УДК 004.056

АЛГОРИТМЫ ЗАМЕНЫ КОНТЕЙНЕРОВ-КЛЮЧЕЙ ПРИ ПОТОКОВОМ ШИФРОВАНИИ ИНФОРМАЦИИ МЕТОДОМ КОСВЕННОГО ШИФРОВАНИЯ

Н.И. АЛИШОВ, В.А. МАРЧЕНКО, А.Н. МИЩЕНКО

Описан новый подход построения систем потокового шифрования с использованием метода косвенной стенографии. Приведены алгоритмы различных реализаций предложенного подхода.

ВСТУПЛЕНИЕ

Основной задачей всякого криптоалгоритма является обеспечение необходимой защищенности шифруемой информации. Согласно требованиям Керкгоффса [1], надежность криптографической системы должна определяться сокрытием секретных ключей, но не сокрытием используемых алгоритмов или их особенностей. Поэтому вопросам управления ключами шифрования, их генерации и удобства использования уделяется особое внимание при создании современных систем защиты, работающих с криптографическими алгоритмами. Именно ключ шифрования является базовым секретным компонентом при шифровании/расшифровке сообщений, создании и проверке цифровой подписи, вычислении кодов аутентичности. В общем случае при использовании одного и того же алгоритма результат шифрования должен зависеть только от используемого ключа и не зависеть от реализации криптоалгоритма.

В современных информационных системах широкое распространение получили поточные криптографические алгоритмы. Райнер Рюппель [2] выделил четыре основных подхода к проектированию поточных шифров:

- Теоретико-системный подход, ориентированный на создание для криптоаналитика сложной, ранее не исследованной проблемы.
- Теоретико-сложностный подход, базирующийся на сложной, но ранее уже исследованной проблеме (например, факторизация чисел, дискретное логарифмирование и т.д.).
- Теоретико-информационный подход, в соответствии с которым делается попытка скрыть сам исходный текст от криптоаналитика так, что вне зависимости от того, сколько времени потрачено на расшифрование сообщения, криптоаналитик не сможет однозначно указать соответствие криптограммы и исходного сообщения.

- Эмперический подход, предусматривающий создание задачи большого объема, решение которой будет физически неосуществимым для криптоаналитика.

Соответственно этим подходам были указаны и теоретические критерии для проектирования поточных криптоалгоритмов:

- длинные периоды выходных последовательностей;
- большая линейная сложность;
- диффузия — рассеивание избыточности в подструктурах, «размазывание» статистики по всему тексту;
- каждый бит потока ключей должен быть результатом сложных преобразований большинства битов ключа;
- нелинейность применяемых логических функций.

На данный момент не существует теоретического доказательства [3] необходимости и достаточности этих критериев для создания криптостойкой системы поточного шифрования.

МЕТОД КОСВЕННОГО ШИФРОВАНИЯ

Клод Шеннон в 1949 г. в работе «Теория связи в секретных системах» [4] доказал существование абсолютно секретных систем и криптостойких шифров и определил необходимые для этого условия. Он также сформулировал основные требования, предъявляемые к надежным шифрам. Этим требованиям отвечает схема одноразовых блокнотов, реализованная ранее Гильбертом Вернамом [5]. В этой схеме используемый ключ должен обладать тремя критически важными свойствами:

- быть истинно случайным — содержать истинно случайные последовательности;
- совпадать по размеру с заданным открытым текстом — быть не меньше открытого текста;
- применяться только один раз — не допускается повторное применение ключа.

При этом условия, которым должен удовлетворять ключ, настолько сложны, что практическая реализация криптоалгоритма, отвечающего трем требованиям абсолютной криптоустойчивости, является трудно осуществимой. Современные реализации одноразовых блокнотов используются только для передачи сообщений наивысшей секретности.

Большинство известных современных алгоритмов компьютерного шифрования не отвечают условиям абсолютной безопасности [6]. Это определяет изначальную уязвимость используемых криптосистем, так как они построены на основе алгоритмов, для которых не доказана теоретическая криптостойкость.

Использование в качестве поточного криптоалгоритма метод одноразовых блокнотов гарантирует абсолютную надежность и криптостойкость всей системы.

