разрешение на доступ относится к некоему приемнику, в то время как в варианте отделимых от оборудования устройств (например, персональных кодовых карточек) доступ можно не ограничивать каким-то определенным телевизионным приемником. Оборудование управления доступом связано с дескремблером через стандартное физическое промежуточное устройство (интерфейс) и логические цепи. Стандартизация такого промежуточного устройства имеет важное значение, для того чтобы имелась возможность:

— независимости функций модуля скрытности и дескремблирования, осуществляемых в приемнике;

— дальнейшего совершенствования оборудования управления доступом.

Если модуль скрытности содержит разрешение с таким же опознавателем, что и указатель разрешения в сообщении проверки разрешения, этот модуль формирует управляющее слово, если, кроме того, управляющие параметры соответствуют условиям принятых параметров разрешения. Они могут включать:

— требования в отношении даты при условии, что даты в управляющих параметрах находятся между датами начала и конца в параметрах разрешения;

— требования в отношении стоимости, при которых разрешение может быть предоставлено только в том случае, если модуль скрытности отметит получение оплаты.

Действия, связанные с модулем скрытности, могут включать три отдельных этапа:

— предварительные инструкции, если таковые имеются (например, пароль, одобрение пользователя и т.п.);

— инструкция по использованию модуля скрытности;

— обработка результатов (например, формирование управляющего слова).

Поскольку могут использоваться разнообразные модули засекречивания, было бы желательно, чтобы оборудование управления доступом не зависело от конкретных действий. Такая независимость может быть достигнута, если оборудование управления доступом воспринимает последовательность инструкций, составленных на определенном языке и передаваемых в рамках конкретных сообщений.

ДОПОЛНЕНИЕ 1

Некоторые термины и определения, связанные с радиовещательными системами с условным доступом

Скремблирование [в радиовещании] (Embrouillage, aleatorizacion)

Изменение характеристик радиовещательного сигнала изображения /звука/ данных с целью предотвращения неразрешенного приема информации в открытой форме. Такое изменение производится в результате определенного процесса, управление которым осуществляется системой условного доступа (на передающем конце линии передачи).

Дескремблирование [в радиовещании] (Desembrouillage, desaleatorization)

Восстановление характеристик радиовещательного сигнала изображения /звука/ данных с целью обеспечения приема информации в открытой форме. Такое восстановление производится в результате определенного процесса, управление которым осуществляется системой условного доступа (на приемном конце линии передачи).

Примечание 1. — Термины «скремблирование» и «дескремблирование» применимы как к аналоговым, так и к цифровым сигналам.

Примечание 2. — Эти термины не должны использоваться для описания процессов, таких как рассеяние энергии несущей в спутниковых системах.

Условный доступ

Доступ пользователя к защищенной службе путем взаимодействия через приемный модуль скрытности, модуль засекречивания или декодер. Если в ходе работы выполняются все условия доступа, то пользователь получает разрешение, ключ скремблирования начинает действовать и содержание передачи дескремблируется.

Опознавание пользователя, подтверждение об оплате, о наличии службы или других параметров управления программой приводят в действие ключ шифровки/дешифровки для завершения процесса получения разрешения.

Управление условным доступом

Функция управления условным доступом на передающем конце линии передачи обеспечивается генерированием сигналов управления скремблированием и «ключей», связанных с работой соответствующей службы.

Функция управления условным доступом на приемном конце линии передачи обеспечивается оборудованием сигналов управления дескремблированием с использованием «ключей», связанных с работой соответствующей службы.

Примечание 1. — Слово «ключ» используется в приведенных выше определениях в общем смысле, соответствующем смыслу, придаваемому этому слову в Вопросе 37/11.

Шифрование и *дешифрование* — это термины, используемые для описания методов защиты (и интерпретации) некоторой информации в «сообщениях, связанных с доступом», которые передаются от передающего конца линии передачи к приемному концу для осуществления функций управления условным доступом.

