КОМП'ЮТЕРНІ ЗАСОБИ, МЕРЕЖІ ТА СИСТЕМИ

A.N. Mishchenko

ALGORITHMS OF CHANGEOVER OF CONTAINERS-KEYS AT STREAM ENCIPHERING BY A METHOD OF INDIRECT ENCIPHERING

The encryption algorithm of the stream information – "a method of indirect scrambling" and changeover of encrypting keys is presented. The variant of flexible integration of a method in existing VoIP systems is offered.
Key words: encryption, cryptography, onetime pad, container-key.

Представлений алгоритм шифрування потокової інформації – "метод непрямого шифрування" і заміни ключів шифрування. Запропонований варіант гнучкої інтеграції методу в існуючі VoIP системи.
Ключові слова: шифрування, криптографія, одноразовий блокнот, контейнер-ключ.

Представлен алгоритм шифрования потоковой информации – "метод косвенного шифрования" и замены ключей шифрования. Предложен вариант гибкой интеграции метода в существующие VoIP системы.
Ключевые слова: шифрование, криптография, одноразовый блокнот, контейнер-ключ.

УДК 004.056

А.Н. МИЩЕНКО

АЛГОРИТМЫ ЗАМЕНЫ КОНТЕЙНЕРОВ-КЛЮЧЕЙ ПРИ ПОТОКОВОМ ШИФРОВАНИИ МЕТОДОМ КОСВЕННОГО ШИФРОВАНИЯ

Введение. Основной задачей любого криптоалгоритма является обеспечение максимальной криптоустойчивости шифруемой информации. Согласно требованиям Керкгоффса [1], надёжность 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 криптоалгоритмы. Райнер Рюппель [2] выделил четыре основных подхода к проектированию поточных шифров:

- системно-теоретический подход, ориентированный на создание для криптоаналитика сложной, ранее не исследованной проблемы;

- сложно-теоретический подход, базирующийся на сложной, но ранее уже исследованной проблеме (факторизация чисел, дискрет-

ное логарифмирование и т. п.);

- информационно-технический подход, в соответствии с которым делается попытка скрыть сам исходный текст от криптоаналитика так, что, вне зависимости от того, сколько времени потрачено на дешифрование сообщения, криптоаналитик не сможет однозначно указать соответствие криптограммы и исходного сообщения;

- рандомизированный 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, определил необходимые для этого условия. Шеннон также сформулировал основные требования, предъявляемые к надежным шифрам. В частности, ключ для нераскрываемого шифра 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.

Этим требованиям отвечает схема одноразовых блокнотов (One-time pad), реализованная ранее Гильбертом Вернамом [5].

При этом условия, которым должен удовлетворять ключ, настолько сложны, что практическая реализация криптоалгоритма, отвечающего трём 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 ос-

нове алгоритмов, для которых не доказана теоретическая криптостойкость.

Использование в качестве поточного криптоалгоритма метод одноразовых блокнотов гарантирует абсолютную надежность и 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 байт 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.

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

Распространение контейнеров-ключей. Основная проблема криптографии – способ распространения и передачи ключей. В предложенном методе косвенного шифрования могут использоваться несколько схем работы с ключами. В данной статье рассматривается схема работы криптоалгоритма, максимально близкая к одноразовым блокнотам. Таким образом, длина контейнеров-ключей должна быть не меньше длины передаваемых сообщений.

Обозначения, используемые в работе:

КК – контейнер-ключ;

n – сегмент контейнера-ключа (схема предполагает условное деление контейнера-ключа на небольшие части для ускорения шифрования/дешифрования новых сегментов КК симметричным блочным алгоритмом);

KEY – ключ, используемый для симметричного блочного шифрования сегмента *n*.

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 данны-

ми, 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 будет применяться 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 так далее 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 так:

- физически передавать всякий раз новый КК (это выходит за рамки объективной информационной безопасности, так как 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 – метод косвенного шифрования.

Целесообразность применения гибридной схемы обусловлена тем, что:

- блочный шифр обеспечивает высокий уровень криптоустойчивости шифруемого КК, для него 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;
- 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, 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. п.), 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 взаимодействующими криптосистемами (рис. 1), будут работать в параллельном режиме. Один канал (поток) предполагается использовать для обмена шифруемой методом косвенного шифрования полезной информацией. Этот канал является основным, так как 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 с сервера клиенту зашифрованных блочным шифром новых сегментов КК – *n*.

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, 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.

