# ГИБРИДНАЯ ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА МУЛЬТИМЕДИЙНОГО ВЕЩАНИЯ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

**Афанасьев А.В.**
***Научный руководитель: д.т.н., профессор Шахнов В.А.***
МГТУ им.Н.Э.Баумана, Москва

# HYBRID IP BROADCASTING MULTIMEDIA CONTENT PROTECTION SYSTEM

**Afanasyev A.V.**
***Science Advisor: d.t.n., Professor Shakhnov V.A.***
MSTU named after Bauman, Moscow

**Аннотация**
Развитие и коммерциализация цифрового вещания в сетях передачи данных ставит задачу формирования простой и надежной системы защиты вещания от несанкционированного доступа. В статье рассматриваются принципы защиты в спутниковом вещания и проблемы непосредственного применения этих принципов в IP-сетях. Обсуждаемое решение проблемы защиты данных основывается на принципах двухуровневого шифрования данных с применением эффективных современных алгоритмов, и расширяется гибридностью используемых каналов передачи данных – высокоскоростного однонаправленного и низкоскоростного двунаправленного.

**Abstract**
IP broadcasting development and its commercialization tends to problem of simple and reliable content protection system design. Article describes basics of satellite broadcasting protection and its adopting in IP networks problems. Proposed content protection system design based on 2-level encryption embedding state-of-art algorithm, as well as new hybrid principle of network usage – high speed one-directional and low speed bi-directional channels.

Защита от несанкционированного доступа к вещанию является одним из важнейших элементов любой вещательной деятельности, в том числе, важнейшим элементом мультимедийного вещания в сетях передачи данных. Защита используется с целью: ограничения зоны вещания, коммерциализации системы вещания и, в ряде случаев, недопущения использования несертифицированного оборудования.

Обычное эфирное телевидение естественным образом ограничено в зоне вещания и является общедоступным. Спутниковое телевещание может практически полностью покрывать всю территорию земного шара. В спутниковом вещании присутствуют общедоступные материалы, а также масса коммерческих телеканалов, таких как НТВ+, Viasat, TPS France [l, 2, 3] и другие. Существует проект «Триколор ТВ» [4], который реализует общедоступное вещание с ограничением на территорию Российской Федерации с применением сертифицированного оборудования.

Вещание в сетях передачи данных (IP-вещание) реализуется в основном на платной основе и может являться как ограниченным, так и неограниченным (сеть Интернет) территориально. Используемые в настоящий момент реализации ограничения доступа к IP-вещанию полностью повторяют модель спутникового телевидения, в которой имеется ряд недостатков: требование наличия у каждого абонента специальных индивидуальных абонентских устройств или, как минимум, специализированных высокозащищенных смарт-карт. Обнаружен ряд уязвимостей такой системы, которые широко использовались, а некоторые продолжают использоваться в настоящее время: клонирование смарт-карт, программное эмулирование смарт-карт, аппаратное эмулирование смарт-карт и проч. [5]

Существенное отличие спутникового и IP-вещания состоит в направленности канала передачи данных - однонаправленный и двунаправленный каналы соответственно. На рис.1 показаны способы предоставления доступа абонентов к контенту и методы идентификации пользователей. Защита от несанкционированного доступа может либо отсутствовать вовсе (свободный доступ), либо основываться на группах абонентов (ограничение территории вещания), либо индивидуализировать каждого подключенного абонента (коммерциализация). В случае однонаправленного распространения мультимедийных данных индивидуализация абонентов возможна только с помощью индивидуализированных абонентских приемников (индивидуализация на базе смарт-карт). При двунаправленной связи «Оператор-Абонент» появляются дополнительные возможности: аутентификация пользователей, использование цифровой подписи и цифровых сертификатов, индивидуализация по аппаратным ключам и информации IP пакетов вкупе с MAC аутентификацией [6].