Точка возникновения

Это — точка в системе распределения, в которой программа или другая информация впервые становится сигналом в своем окончательном радиовещательном/распределительном формате. Такая точка отмечает начало защищенного участка линии. Вводимая информация может иметь любую форму, причем не обязательно пригодную для человеческого восприятия. Содержание входного сигнала само по себе не должно быть понятным.

Точка воспроизведения

Это — точка, в которой программа или другая информация в последний раз имеет форму сигнала распределительной системы, прежде чем она примет форму, пригодную для человеческого восприятия на экране приемника или в громкоговорителе. Данная точка отмечает конец защищенного участка линии.

Примечание 1. — Владельцы авторских прав, поставщики услуг и распределители образуют обширную сеть многочисленных возможных точек возникновения потока информации, предназначенного для пользователей, а следовательно, и направляемого к ним потока скремблированных сигналов и зашифрованных ключей. Точка возникновения может располагаться у владельца авторских прав или изготовителя программ. На практике большая часть точек возникновения представляет собой просто точки ввода сигнала в любом месте системы, где это удобно по деловым и эксплуатационным соображениям. Поскольку может быть много таких точек ввода сигналов, то каждая из них представляет собой единственную и независимую точку, в которой информация может поддерживаться в любой форме, пригодной для передачи пользователю любым способом.

ДОПОЛНЕНИЕ 2

Примеры применения системы условного доступа

Ссылка на приложение 1	Страничные системы телетекст		Системы вещательной передачи данных		Семейство МАК/пакет (С-МАК/пакет и Д2-МАК/пакет)	Цифровая поднесущая/НТСЦ
	Система телетекст А	Система телетекст В	Независимые строки для передачи данных в системе телетекст В	Уровни 1—4 системы телетекст С, принятой во Франции		
Процесс скремблирования (§ 4.1)	Комбинация байтов данных с байтами от генератора псевдослучайной последовательности, образованная по правилу «исключающего ИЛИ». Интерпретирующий байт в головном слове определяет, скремблирована информация или нет	Комбинация байтов данных с байтами от генератора псевдослучайной последовательности, образованная по правилу «исключающего ИЛИ». Байты связи в пакете 27 означают, что страница скремблирована	Комбинация байтов данных с байтами от генератора скремблирующей последовательности, образованная по правилу «исключающего ИЛИ». Регулярное появление блоков ключа данных пользователя означает, что служба скремблирована	Комбинация байтов данных с байтами от генератора псевдослучайной последовательности, образованная по правилу «исключающего ИЛИ». Один из байтов инициализирующего модификатора указывает, скремблирована или нет данная группа данных. Группы данных с GT = 0 или 1 не скремблируются	*Изображение:* двойное деление компонента или одинарное деление строки пополам с перестановкой частей при управлении от генератора псевдослучайной последовательности. *Звук:* комбинация битов данных с битами непрерывно сдвигаемой псевдослучайной последовательности, образованная по правилу «исключающего ИЛИ»	*Изображение:* поворот строк, перестановка строк или комбинация обеих способов при управлении от генератора псевдослучайной последовательности. *Звук:* комбинация битов данных с битами непрерывно сдвигаемой псевдослучайной последовательности, образованная по правилу «исключающего ИЛИ»
Генератор псевдослучайной последовательности (§ 4.1)	Комбинация из трех многокаскадных сдвиговых регистров с линейной обратной связью	Использование однонаправленной функции с применением алгоритма шифрованной обратной связи	Генератор скремблирующего потока, использующий дешифрующий алгоритм, соединенный в режиме выходной обратной связи (ИСО DIS 8372)	Комбинация из трех многокаскадных сдвиговых регистров с линейной обратной связью	*Изображение:* два многокаскадных сдвиговых регистра с линейной обратной связью. *Звук:* два многокаскадных сдвиговых регистра с линейной обратной связью, запускающие многокаскадный сдвиговый регистр с линейной обратной связью	Нелинейная комбинация выходов трех многокаскадных сдвиговых регистров с линейной обратной связью (по 13, 11 и 8 каскадов каждый)