В предложенном методе косвенного шифрования [7, 8] у отправителя и получателя имеются одинаковые массивы данных, которые являются секретными ключами. Байты информации, подлежащие защите, заменяются

(по определенному алгоритму) байтами секретного массива. Полученный новый массив байтов размером исходного сообщения передается адресату. Полученный по каналу массив данных, подвергается обратному преобразованию: байты заменяются байтами секретного файла (зеркальный алгоритм). Этот метод способен обеспечить абсолютную безопасность по Шеннону, поскольку объединяет принцип одноразовых блокнотов и небольшое количество алгебраических преобразований, к тому же он легко реализуется на большинстве существующих программно-аппаратных средствах, и при его использовании можно:

- создать средства для заполнения ключа истинно случайными числами;
- вне зависимости от количества передаваемых данных, размер ключа будет равен объему передаваемой информации;
- обеспечить однократность применения ключа.

Особенностью метода косвенного шифрования является то, что при шифровании одного и того же байта открытого текста всегда получаются различные байты шифротекста. Таким образом, отпадает необходимость «нормализации» шифруемых сообщений для противодействия атакам с использованием статистических методов. С точки зрения криптостойкости в передаваемых криптограммах не содержится исходная информация, а только ее образ в памяти. Исходя из этого, даже зная характер передаваемых данных (формат данных, различные заголовки и т.п.), невозможно восстановить часть ключевой информации или передаваемых данных.

В методе косвенного шифрования, ключ представляет собой массив байтов достаточно большого размера, называемый контейнером-ключом.

РАСПРОСТРАНЕНИЕ КОНТЕЙНЕРОВ-КЛЮЧЕЙ

Основной проблемой криптографии является способ распространения и передачи ключей. В предложенном методе косвенного шифрования могут использоваться несколько схем работы с ключами. В данной работе рассматривается только схема работы криптоалгоритма, которая максимально близка к одноразовым блокнотам. Следует отметить, что в качестве используемых протоколов обмена ключами могут применяться различные известные схемы, но подробный анализ конкретных схем выходит за рамки темы рассматриваемой в работе. Таким образом, длина контейнеров-ключей должна быть не меньше длины передаваемых сообщений.

В рассматриваемой реализации метода косвенного шифрования возможны следующие варианты работы с контейнером-ключом:

- системы реального времени — без разрыва связи для замены контейнера-ключа;
- системы периодической связи — не требуют постоянного обмена потоками данных, однако обеспечивают максимальную криптозащиту в процессе связи.

Вариант для систем реального времени не отвечает критериям абсолютной безопасности по Шеннону, так как даже при реализации максимальной безопасности в этом случае контейнер-ключ (КК) будет приме-

няться дважды: первый раз — для шифрования полезной информации, а второй — для шифрования нового КК. Для передачи нового КК предлагается использовать следующий алгоритм: адресату передается один байт зашифрованной полезной информации, затем один байт зашифрованного нового КК и т.д. по очереди. Это вдвое увеличивает нагрузку на используемый канал связи, но при этом гарантирует отсутствие задержек при шифровании следующей порции передаваемых данных.

Чтобы создать условия, близкие к абсолютной безопасности по Шеннону, в варианте для систем периодической связи замену контейнеров-ключей можно организовать следующими способами:

- физически передавать всякий раз новый КК (это выходит за рамки объективной информационной безопасности, т.к. безопасность передачи и конфиденциальности информации зависит только от субъектов, осуществляющих доставку контейнера-ключа);
- применять гибридную схему — для шифрования нового КК использовать известный алгоритм блочного шифрования (например AES), а для шифрования потоков полезной информации — рассматриваемый метод косвенного шифрования.

Целесообразность применения гибридной схемы обусловлена тем, что:

- блочный шифр обеспечивает высокий уровень криптоустойчивости шифруемого КК, для которого малоэффективны атаки с помощью методов линейной алгебры, а также другие методы криптоанализа, применяемые для поточных шифров. Однако криптостойкий блочный шифр в силу своей архитектуры не может быть использован для шифрования потоковой информации без потерь исходных свойств;
- метод косвенного шифрования позволяет реализовать шифрование потоковой информации с криптостойкостью, не уступающей криптостойкости применяемого алгоритма блочного шифрования. Так как он сам обладает теоретически доказанной криптостойкостью.