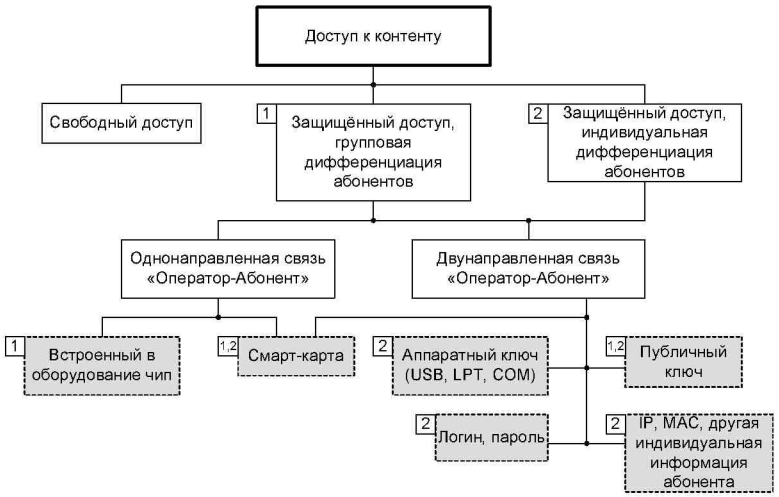


Рисунок 1 - Методы идентификации абонентов

**Текущие реализации**

Как уже было отмечено выше, в существующем IP-вещании используется адаптация спутниковой модели защиты от несанкционированного доступа DVB (DVB-CSA, DVB-CAM, DVB-CI [7]) к новой среде (рис.2). Модель является двухуровневой моделью защиты информации: оцифрованный мультимедийный поток подвергается симметричному шифрованию (собственно алгоритм, описываемый стандартом DVB-CSA), шифруются ключи шифрования проприетарным способом, после чего этот поток вместе с зашифрованными ключами шифрования передается в едином канале абоненту. Абонентское оборудование для просмотра получаемых данных должен из приходящего потока получить ключи и соответствующим образом их применить. Сущность защиты скрывается в способе шифрации, и дешифрации самих ключей. В настоящее время существует множество таких систем: Viacess, Conax, BISS, Mediaguard и многие другие [8].

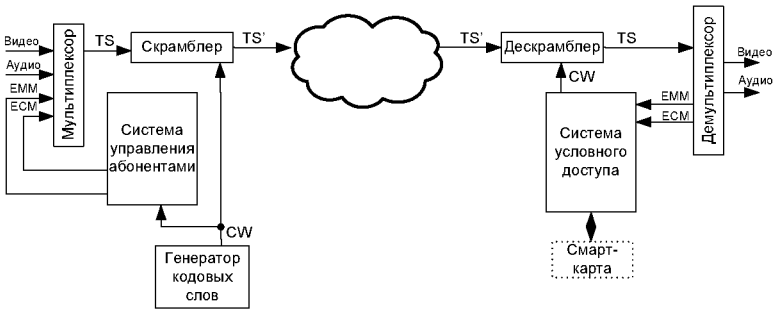


Рисунок 2 - Модель DVB-CSA

Основным достоинством такой двухуровневой модели является возможность параллельной работы нескольких систем защиты, либо различных версий одной и той же системы. Это не только позволяет разработчикам систем защиты легко конкурировать между собой, но и относительно безболезненно для абонентов производить обновление системы (введение в эксплуатацию обновленной системы и плавная замена абонентского оборудования).

Недостатками переноса этой технологии в IP-сети являются:

1. Невозможность использования персонального компьютера для просмотра вещания, поскольку требуется специальное индивидуализирующее абонентское устройство (STB и смарт-карта);

2. Дороговизна лицензирования разработки и использования скрамблера и дескрамблеров DVB-CSA [9], что зачастую является неприемлемым для малых и средних сетей;

3. Неоптимальность передачи всех канальных данных (зашифрованный поток и ключи) без разделения по IP адресам/портам.

## Гибридная модель защиты данных IP-вещания

Для эффективной работы системы в условиях полноценной двунаправленной IP сети, необходима модификация структурной схемы работы системы. Предлагаемая модифицированная структурная схема представлена на рис.3. Для преодоления трудностей использования дорогих (в смысле лицензирования) алгоритмов скрамблирования DVB-CSA, в рамках IP-вещания целесообразно воспользоваться AES (Advanced Encryption Standart) симметричного блочного шифрования [10], а для передачи ключей использовать безопасное двунаправленное соединение абонентского терминала с системой управления пользователями оператора с непосредственной аутентификацией и авторизацией абонента. Таким образом, блоки скрамблирования и дескрамблирования (схема на рис.2) преобразуются в симметричное шифрование на основе алгоритма AES, а вместо системы условного доступа, работающей на основе ECM/EMM сообщений, система аутентификации и авторизации пользователей на основе асимметричного алгоритма шифрования RSA [11].