ДОПОЛНЕНИЕ 2 *(продолжение)*

Ссылка на приложение 1	Страничные системы телетекст		Системы вещательной передачи данных		Семейство МАК/пакет (С-МАК/пакет и Д2-МАК/пакет)	Цифровая поднесущая/НТСЦ
	Система телетекст А	Система телетекст В	Независимые строки для передачи данных в системе телетекст В	Уровни 1—4 системы телетекст С, принятой во Франции		
Синхронизация генератора псевдослучайной последовательности (§ 4.1)	Первый байт после первой последовательности блока US-X-Y	Первый байт данных пакета 0 обозначения страницы	Первый байт данных пользователя в блоке данных пользователя	Первый байт после инициализирующего модификатора	В начале каждого кадра изображения	Сигнал синхронизации передается как часть кодовой посылки управления кадром звука. Скремблирование сигнала изображения происходит в начале кадра изображения немедленно после сигнала синхронизации; скремблирование сигнала звука начинается со скремблирования кадра звука немедленно после сигнала синхронизации
Инициализирующее слово (§ 4.2)	12 байтов	56 битов ключа страницы	Первоначальной переменной скремблирующего потока является один байт в начале блока данных, повторенный восемь раз	12 байтов	60 битов	32 бита
Управляющее слово (§ 4.3)	8 случайных байтов	56 битов действующего ключа системы	64 бита ключа пользователя	8 случайных байтов	60 случайно выбранных битов или криптограмма 256 кадров цикла	32 бита, выбранных случайно (так же, как и инициализирующее слово)
Инициализирующий модификатор (§ 4.4)	4 байта, следующих за головной частью блока информации	Не применяется	Не применяется	4 байта после головной части группы данных	8 битов счета кадров	Не применяется
Управление содержанием (§ 3.10)	Не применяется	Не применяется	Не применяется	Не применяется	Не применяется	*Изображение:* применяется. *Звук:* не применяется

Сообщения проверки права на доступ (ECM) (§ 5)	Специальные блоки информации, обозначенныеи классификационными номерами FFF и Y_{11} = 1; байт Y_{12} дает индекс управляющего слова. Каждое сообщение вводится последовательностью US-3/F-3/F и содержит: — 3 байта для указателя разрешения; — 3 байта для управляющего параметра; — 16 байтов для шифрованного управляющего слова.	Специальные пакеты включают 22 бита параметров разрешения и управляющих параметров, 112 битов — шифрованное управляющее слово	Один из типов блоков управления несет ключ данных пользователя для всех пользователей, которые имеют соответствующий системный ключ, позволяющий расшифровать его	Группы данных, для которых GT (тип группы данных, см. § 4.1 таблицы 1a в Рекомендации 653) равно 14. Эти группы данных состоят из команд, причем каждая команда опознается опознавателем команд и опознавателем длины команды и состоит из параметров, опознаваемых опознавателем параметров и опознавателем длины параметров; имеется два типа команд: CI = 0: команда модулю скрытности на использование CI ≠ 0: команда на проверку разрешения на доступ, где каждый параметр несет ECM и состоит из: — 3 байтов для принтера разрешения; — 3 байтов для параметров управления; — 16 байтов для зашифрованного управляющего слова	Специальные пакеты в канале опознавания службы. В системе условного доступа для Д2/МАК/пакета, используемого, среди прочих, во французской системе непосредственного спутникового радиовещания TDF1-TDF2; кодирование пакетов производится в соответствии с требованиями, указанными в «Системе условного доступа для семейства МАК/пакет-EUROCRYPT» (Март, 1989 г.). В Соединенном Королевстве, где принят Д-МАК/пакет, Радиовещательная спутниковая служба Британской компании спутникового радиовещания начинает работать на базе «Системы условного доступа, предназначенной для использования с форматом передачи семейства МАК/пакет-EuroCypher»	Пакеты, передаваемые в канале данных в цифровом кадре звука. Предназначение каждого бита известно, однако более подробные данные определяются поставщиком услуги
Индекс управляющего слова § 4.5	Байт Y_{16} скремблированного блока для дескремблирования и байт Y_{12} ECM для обновления	Не применяется	Не применяется		Не применяется	Не применяется

