70. *Пат.* № 2302085 РФ, H04L9/00 (2006.01). Способ кодирования и передачи криптографических ключей / Молотков С., Кулик С. – № 200513476; 16.11.2005.

71. *Пат.* № 2325039 РФ, H04L9/00 (2006.01). Способ кодирования и передачи криптографических ключей / Молотков С., Кулик С. – № 2006119652; 06.06.2006.

72. *Pat.* № 7461323 USA, H03M 13/00 (20060101). Quantum key delivery method and communication device / Matsumoto, Wataru et al – 02.12.2008.

73. *Pat.* № 7266304 USA, H04B 10/00 (20060101), H04K 1/00 (20060101). System for secure optical transmission of binary code / Duraffourg, Laurent et al – 04.09.2007.

74. *Pat.* № 7178277 USA, H04K 1/00 (20060101). Quantum cryptography communication system and quantum cryptography key distributing method used in the same / Takeuchi, Takeshi et al – 20.02.2007.

75. *Pat.* № 6748081 USA, H04L 9/08 (20060101), C09K 19/02 (20060101), G02F 1/13 (20060101). Quantum cryptography system for a secure transmission of random keys using a polarization setting method / Dultz, Wolfgang et al – 08.06.2004.

76. *Pat.* № 6438234 USA, H04L 9/08 (20060101), H04K 001/00. Quantum cryptography device and method / Gisin, Zbinden et al – 20.08.2002.

77. *Pat.* № 6895092 USA, H04L 9/08 (20060101), G06F 017/00. Cryptographic key distribution method and apparatus thereof / Tomita, Akihisa et al – 17.05.2005.

Поступила 23.11.09

УДК 003.26:004.056.55 **Климентов В.В., Трощило А.С.**

КРИПТОСИСТЕМА С «ВИРТУАЛЬНЫМ КЛЮЧОМ»

Возникновение и развитие области защиты информации (ЗИ) как неотъемлемой части информационной индустрии связано с острой необходимостью в средствах противодействия высокой уязвимости информационных технологий к различным злоумышленным действиям.

Совершенно очевиден тот факт, что информация по характеру не материальна, однако она всегда имеет стоимость, т.е. материальный эквивалент. Это свойство делает ее объектом копирования, модифицирования и хищения. Типичной является ситуация, когда совместное владение информацией наносит непоправимый ущерб одной из сторон, владеющей ею. Поэтому функция ЗИ актуальна практически во всех сферах коммуникации.

Постоянный рост и разнообразие задач, относящихся к сфере ЗИ, обусловлены тем, что информационные взаимодействия, развиваясь, приобретают все более сложный характер, соответственно становятся более разнообразными и изощренными угрозы в их сторону, а это, в свою очередь, приводит к возникновению новых задач.

Если раньше все потребности в защите информации сводились к обеспечению секретности и подлинности передаваемых сообщений, то есть к их защите от прочтения и внесения изменений, то сейчас количество проблем многократно возросло.

Особенно остро встала проблема защиты компьютерных сетей. Актуальность этой проблемы подтверждается следующими фактами.

США уже финансирует создание модели интернета будущего, где в условиях строгой секретности изучаются способы хакерского блокирования электросетей, сетей связи и аэропортов, а также финансовых рынков, дабы усовершенствовать как методы защиты, так и виртуальное оружие нового поколения.

На сегодняшний день в США возникла необходимость в создании «цифровых войск», которые смогли бы защитить страну от внешних электронных угроз, сообщает источник BBC. Идею создания подобного подразделения, которое бы занималось проблемами цифровой безопасности, озвучил глава АНБ США. Ожидается, что организация этого подразделения будет полностью завершена в 2010 г.

Информационные технологии все чаще используются в качестве оружия. Только за последние полгода Пентагон потратил более $100 млн на устранение последствий от хакерских атак. Началась международная гонка кибервооружений и оборонительных систем, которую можно сравнить с развитием событий после появления атомной бомбы. По мнению экспертов аналитического центра Center for Strategic and International Studies (Вашингтон), Китай, Россия и ряд других держав уже вкладывают колоссальные деньги в разработку кибероружия. Европа также осознала необходимость в подобной защите на государственном уровне, по информации интернет источников [1;2].

