Кібернетична безпека

УДК 004.056 (043.2)

Н.И. Алишов, А.Н. Алишов, А.Я. Бойко, Н.А. Бойко,
С.В. Зинченко, А.В. Палагин, Н.А. Сапунова

Институт кибернетики имени В.М. Глушкова НАН Украины, Киев

ТЕХНОЛОГИЯ СИСТЕМНОЙ ИНТЕГРАЦИИ АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ПОТОКОВОЙ ИНФОРМАЦИИ НА БАЗЕ НЕРАСКРЫВАЕМЫХ ШИФРОВ

Технология защиты информационных потоков в современных компьютерных сетях является наиболее актуальной задачей. Средства защиты информационных ресурсов, как правило, ориентированы на передачу статических данных, таких как файлы. Однако развитие связи и Интернет обусловливают передачу потоков данных (видео, речь, аудио) в реальном времени и необходимость создания соответствующих средств защиты такой информации. В статье описываются технология и аппаратно-программные средства организации защиты передачи потоковой мультимедийной информации в реальном времени на базе разработанного авторами USB-устройства шифрования.

***Ключевые слова**: системная интеграция, потоковая информация, защита информации, нераскрываемые шифры, протоколы передачи данных в реальном времени, устройство защиты информации.*

Введение

Постановка задачи. В 1917 г. американский инженер из компании AT&T Джилберт Вернам для шифрования телеграфных сообщений предложил алгоритм, который впоследствии был назван «одноразовым блокнотом» (One Time Pad). Вернам интуитивно понимал, что данный алгоритм обладает предельно криптоустойчивыми характеристиками, но не смог представить соответствующее теоретическое обоснование. В 1949 г. К. Шеннон доказал, что существуют шифры, обладающие предельной криптоустойчивостью, на примере алгоритма Вернама. Суть идеи Шеннона состоит в том, что если символы шифра имеют равновероятные значения, то такие алгоритмы являются нераскрываемыми. Здесь уместно привести слова самого известного современного специалиста в области криптографии «…Эти сообщения не могут быть раскрыты и останутся нераскрытыми. На этот факт не повлияет время работы суперкомпьютеров над этой проблемой. Даже если «враги» из созвездия Андромеды приземлят свои тяжелые корабли с компьютерами немыслимой мощности, то и они не смогут прочесть эти сообщения…» [1].

Состояние проблемы. Авторами данной статьи за последние семь лет были проведены исследования по созданию аппаратно-программных средств с целью компьютерной реализации алгоритмов нераскрываемых шифров [2, 3]. Первая разработка была выполнена на базе процессора для шифрования статических файлов (тексты, изображения и другие компьютерные данные), не в реальном масштабе времени, т.е. файлы шифровались на передающем компьютере и потом передавались по сети. Такой подход был связан с тем, что разработанное устройство (рис. 1) не обеспечивало требуемую для систем реального времени производительность.

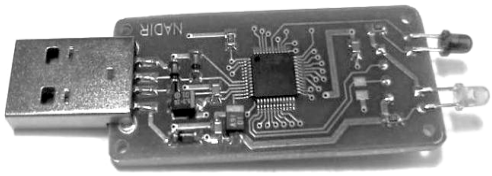

Рис. 1. Общий вид устройства для режима off-line

Цель статьи. С учетом растущей необходимости в передаче потоковой мультимедийной информации в компьютерных сетях следующий вариант устройства (рис. 2, 3) был создан на базе процессора серии TMS320 C5505 для цифровой обработки сигналов, что обеспечило требуемую производительность [4, 5].