Используемый при этом контейнер-ключ имеет большой размер, его шифрование целиком с помощью выбранного блочного шифра теряет какой-либо практический смысл, — так как это займет время, соизмеримое со временем работы самого блочного шифра. Поэтому, чтобы избежать задержек, вызванных необходимостью ожидания окончания шифрования и передачи всего КК, предлагается условно делить новый КК на сегменты небольшого размера — n (где n — сегмент контейнера-ключа (схема предполагает условное деление контейнера-ключа на небольшие части для ускорения шифрования/дешифрования новых сегментов КК симметричным блочным алгоритмом)), которые, в свою очередь, шифруются и передаются как часть нового КК. При этом параметры ключа, используемые в блочном алгоритме шифрования (длина ключа, его криптостойкость и т.д.), напрямую зависят от:

- объема шифруемых данных в потоковом режиме;
- максимально допустимых задержек;
- необходимой скорости передачи зашифрованных данных.

Применение такой гибридной схемы обусловливает создание двух виртуальных каналов (потоков) передачи информации между взаимодействую-

щими криптосистемами (рис. 1), которые будут работать в параллельном режиме.

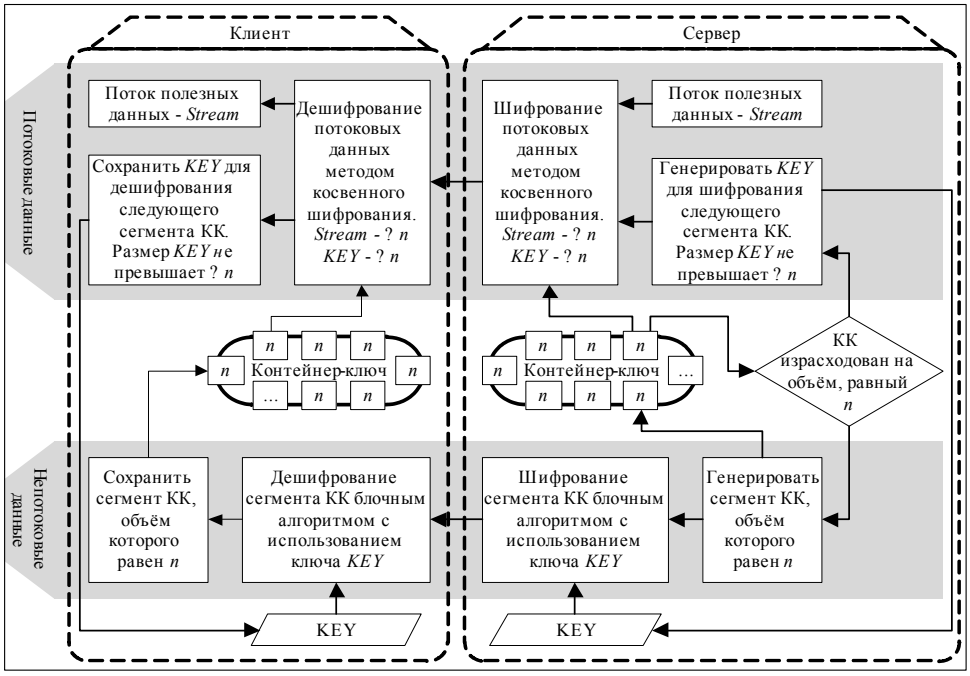

Рис. 1. Взаимодействие потоковых и непотоковых данных в гибридном методе, где *KEY* — ключ, используемый для симметричного блочного шифрования сегмента *n*

Один канал (поток) предполагается использовать для обмена шифруемой методом косвенного шифрования полезной информацией. Этот канал является основным, т.к. по нему идет обмен в потоковом режиме. Перебои в его работе мгновенно скажутся на работе всей системы обмена информацией в целом, поэтому исходные параметры функционирования этого канала должны полностью удовлетворять требованиям системы. Второй канал будет использоваться для передачи зашифрованных блочным шифром новых сегментов КК (*n*) с сервера клиенту.

В данной схеме в качестве сервера может выступать любая из двух взаимодействующих систем. Сервер выбирается при организации каналов для генерирования и передачи контейнера-ключа. Перебои в работе этого канала не сказываются мгновенно на работе всей системы обмена информацией в целом, так как динамическое изменение параметров используемой симметричной криптосистемы позволит компенсировать такие отклонения, как перебои в связи и временные ухудшения параметров канала (время задержки, потеря пакетов и т.п.)‘. Следует учесть, что компенсация ухудшения некоторых параметров канала связи приводит к уменьшению криптостойкости передаваемых шифрограмм.