Промышленно развитые страны сильно зависят от промышленных усилий по борьбе с электронными угрозами, которые не поспевают за ростом уровня самих угроз. Одним из вариантов решения данной проблемы в комплексе мер по ЗИ в компьютерных сетях являются криптосистемы.

Основными критериями их оценки при внедрении являются: гибкость, надежность, стоимость и криптостойкость.

Новая криптосистема, разработанная авторами данной статьи, обладает эффективными показателями вышеназванных качеств. Новизна подхода состоит в отказе от некоторых общепризнанных в криптографии позиций.

Принято считать, что второй принцип Керкгоффса является одним из основополагающих в криптографии. Он гласит следующее: криптостойкость криптосистемы обеспечивается не секретностью алгоритма, а секретностью ключа [3]. То есть, для преобразования информации в передаваемом сообщении справедливо равенство:

$$A + K = ПС,$$

где A – алгоритм, который является константой;
K - ключ, который является переменной величиной,
$ПС$ - преобразованное сообщение.
Предлагаемая формула имеет условный характер и дана для наглядности.

Таким образом, если рассматривать преобразование информации в зашифрованном сообщении при N-ом обмене в режиме передатчик – приемник, преобразованная информация в зашифрованном сообщении будет равна информации, преобразованной алгоритмом, который видоизменен по закону изменения ключа, т.е. фактически новому алгоритму. Поэтому можно говорить о создании постоянно нового алгоритма в системе шифрования – дешифрования сообщения при N-ом обмене.

Способ шифрования, разработанный авторами, является альтернативой известным криптосистемам. Он позволяет пересмотреть незыблемость позиции второго принципа Керкгоффса и избежать соблюдения некоторых общепринятых требований к шифрованию. Ноу-хау авторской позиции состоит в том, что классическое понятие «ключ» наполняется новым содержанием: фактически функция ключа подменяется функцией алгоритма и функциями синхронизации, уникальными для каждого сообщения. Ключ, по сути, является виртуальным. Таким образом, появляется возможность создавать совершенно стойкие шифры, в соответствии с формулировкой Шеннона [4].

Общеизвестно, что принципиально нераскрываемые шифры (например, совершенно секретные системы Клода Шеннона, в которых ключ не может использоваться повторно, а его размер больше либо равен объему текста) не удобны на практике (симметричные криптосистемы с разовым использованием ключа требуют большой защищенной памяти для хранения ключей).

В силу своей непрактичности и высокой ресурсозатратности абсолютно стойкие шифры применяются только в сетях связи с небольшим объемом передаваемой информации, когда есть возможность обеспечить всех абонентов достаточным запасом

случайных ключей и исключить возможность их повторного применения: обычно это сети для передачи особо важной государственной информации.

Новый альтернативный способ позволяет избежать этих недостатков. Решение опирается на следующие методологические предпосылки:

1 – вне зависимости от подходов к решению проблемы зашифрованная информация должна быть защищена от вскрытия либо модификации и представлять собой целостную материальную систему;

2 – информация в компьютере представлена в цифровом виде, т.е. уже трансформирована при помощи математических функций, что существенно облегчает анализ математическими методами;

3 – шинный интерфейс компьютера (например, «Q-bus») - это не только система протоколов, но и система синхронизации, что усложняет анализ сигнала в связи с большим количеством переменных;

4 – каждый сложный сигнал любой природы (зашифрованная информация, речь, музыка, видеосигнал и т.д.) представляет собой некую целостность, которая, с философской точки зрения, не сводима к сумме частей ее составляющих.

В нашем случае, математические методы, несмотря на их ценность и аналитическую мощь, могут дать лишь поверхностное представление о том, из чего мог бы состоять рассматриваемый сигнал, но принципиально не отвечают на вопрос о его сущности как целостной материальной системы, взаимодействующей с другими системами. Есть основание утверждать, что реализация вышеизложенного позволяет зашифрованному сообщению попадать в канал с «ключом», приблизительно равным длине передаваемого файла.