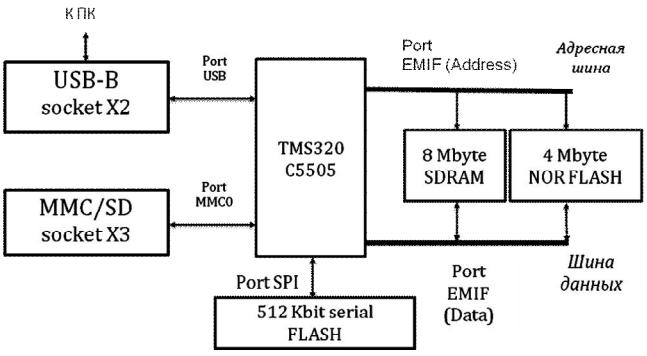

Рис. 2. Блок-схема устройства on-line

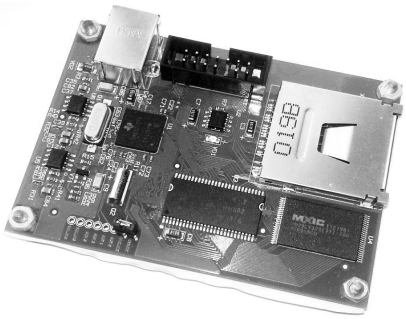

Рис. 3. Общий вид устройства on-line

Изложение основного материала

Суть алгоритма шифрования заключается в следующем. В массив памяти на базе SD-карточки записываются истинно случайные числа (шум в лесу, шум автомобильного двигателя и т.п.), из которых организуется специальный массив (он и будет секретным ключом). Берется байт шифрируемого мультимедийного файла, в секретном ключе разыскивается его адрес и этот адрес передается по сети. На приемной стороне имеется такой же массив истинно случайных чисел (секретный ключ), где по принятому адресу разыскивается значение байта, которое станет байтом зашифрованной последовательности. Данный алгоритм является предельно криптоустойчивым. Существует множество вариантов его реализации. Например, выбирается один из лучших алгоритмов генерации псевдослучайных чисел с определенными параметрами («зерно»). Передающая сторона на базе истинно случайных чисел (по вышеописанному алгоритму) отправляет принимающей стороне «зерно». Принимающая сторона, используя эти параметры, на лету генерирует соответствующие псевдослучайные числа и из этих чисел выбирает байты передаваемой мультимедийной информации. В таком случае объем исходного массива чисел может быть значительно меньшим.

Схема упрощенного варианта предлагаемого алгоритма шифрования показана на рис. 4.

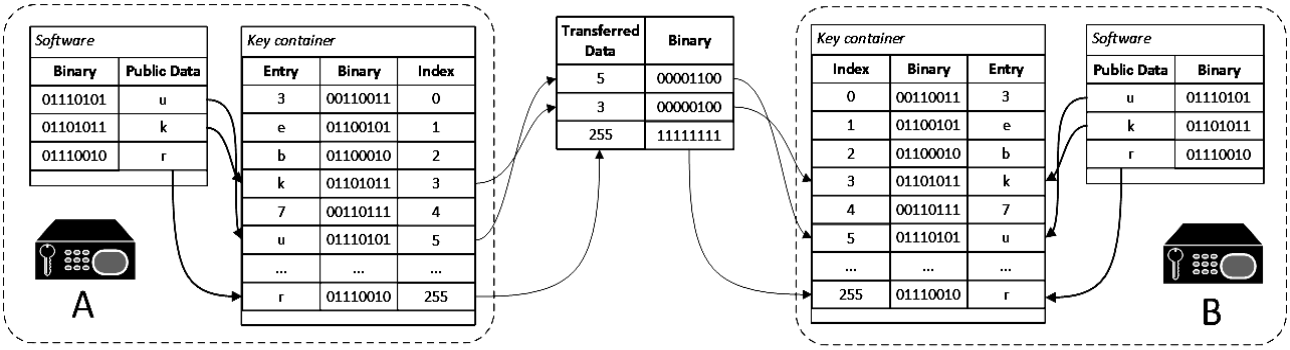

Рис. 4. Упрощенный алгоритм передачи зашифрованной потоковой информации в реальном времени

В настоящее время существуют множество стандартных международных протоколов, предназначенных для передачи потоковой информации в компьютерных сетях. Кроме того, многие известные фирмы предлагают программные приложения, которые являются надстройками над этими протоколами для передачи мультимедийной потоковой информации в компьютерных сетях. Поэтому разработка собственных протоколов и приложений не представляется актуальной. Задача авторов заключалась в том, чтобы интегрировать разработанные программные средства для устройства шифрования с существующими протоколами и приложениями. Данная задача не является тривиальной и требует высокого профессионализма, так как эти системы не предназначены для «чужеродных» устройств. Наиболее известные протоколы и их взаимодействие для решения поставленной задачи показаны на рис. 5.