Криптостойкость рассматриваемого гибридного метода зависит от криптостойкости блочного шифра, используемого для шифрования сегментов *n* нового КК. Повысить криптозащиту поможет использование нового ключа *KEY* для шифрования каждого нового сегмента *n* нового КК. Нужно отметить, что при таком подходе быстрее расходуются ресурсы КК, а также увеличивается вычислительная нагрузка на серверную систему.

Уязвимым местом предлагаемого способа является гипотетическая возможность вскрыть зашифрованный новый сегмент КК с помощью различных методов криптоанализа для блочных шифров, так как используемый в данной схеме алгоритм компьютерной криптографии не отвечает требованиям абсолютной безопасности по Шеннону. Однако на выполнение такого анализа понадобится значительно больше времени, нежели шифруемая с помощью нового КК полезная информация будет оставаться актуальной.

Вообще процесс криптоанализа зашифрованного нового КК является нетривиальной задачей, так как для того, чтобы определить правильно ли выполнено расшифрование, субъект, выполняющий криптоанализ (ПО, использующее аппаратно-вычислительные мощности суперкомпьютера), должен сопоставить расшифрованный результат с чем-то и прийти к выводу, что полученная (расшифрованная) информация имеет какой-либо смысл или является частью исходного текста. Если же зашифрованная информация представляет собой истинно случайную последовательность, то прийти к выводу, что полученный результат (расшифрованная информация) имеет какой-либо смысл, крайне проблематично. В этом случае должны применяться методы криптоанализа, пригодные для взлома шифров, которые используют информационно-технический подход по Рюппелю [9].

ОСОБЕННОСТИ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ

Для реализации метода косвенного шифрования могут использоваться как программные, так и аппаратные подсистемы, выполняющие шифрование/расшифрование потоков полезной информации и способные генерировать истинно случайные числа, а также содержащие средства для хранения контейнера-ключа с возможностью его перезаписи (замены).

Как правило, аппаратные устройства инициализируются (заполняются контейнеры-ключи) по месту изготовления, затем передаются конечным пользователям, где их устанавливают (инсталлируют).

В случае использования программных реализаций метода косвенного шифрования после установки соответствующего ПО на конечную систему необходимо дополнительно обеспечить организационную защиту помещений, где размещены эти средства.

В настоящее время все большую популярность обретают различного рода приложения для организации видео и аудио трансляций по распределенным телекоммуникационным сетям, системы конференцсвязи и телеприсутствия которые используют высокоскоростные сетевые каналы с малыми задержками для эффективной работы. Для защиты информации, которая обрабатывается в подобных системах, используются криптосистемы потокового шифрования.

Такая криптосистема призвана обеспечить:

- необходимую криптографическую стойкость шифруемой информации;
- шифрование в реальном времени больших объемов информации;
- максимальную гибкость в применении для обеспечения безопасности различных сетевых приложений.

Авторами, для построения системы защиты, предлагается использовать промежуточные «прослойки» между защищаемым приложением и самой

криптосистемой потокового шифрования, которые реализованы в виде прокси-сервера. Таким образом, это вариант реализации обеспечивает гибкую интеграцию системы защиты с конечным защищаемым приложением без необходимости вносить дополнительные изменение в ПО конечного приложения.

К примеру, на двух ЭВМ установлены VoIP приложения и предлагаемая криптосистема (рис. 2), в таком случае реализуется следующая схема:

1. Криптосистема постоянно следит за сетевой активностью VoIP-приложения.

2. VoIP-приложение инициализирует сетевое подключение к удаленной ЭВМ.

3. Криптосистема блокирует передачу информации от приложения в сеть, перенаправляет исходящий поток данных от VoIP-приложения на себя и выполняет подключение от своего имени к запрашиваемой удаленной системе.