Поэтому о «ключе» можно говорить только условно, т.к. сигналы информации, шума, гаммирования, имитовставки, синхронизации, идентификации и т.д. являются частью построенной материальной системы.

Алгоритм реализации многослойный и состоит из следующих этапов: шифрования и сжатия исходного текста, преобразования зашифрованного текста, вложения преобразованного текста в аудиоинформацию, кодирования и сжатия аудиоинформации с плавающим коэффициентом сжатия [5], который зависит от природы используемого аудиосигнала. Такой подход объединяет три метода: кодирование со сжатием, шифрование и сжатие, и может быть использован для криптозащиты больших объемов данных.

Из этого следует, что криптоаналитик, не обладая соответствующими комплектами физических устройств, т.е. не будучи пользователем криптосистемы, будет анализировать только поверхностный слой информации и не будет иметь доступа к основным слоям зашифрованного текста. То есть, информация сохранит свою защищенность и целостность [6].

Авторами разработана реальная криптосистема, использующая принцип многократного сужения и расширения спектра шифруемой информации, краткое описание которой приведено ниже.

Назначение:

обмен конфиденциальной информацией (аудио, видео, текст) по открытым каналам проводной и беспроводной связи (телефонная связь, Интернет и т.п.) и ее хранение на электронных носителях.

Криптоалгоритм:

получение зашифрованного сообщения: шифрование со сжатием – преобразование – вложение в аудиоинформацию (например, в музыку) - кодирование и сжатие аудиоинформации.

Получение расшифрованного сообщения: декодирование с декомпрессией – идентификация аудиоинформации (распознавание) – преобразование – декомпрессия – преобразование – декодирование (дешифрование).

Состав:

система состоит из абонентских устройств, центра синхронизации передаваемых сообщений, канала аудиоданных и устройства активации.

Структурная схема представлена на рис 1.

- Количество абонентских устройств от 2 до n.
- А - абонентское устройство, состоящее из: компьютера; ШДУ - шифрующего/дешифрующего устройства, реализующего криптоалгоритм и обеспечивающего внутреннюю синхронизацию, которое можно условно назвать «физическим ключом» абонентского устройства, и устройства сопряжения с сетью (например, модем и т.п.);

ШДУ - конструктивно выполнено в виде «флешки» и подключается к USB;

- ЦСС - центр внешней синхронизации сообщений, реализует алгоритм синхронизации обмена между абонентскими устройствами; производит учет абонентов, состоявшихся и несостоявшихся соединений, проверку правильности работы сигналов синхронизации и обнаружения несанкционированного использования устройства (работа под контролем); осуществляет арбитраж и отключение абонентов;

ЦСС - состоит из компьютера, мультиплексора и устройства сопряжения сетью;

- КАД - виртуальный канал аудиоданных, предназначен для постоянной передачи аудиоинформации пользователям системы;

КАД - реализуется пользователем;

- Устройство активации – предназначено для активации ШДУ в момент запуска (на рис.1 не показано).