Из них базовыми для потоковой передачи информации являются:

- *RTSP* (*Real Time Streaming Protocol)*, будучи сетевым прикладным протоколом, предназначен для использования в системах, которые работают с мультимедийными данными и позволяют клиентам удаленно управлять потоком данных с сервера;
- *RSVP* (*Resource Reservation Protocol)* – протокол резервирования сетевых ресурсов для обеспечения необходимого качества обслуживания между взаимодействующими узлами при передаче потоковой информации;
- *RTCP* (*RTP Control Protocol)* – поддержка RTP-протокола путем оценки состояния сети;
- *RTP* протокол (*Real-time Transport Protocol*) – работает на прикладном уровне и является основным протоколом для передачи данных в реальном масштабе времени;
- *H26x MPEG* – серия стандартов для сжатия видеоинформации с сохранением требуемого качества.

На рис. 6 приведена упрощенная схема взаимодействия клиента с мультимедийным сервером через базовые протоколы передачи потоковой информации. Как видно, открытый канал организуется с использованием протоколов *RTSP* и *RTCP*. Первый управляет передачей потоковой информации в реальном масштабе времени, второй контролирует изменения в сети для предоставления информации *RTP*-протоколу.

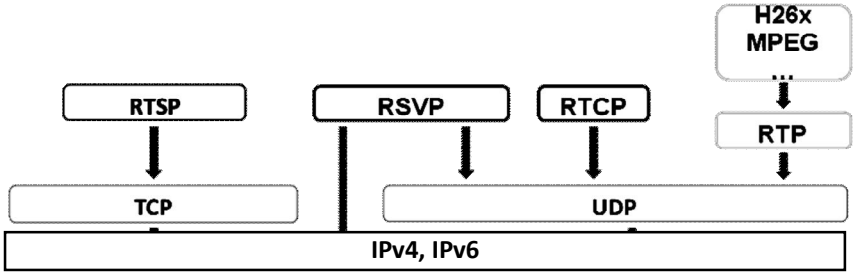

Рис. 5. Протоколы реального времени

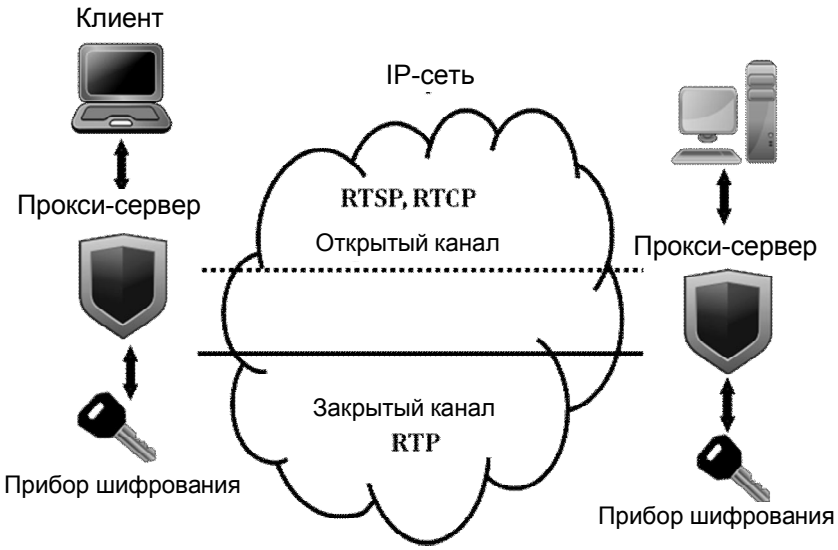

Рис. 6. Схема взаимодействия клиентов IP-сети

Защищенный канал базируется на использовании *RTP*-протокола. Как отмечалось, существует множество приложений, обеспечивающих взаимодействие клиентов через открытый канал (например, приложения *XLITE*, *EKIGA* и т.п.). Поэтому основной задачей авторов было создание не только интерфейса взаимодействия с этими приложениями для организации передачи открытых данных, но и способа использования интерфейса протокола *RTP* для интеграции с разработанным устройством шифрования передаваемых потоковых мультимедийных данных в реальном масштабе времени. В данной реализации для этой цели используются прокси-серверы, хотя возможны и другие варианты. Считаем, что в настоящее время представленный вариант является наиболее эффективным.

Таким образом, с точки зрения системной интеграции разработанный комплекс состоит из двух подсистем: программная подсистема, организующая интерфейс с сетевыми протоколами, и аппаратная подсистема, реализующая предложенный алгоритм шифрования потоковой информации на базе нераскрываемых шифров.