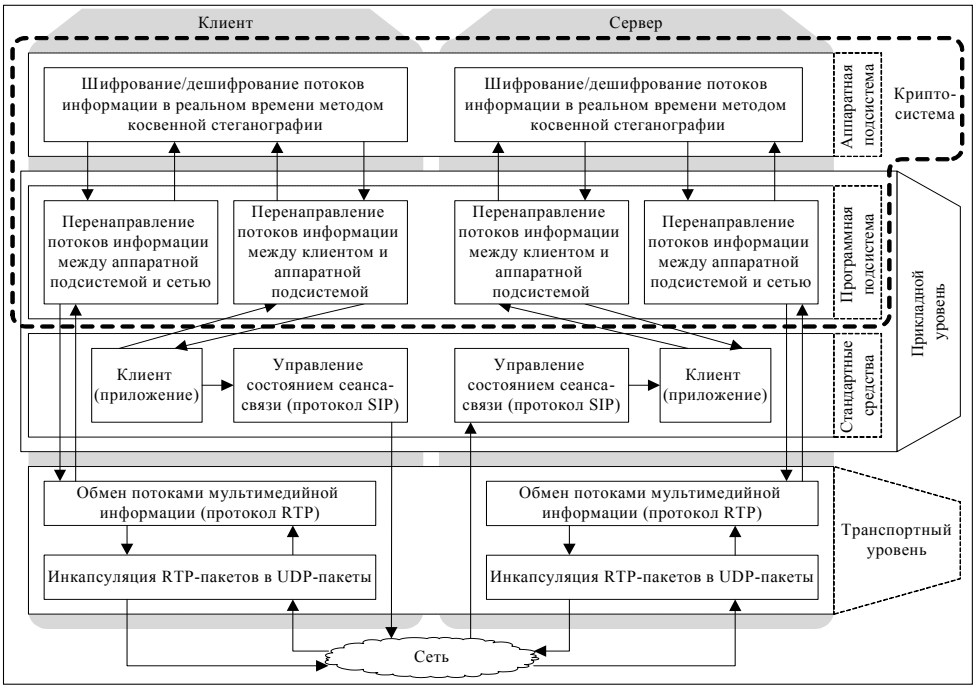

Рис. 2. Концептуальная схема функционирования криптосистемы

Если на удаленной системе используется такая же система защиты, то происходит процесс согласования и обмена ключами и другими параметрами шифрования. В противном случае, если данная система защиты не используется, то в зависимости от настройки или отключается шифрование или сеанс связи разрывается.

После установления соединения с удаленной криптосистемой начинается обмен потоками зашифрованной полезной информации (рис. 3).

Таким образом, в такой реализации криптосистема прозрачно для защищаемого приложения обеспечивает передачу данных по сети. При этом есть возможность использовать различное клиентское ПО достаточно, что бы оно использовало стандартный стек протоколов для потокового вещания.