Отличие от схемы работы DVB-CSA заключается в том, что транспортный поток мультиплексированных данных всех каналов и служебной информации (TS) заменен транспортным потоком мультиплексированных данных одного канала (канальный поток, CS), причем в этот транспортный поток не включены данные для системы условного доступа (ECM и EMM). Канальный поток (CS) после скрамблирования (CS') доставляется до абонентов, например по мультикаст сети, а необходимые данные для дескрамблирования передаются индивидуально каждому абоненту по защищенной юникаст сети (Secured Unicast), что может быть реализовано на основе SSL (Secured Socket Layer [12]) технологии. Поток данных в рамках Secured Unicast по сравнению с канальным потоком (CS') - незначительный (установление соединения абонентом, аутентификация, авторизация, передача необходимых ключей для дескрамблирования данных), поэтому применение unicast технологии не будет являться каким либо ограничением работы системы.

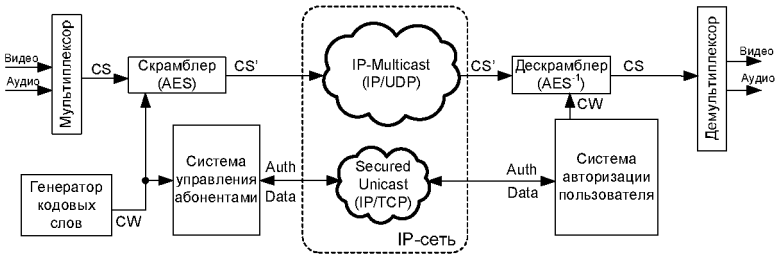


Рисунок 3 - Гибридная модель защиты в IP-сетях

В случае необходимости более глубокой системы защиты, возможно реализация аутентификации и авторизации на базе аппаратных ключей (USB, COM, LPT). Максимальная, но и самая дорогостоящая, защита может быть при реализации блоков системы авторизации и дескрамблирования в рамках одного абонентского устройства STB.

Выбор алгоритма AES [13] в качестве основы процесса скрамблирования и дескрамблирования был сделан на основании ряда критериев: алгоритм AES может быть эффективно реализован в аппаратной и программной форме, стандарт AES имеет высокую стойкость к взлому, а также минимальная (или нулевая) стоимость использования алгоритма.

Алгоритм может быть сформулирован в терминах всего лишь двух операций: побитового суммирования по модулю 2 и индексированного извлечения из памяти, выполняемых над байтами. Поэтому он может быть эффективно реализован на любых компьютерных платформах от младших микроконтроллеров до суперпроцессоров. В силу тех же причин, а

также потому что архитектура алгоритма допускает высокую степень параллелизма, он может быть также очень эффективно реализован в аппаратуре.

Прямое и обратное преобразования в шифре имеют одинаковую алгоритмическую структуру и различаются константами сдвига, ключевыми элементами, узлами замен и константами умножения. При аппаратной реализации они могут быть совмещены на 60%, при программной оптимальное быстродействие может быть достигнуто лишь при полностью раздельных реализациях обеих функций.

Все преобразования в шифре имеют строгое математическое обоснование. Сама структура и последовательность операций позволяют выполнять данный алгоритм эффективно как на 8-битных так и на 32-битных процессорах. В структуре алгоритма заложена возможность параллельного исполнения некоторых операций, что на многопроцессорных рабочих станциях может еще поднять скорость шифрования в 4 раза.

Принятый стандарт AES на основе алгоритма Rijndael [14] определяет ряд комбинаций длин ключа, размера шифруемого блока и количество раундов (один шаг преобразования) шифрования, представленных в таблице 1. Результат каждого раунда представляет собой состояние или промежуточный результат.

Таблица 1 - Комбинации длин ключа, шифруемого блока и числа раундов AES

| | **Длина ключа** *($N_k$ слов)* | **Размер блока** *($N_b$ слов)* | **Число раундов** *($N_r$)* |
|---|---|---|---|
| **AES-128** | 4 | 4 | 10 |
| **AES-192** | 6 | 4 | 12 |
| **AES-256** | 8 | 4 | 14 |

Вторым основным компонентом защиты от несанкционированного доступа гибридной модели системы IP-вещания является организация защищенного канала «Оператор-Абонент» (блок «Secured Unicast» на схеме на рис.3), в рамках которого осуществляется аутентификация абонента, авторизация (выдача списка разрешенных к просмотру каналов) и собственно передача ключей для дескрамблирования мультимедийных данных.