Обобщенная схема взаимодействия этих подсистем показана на рис. 7.

Следует отметить, что основной частью оригинальной разработки авторов являются собственно устройство шифрования, реализованное на базе процессора цифровой обработки сигналов, и авторское программное обеспечение для этого устройства. При создании программного обеспечения для устройства использовалась стандартная система отладки фирмы *TMS* на базе «С»-подобного языка программирования. С точки зрения технической реализации устройства были представлены схемотехнические решения интеграции процессора с *SD*-карточкой практически любого типа и любого размера. Кроме того, были разработаны оригинальные программные средства для связи с *USB*-портом базового компьютера, отличающиеся тем, что обеспечена возможность получения предельной производительности при передаче потоковой информации в реальном масштабе времени. Из любого приложения, требующего шифрования данных, передаются открытые локальные данные к аппаратной системе. Аппаратная подсистема определяет позицию текущего сегмента и извлекает значения по его позиции. Далее контейнер-ключ передается в сеть (уже в зашифрованном виде) абоненту-адресату, который на базе секретного ключа дешифрирует потоковую информацию в реальном времени. При получении из сети зашифрованных данных программная подсистема передает эти данные в устройство дешифрования, которое передает значения текущего сегмента в качестве индекса в контейнер-ключ. Далее дешифрованные данные передаются в соответствующее приложение.

Заключение

Таким образом, разработаны технология и аппаратно-программные средства защиты мультимедийной информации, передаваемой в реальном времени, на основе нераскрываемых шифров. Организация такой защиты предполагает интеграцию разработанных алгоритмов с современными стандартными протоколами и приложениями. Дальнейшее развитие данной работы связано с необходимостью оптимизации отдельных подсистем технологии интеграции.