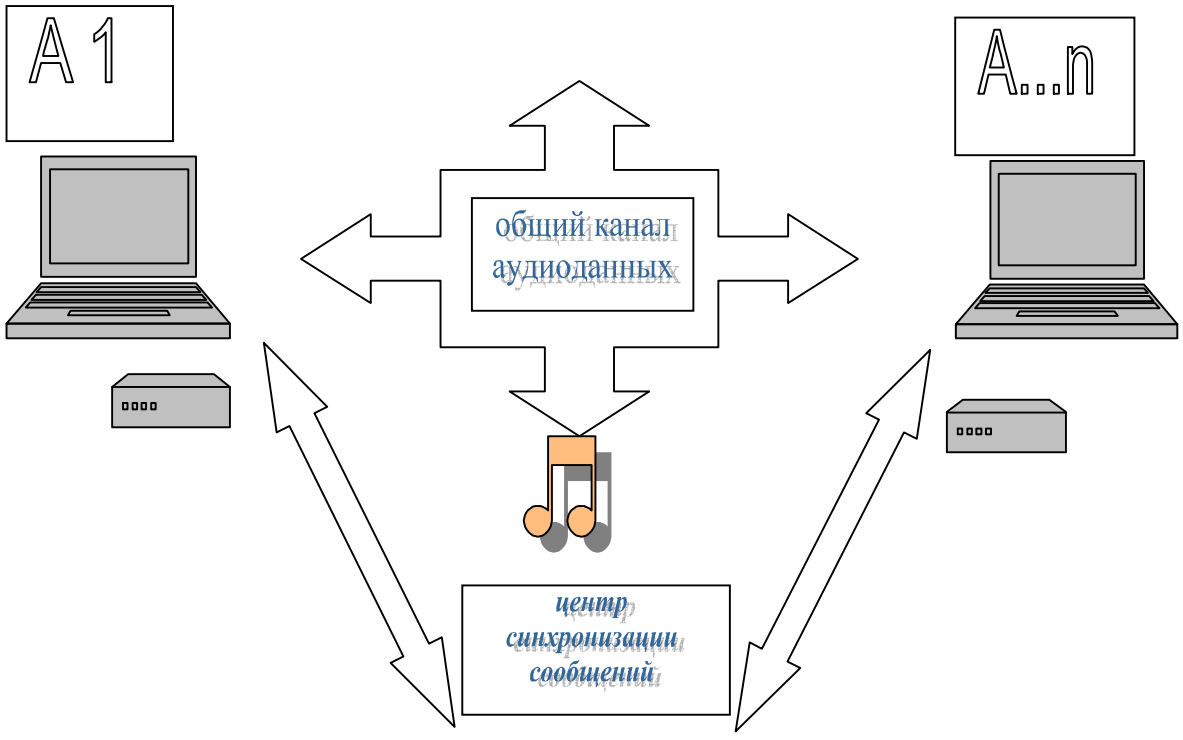

Рис.1. Структурная схема

Канал аудиоданных:

предназначен для постоянной передачи аудиоинформации

пользователям системы и является носителем «элемента синхронизации сообщения». Канал аудиоданных может быть реализован пользователем по собственному усмотрению. Например, в качестве источника аудиоинформации могут быть использованы каналы телевидения, радиовещания и т.п.

Особенности системы

гибкость – возможность (при условии соблюдения структурной схемы):

- видоизменения пользователем без участия разработчика;
- создания локальных криптосистем без участия разработчика.

Активация:каждое из ШДУ активируется пользователем в момент первого включения при получении устройства у оператора (провайдера). Для этого проводится активирующая серия, состоящая из *x* сообщений прием – передача для начальных установок синхросигналов системы, которые не являются подконтрольными оператору.

Учет абонентов:проводится в ЦСС по аналогии с существующими системами, которые применяются фирмами, предоставляющими услуги связи.

При активации в ЦСС открывается карточка абонента, в которой регистрируется номер физического устройства, данные о владельце, дата и факт активации (факт проведения активирующей серии сообщений прием – передача), производится учет состоявшихся и несостоявшихся соединений, осуществляется проверка правильности работы сигналов синхронизации и обнаружения несанкционированного использования устройства (работа под контролем).

Арбитраж:

ЦСС может выступить арбитром в случае возникновения конфликтных ситуаций, требующих участия третьей стороны, т.к. абонент, желающий создать ложное сообщение, не сможет сослаться на него как на истинное в связи с тем, что:

1. не будет подтвержден истинный факт связи и получения сообщения абонентом - получателем;
2. будет разрушена система синхронизации физического устройства абонента, создавшего ложное сообщение, что приведет к удалению этого физического устройства из сети, потому что его сообщения станут нечитаемыми для всех абонентов системы.

Перехват и доступ к передаваемой информации:

система построена по принципу передачи образа зашифрованного сообщения, поэтому ЦСС, несмотря на то что принимает участие в передаче каждого сообщения, не в состоянии выполнить функцию перехвата и расшифровки передаваемых сообщений. Даже в случае острой необходимости (например, запрос от компетентных органов) передаваемое сообщение будет защищенным в связи с тем, что ЦСС не работает с реальными данными, а работает либо с образами данных, передаваемых абонентам, либо со служебными сигналами.