Эффективной реализацией такой защиты может стать полное шифрование передаваемых данных от абонента к оператору и наоборот с помощью какого либо симметричного шифрования (например с помощью рассмотренного ранее AES) с генерацией и согласованием сессионного ключа этого шифрования во время установления соединения с помощью асимметричного шифрования (шифрование с открытым ключем). Такая гибридная модель необходима, поскольку, для обеспечения сравнимого уровня стойкости, асимметричному шифрованию требуется длина ключа на несколько порядков больше, чем симметричному шифрованию, а следовательно низкая скорость шифрования (около 30 кбит/с при 512 битном ключе на процессоре 2 ГГц).

В шифровании с помощью открытого ключа, например RSA, используется пара ключей: открытый ключ и частный ключ [11], известный только его владельцу. Открытый ключ может распространяться по сети. Секретный ключ в криптографии с открытыми ключами используется для формирования электронной подписи и расшифрования данных. Однако, непосредственное использование открытых ключей требует дополнительной их защиты и идентификации для определения связи с секретным ключом. Без такой дополнительной защиты злоумышленник (нелегальный пользователь системы IP-вещания) может представить себя как отправителем подписанных данных, так и получателем зашифрованных данных, заменив значение открытого ключа или нарушив его идентификацию. Другими словами, остро стоит необходимость верификации или проверка подлинности открытого ключа. Для этих целей используется электронный сертификат.

Электронный сертификат представляет собой цифровой документ, который связывает открытый ключ с определенным пользователем или приложением. Для заверения электронного сертификата используется электронная цифровая подпись доверенного центра - Центра Сертификации (ЦС). В системе IP-вещания, таким ЦС будет выступать подсистема

системы управления пользователями (см.рис.3). Используя открытый ключ ЦС, каждый пользователь (и абоненты, и оператор) может проверить достоверность электронного сертификата, выпущенного ЦС, и воспользоваться его содержимым.

Использование смешанного асимметричного и симметричного шифрования вкупе с электронными сертификатами позволяет защитить от несанкционированного доступа передачу данных от абонента до оператора и обратно. Пара логина и пароля может обеспечить возможность, дополнительно к данным открытого ключа, идентифицировать пользователя. Использование IP и MAC адресов позволяет ограничить использование IP-вещанием одним абонентским устройством (в т.ч. ПК) на один логин/пароль/сертификат. Процессы шифрования с помощью открытого ключа и работа с электронным сертификатом основаны на одних и тех же принципах работы асимметричного шифрования. В процессе шифрования и дешифрации открытый ключ используется для собственно шифрации данных, а соответствующий ему частный ключ для дешифрации. Процесс подписывания и проверки электронного сертификата обратный: частный ключ используется для формирования электронной подписи, а публичный ключ - для проверки электронного сертификата.

**Литература**


1. ОАО «НТВ-Плюс». *Система спутникового телевидения. //* http://ntvplus.ru/.
2. *VIASAT, //*http://www.viasatworld.com/.
3. *TPS (Television Par Satellite). //* http://www.tps.fr/.
4. Национальная спутниковая компания. *ТРИКОЛОР ТВ. //* http://www.tricolor.tv/.
5. *Viaccess for Free Forum. //* http://viaccessfree.biz/forum/.
6. David Davis. *Lock down Cisco switch port security. //* http://articles.techrepublic. com.com/5100-1035-6123047.html.
7. DVB Project. *DVB - Digital Video Broadcasting. //* http://www.dvb.org/.
8. Wikipedia. *Conditional access. //* http://en.wikipedia.org/wiki/Conditional_access**.**
9. DVB Project Office. *DVB Common Scrambling Algorithm. Distribution Agreements,* 1996.
10. NIST. *AES - Advanced Encryption Standard. //* http://csrc.nist.gov/CryptoToolkit/aes/.
11. William Stallings. *Cryptography and Network Security Principles and Practices.* Prentice Hall, 4th edition, 2005.
12. Семенов Ю.А. *Telecommunication technologies - телекоммуникационные технологии. II* http://book.itep.ru.
13. Joan Daemen, Vincent Rijmen. *The Rijndael Block Cipher,* AES Proposal 1999.
14. *Federal Information Processing Standards Publication 197, Advanced Encryption Standard,* 2001.