ДОПОЛНЕНИЕ 2 *(продолжение)*

Ссылка на приложение 1	Страничные системы телетекст		Системы вещательной передачи данных		Семейство МАК/пакет (С-МАК/пакет и Д2-МАК/пакет)	Цифровая поднесущая/НТСЦ
	Система телетекст А	Система телетекст В	Независимые строки для передачи данных в системе телетекст В	Уровни 1—4 системы телетекст С, принятой во Франции		
Изменения управляющего слова и указатель (§ 5)	Бит b_8 байта Y_{12} ECM	Действующие и новые ключевые слова, включенные в обозначенный пакет адресации пользователя	Правильное значение ключа определяется путем сравнения с опознавателями ключей, передаваемыми совместно с ключами, и блоками данных, требующими этих ключей	Бит b_8 опознавателя параметра в команде проверки разрешения	Новое управляющее слово передается через каждые 256 кадров и становится действующим управляющим словом при кадровом счете, равном 0	Управляющее слово обновляется сигналом синхронизации. Минимальный интервал для обновления равен 1 с.
Сообщение контроля за правом на доступ (EMM) (§ 6)	В настоящее время право на доступ контролируется с помощью системы Видеотекст через сеть электросвязи	Право на доступ контролируется с помощью радиоадресации приемного оборудования с использованием совместных и отдельных пакетов адресации пользователя	Право на доступ контролируется с помощью радиоадресации модуля управления с использованием совместных или отдельных блоков данных адресации. Блоки данных для радиоадресации уплотняются в том же канале, в котором передаются данные сообщения	Пока не стандартизован. Право на доступ может контролироваться с помощью системы видеотекс через сеть электросвязи	Специальные пакеты в канале опознавания службы (SI). В системе условного доступа для Д2-МАК/пакета, используемого, среди прочих, во французской системе непосредственного спутникового радиовещания TDF1-TDF2, кодирование пакетов производится в соответствии с требованиями, указанными в «Системе условного доступа для семейства МАК/пакет-EUROCRYPT» (Март, 1989 г.).	Пакеты, передаваемые в канале данных. Они могут также распределяться с помощью карточек IC. Предназначение каждого бита известно, однако более подробные данные определяются поставщиком услуги

Сообщение контроля за правом на доступ (ЕММ) *(продолжение)*					В Соединенном Королевстве, где принят Д-МАК/пакет, Британская компания спутникового радиовещания начинает работать на базе «Системы условного доступа, предназначенной для использования с форматом передачи семейства МАКпакет-Euro-Cypher»	
Аппаратура управления доступом (§ 7)	Встроена в приемник и включает считыватель кодовой карточки	Встроена в приемник или функционально выделена по выбору поставщика услуги	Полностью включена в модуль скрытности. Принимает серийные данные от пакетного декодера и обеспечивает дешифровку серийных данных для пользователя	Встроена в приемник и включает считыватель кодовой карточки	Функционально отделена от других частей приемника и подключается с помощью интерфейса, подлежащего стандартизации	Функционально отделена от других частей приемника путем установки ее в IC для исключительного пользования
Модуль скрытности (§ 7)	Кодовая карточка с интерфейсом, предложенная для стандартизации ИСО	Встроенные или съемные модуль или кодовая карточка	Блок на базе микропроцессоров, снабженный прикладным программным обеспечением для осуществления обработки данных в соответствии с протоколами и алгоритмами дешифровки	Кодовая карточка с интерфейсом, предложенная для стандартизации ИСО	Предлагаются два решения: — кодовая карточка или — встроенный модуль	Встроенный модуль