Таким образом, система позволяет пользователю:

- создавать совершенно стойкие шифры, в соответствии с формулировкой Шеннона;
- легко перестраиваться в процессе оперативного реагирования на различные виды угроз, не прибегая к дополнительным материальным затратам;
- интегрироваться в существующие системы ЗИ без вложения существенных материальных затрат;
- создавать локальные криптосистемы без участия разработчика, т.к. пользователь имеет инструмент для создания собственных креативных технических решений;
- не вкладывать значительных средств в обслуживание абонентов и подготовку персонала;
- наращивать количество абонентов.

Список литературы

1. Интернет сообщение: www.securitylab.ru
2. Интернет сообщение: www.cnews.ru
3. Kerckhoffs A. La cryptographie militaire // Journal des sciences militaries. - Vol. IX. - Jan. 1883, P. 5-38, (P. 161-191, Feb. 1883).
4. Шеннон К.Э. Работы по теории информации и кибернетике // М.: И.Л., 1963.
5. Жебка С.В. Сжатие звуковой информации // Захист інформації. Спеціальний випуск(40). - 2008. - С. 128 -129; Герасин С.Н., Калиниченко О.В., Лоцман В.П., Трощило А.С. О способе кодирования сигналов различной природы. // Бионика интеллекта. - 2008. - №1 (68). - С. 177-180.
6. Климентов В.В., Трощило А.С., Дыс Л.И., Бурлаков В.М. Проблемы и перспективы применения криптографических систем // Інформаційна Безпека. Матеріали науково-практичної конференції. Україна, Київ, 26-27 березня 2009 року. - С. 270-274.

Поступила 25.11.09

УДК 621.39:534.782 **Демьян Н.И., Осмаловский В.А., Хорошко В.А.**

ЛИНЕЙНЫЕ МОДЕЛИ РЕЧЕВОГО СИГНАЛА С ЛОКАЛЬНО-ПОСТОЯННЫМИ ПАРАМЕТРАМИ

Вступление

Звуки при формировании которых голосовые связки осуществляют колебательные движения называют вокализованными. Все остальные звуки относятся к невокализованным. Более точно: среди последних различают фрикативные звуки, возникающие при образовании турбулентного широкополосного шума, и взрывные звуки, формируемые путем создания в тракте смычки с последующими внезапным высвобождением сжатого в области за смычкой воздуха.

Волны распространяющиеся в речеобразующей системе, могут быть описаны двумя функциями пространственных x, y, z и временной (непрерывной) t координат: звуковым давлением $p(x, y, z, t)$. Для акустических колебаний с длиной волны λ, превышающей размеры голосового тракта, можно считать, что вдоль продольной оси тракта распространяется плоская волна. Такое допущение оправдано в частотном диапазоне ниже 5000 Гц [1]. Звуковое давление и объемная скорость тогда являются функциями только двух переменных: $p(x, t)$, $\upsilon(x, t)$. Если голосовой тракт аппроксимировать цилиндрической трубой с сечением $S(x, t)$, то распространение колебаний по трубе можно описать волновым уравнением Вебстера:

$$\frac{1}{S(x,t)}\cdot\frac{\partial}{\partial x}S(x,t)\frac{\partial\bar{\Phi}(x,t)}{\partial x}=\frac{1}{c^2}\frac{\partial^2\bar{\Phi}(x,t)}{\partial t^2}; \qquad (1)$$

где $\Phi(x,t)$ - потенциал скорости акустических колебаний,

$$\frac{\partial\Phi(x,t)}{\partial x}=\frac{1}{\rho}p(x,t),\ \frac{\partial\bar{\Phi}(x,t)}{\partial t}=-\upsilon(x,t);$$

где ρ - плотность воздуха в трубе; c – скорость распространения звука в воздухе.

Основная часть

Выражение (1) описывает свободные колебания в тракте. При произнесении вокальных звуков речи на вход тракта воздействует волна, поступающая от голосовых связок, объемная