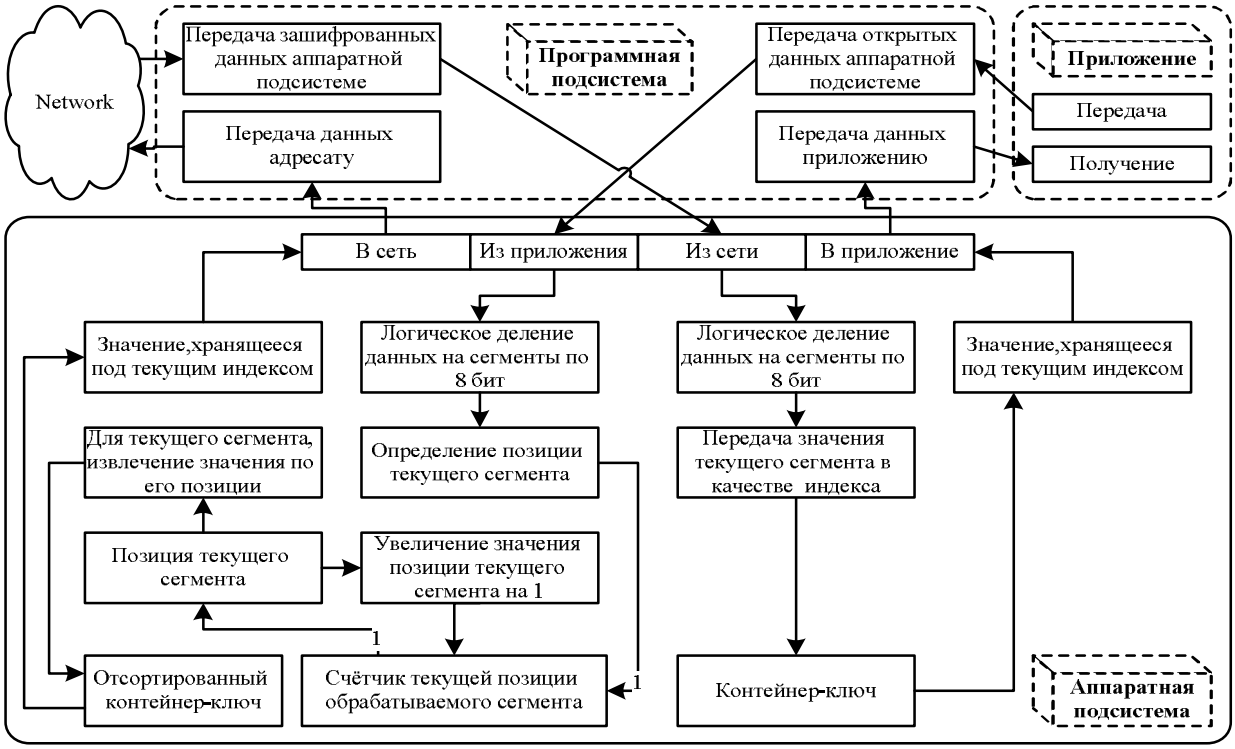

Рис. 7. Схема взаимодействия двух подсистем комплекса защиты

Список литературы

1. Брюс Шнайер Б. Прикладная криптография / Брюс Шнайер Б. – М.: Триумф, 2002. − 816 с.

2. Алишов Н.И. Алгоритмы замены контейнеров-ключей при потоковом шифровании информации методом косвенного шифрования / Н.И. Алишов, В.А. Марченко, А.Н. Мищенко // Системні дослідження та інформаційні технології. – 2012. − № 2. − С. 102-110.

3. Пат. 101796 UA, МПК G09C 1/06. Обчислювальний пристрій захисту інформації / Алішов Н.І., Марченко В.А., Міщенко О.М.; заявник і патентовласник Інститут кібернетики ім. В.М. Глушкова НАНУ. − № 06181; заявл. 17.05.2011; опубл. 25.04.2013, Бюл. № 8. − 9 с.

4. Method of shared data access in distributed computer networks / [Nycolaychuk Y.M., Humenniy P.V., Alishov N.I., Hladyuk V.M.] // Journal of Qafgaz University (Baku): Mathematics and Computer Science. – 2013. – V. 1, no 1. − P. 17-23.

5. Computer technologies in information security / [Valery Zadiraka, Yaroslav Nykolaichuk, Nadir Alishov, Ivan Albanskyi, Boris Bredelev et al.]. − Ternopil: Kart-Blansh, 2015. − 387 p.

Поступила в редколлегию 24.02.2016

Рецензент: д-р техн. наук, проф. В.Н. Опанасенко, Институт кибернетики им. В.М. Глушкова НАН Украины, Киев.

ТЕХНОЛОГІЯ СИСТЕМНОЇ ІНТЕГРАЦІЇ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАХИСТУ ПОТОКОВОЇ ІНФОРМАЦІЇ НА БАЗІ НЕРОЗКРИВНИХ ШИФРІВ

Н.І. Алішов, А.Н. Алішов, О.Я. Бойко, М.О. Бойко, С.В. Зінченко, О.В. Палагін, Н.О. Сапунова

Технологія захисту інформаційних потоків у сучасних комп'ютерних мережах є найбільш актуальним завданням. Засоби захисту інформаційних ресурсів, як правило, орієнтовані на захист передачі статичних даних, таких як файли. Проте розвиток зв'язку та Інтернет зумовлює передачу потоків даних (відео, мовлення, аудіо) в реальному масштабі часу і необхідність створення відповідних засобів захисту такої інформації. У статті описуються технологія й апаратно-програмні засоби організації захисту передачі потокової мультимедійної інформації в реальному часі на базі розробленого авторами USB- пристрою шифрування.

***Ключові слова**: системна інтеграція, потокова інформація, захист інформації, нерозкривні шифри, протоколи передачі даних в реальному часі, пристрій захисту інформації.*

TECHNOLOGY OF SYSTEM INTEGRATION HARDWARE AND SOFTWARE PROTECTION MEANS OF STREAMING DATA BASED ON UNBREAKABLE CIPHERS

N.I. Alishov, A.N. Alishov, A.J. Boyko, N.A. Boyko, S.V. Zinchenko, A.V. Palagin, N.A. Sapunova

Technology of protection of information data streams in modern computer networks is the actual task. Information resources protection means are, as a rule, focused on protecting the transfer of static data, such as files. However, the development of communication and the Internet is an urgent transfer data streams (video, audio) in real time. It causes need for protection technologies of these data in real-time. This article describes the technology and hardware, and software protection means of transfer multimedia stream in real time based on the ciphering USB device developed by authors.

***Keywords**: system integration, stream information, information security, unbreakable ciphers, real-time data transmission protocols, the device of information protection.*