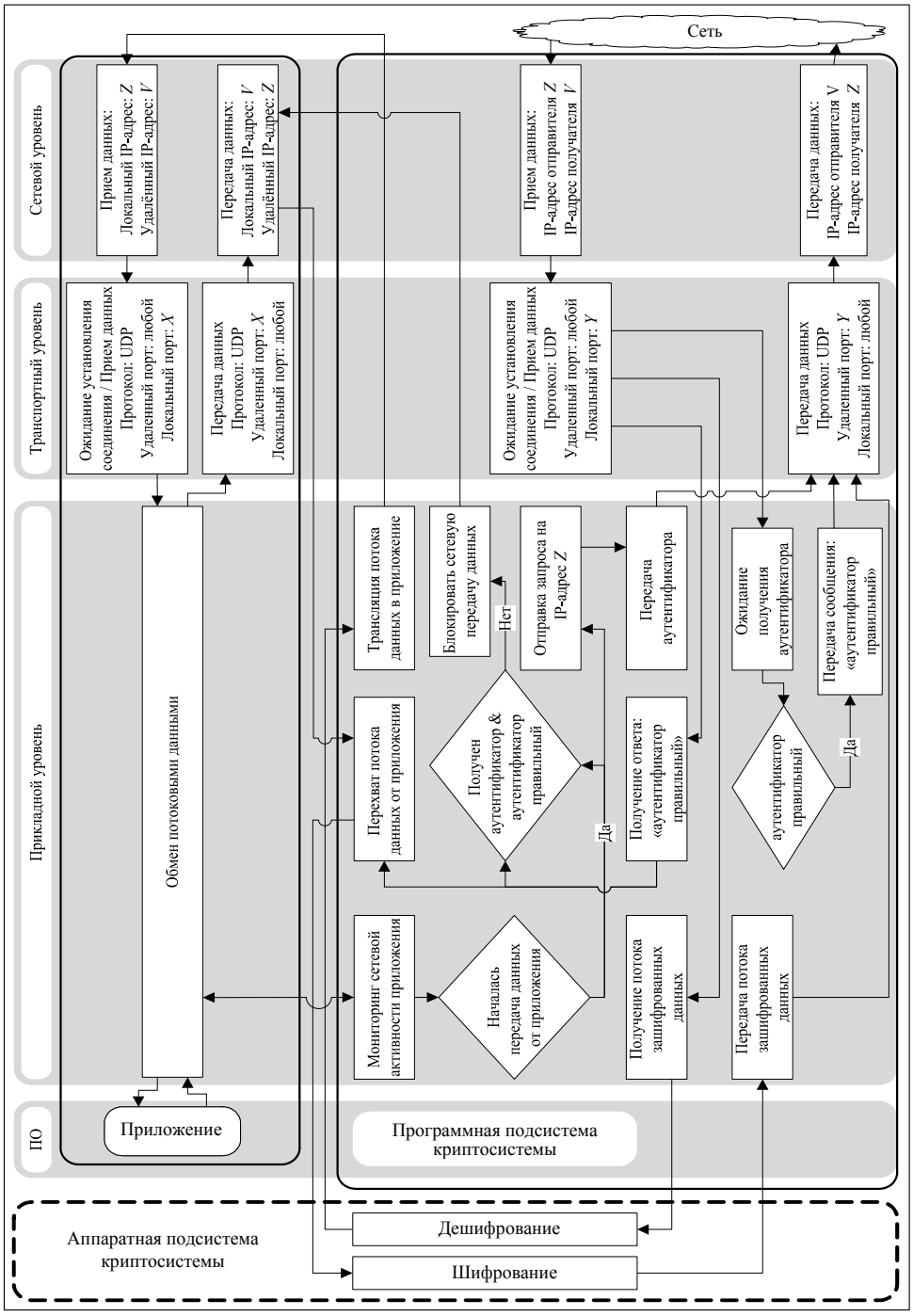

Рис. 3. Алгоритм работы тандема VoIP-приложения и криптосистемы

ВЫВОДЫ

Применение предлагаемой криптосистемы, использующей для шифрования метод косвенного шифрования, позволяет реализовать повышенный уровень безопасности, по сравнению с существующими потоковыми алгоритмами.

Сама система потокового шифрования может работать на каналах, обладающих различными свойствами и качеством, при этом криптостойкость передаваемой информации остается на достаточно высоком уровне.

Слабым местом этой реализации, как и любой другой криптосистемы, является передача ключа, однако представленные в данной работе алгоритмы способны обеспечить высокий уровень безопасности и гибкости при передаче контейнера-ключа. Следует отметить, что система для своей работы в штатном режиме не требует дополнительных схем и протоколов обмена ключами и при этом обеспечивает криптостойкость, не уступающую криптостойкости используемого симметричного алгоритма. Достичь более высокого уровня криптостойкости можно было бы применением асимметричных криптоалгоритмов, но это резко ограничит круг задач, решаемых системой.

ЛИТЕРАТУРА

1. *Kerckhoffs A.* La cryptographie militaire // Journal des sciences militaries. — **IX**. — 1883. — P. 5–38. — Feb. 1883. — P. 161–191.
2. *Rueppel R.A.* Analysis and Design of Stream Ciphers // Springer communications and control engineering series. — 1986. — 244 p.
3. *Асосков А.В., Иванов М.А., Мирский А.А., Рузин А.В., Сланин А.В., Тютвин А.Н.* Поточные шифры. — М.: КУДИЦ-ОБРАЗ, 2003. — 336 с.
4. *Шеннон К.* Работы по теории информации и кибернетике. — М.: Изд-во иностр. лит-ры, 1963. — 830 с.
5. *Vernam G.S.* Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications // Journal of the IEEE. — 1926. — **55**. — P. 109–115.
6. *Сборка* и перевод зарубежных исследований. Поточные шифры. Результаты зарубежной открытой криптологии. — http://www.ssl.stu.neva.ru/psw/crypto/potok/str_ciph.htm.
7. *Алишов Н.И.* Косвенная стеганография // Intern. Book Series «Information and science & conputing» (Sofia: ITHEA). — 2009. — № 11. — P. 53–58.
8. *Алишов Н.И., Марченко В.А., Оруджева С.Г.* Косвенная стеганография как новый способ передачи секретной информации // Комп'ютерні засоби, мережі та системи: зб. наук. пр. — К.: НАНУ, Ін-т кібернетики, 2009. — № 8. — С. 105–112.
9. *Simmons G.L.* (ed.). Contemporary Cryptology: The Science of Information Integrity. — NY: IEEE, 1992. — 592 p.

Поступила 04.06.2010