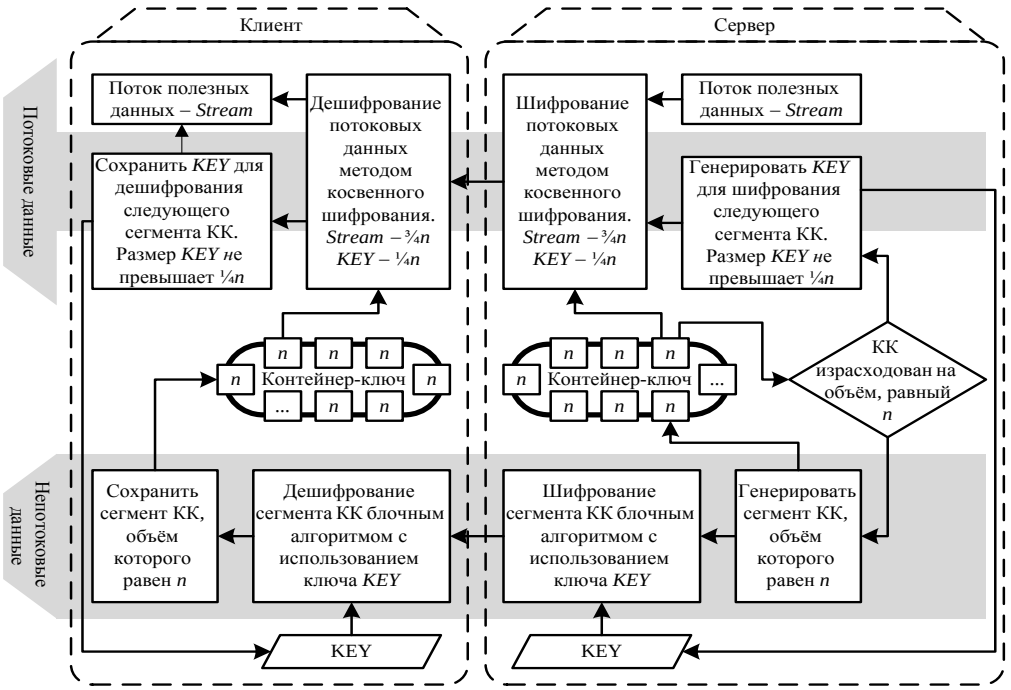

РИС. 1. Взаимодействие потоковых и не потоковых данных в гибридном методе

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.

В общем случае процесс криптоанализа зашифрованного КК является нетривиальной задачей, так как для того чтобы определить, правильно ли выполнено дешифрование, 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 смысл, крайне сложно, в этом случае должны применяться методы криптоанализа, пригодные для взлома шифров, которые используют информационно-технический подход по Рюппелю [2].

Особенности практической реализации. Для реализации метода косвенного шифрования могут использоваться как программные, так и аппаратные подсистемы, выполняющие шифрование/дешифрование 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.

Представленная криптосистема призвана обеспечить:

- качественно новый уровень криптографической стойкости шифруемых данных;
- шифрование в реальном времени больших объемов информации;
- максимальную гибкость в применении для обеспечения безопасности сторонних сетевых приложений.

В настоящее время всё большую популярность обретают различного рода приложения для конференцсвязи.

Один из вариантов реализации метода косвенного шифрования, обеспечивающий гибкую интеграцию решения с VoIP приложениями, заключается в создании промежуточной «прослойки», таким образом, что приложение может выйти в сеть только через этот прокси-сервер.

К примеру, на нескольких ЭВМ установлен предлагаемый защитный программно-аппаратный комплекс, состоящий из двух подсистем (рис. 2): программной и аппаратной.

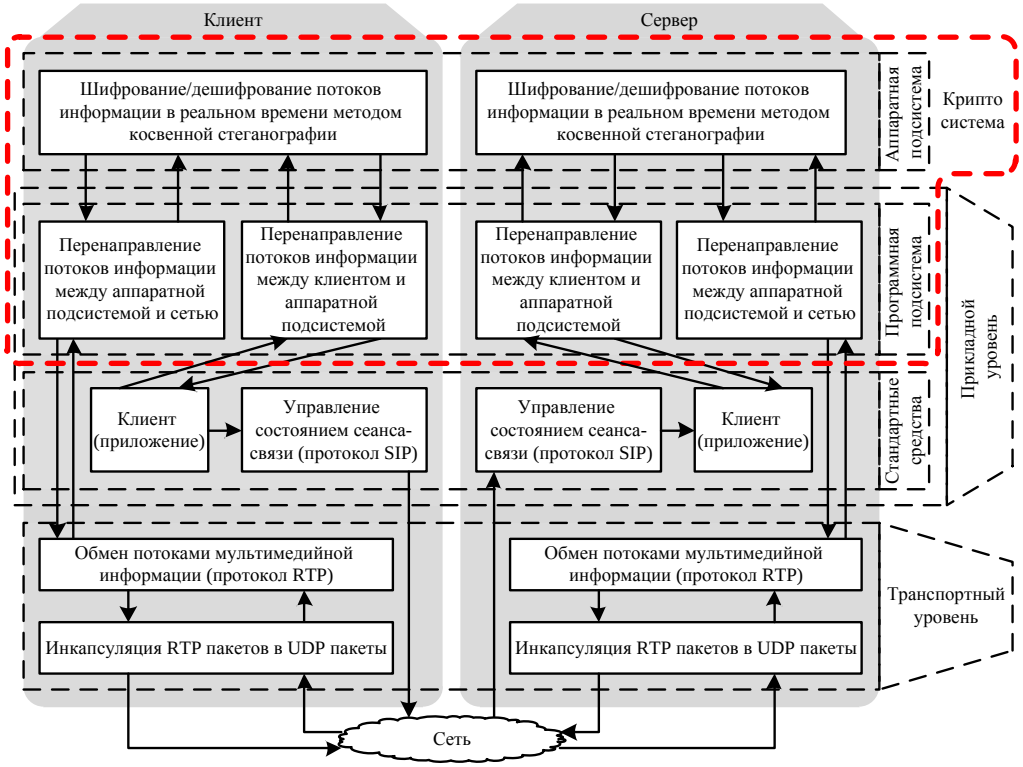

РИС. 2. Концептуальная схема функционирования криптосистемы

Программная подсистема обеспечивает интеграцию защитного программно-аппаратного комплекса в существующую инфраструктуру компьютерной телефонии. Она состоит из следующих модулей, для обработки:

- исходящего потока открытой медиа информации;
- входящего потока зашифрованной медиа информации.

Общий алгоритм функционирования криптосистемы (рис. 3):

- криптосистема постоянно следит за сетевой активностью VoIP-приложения;

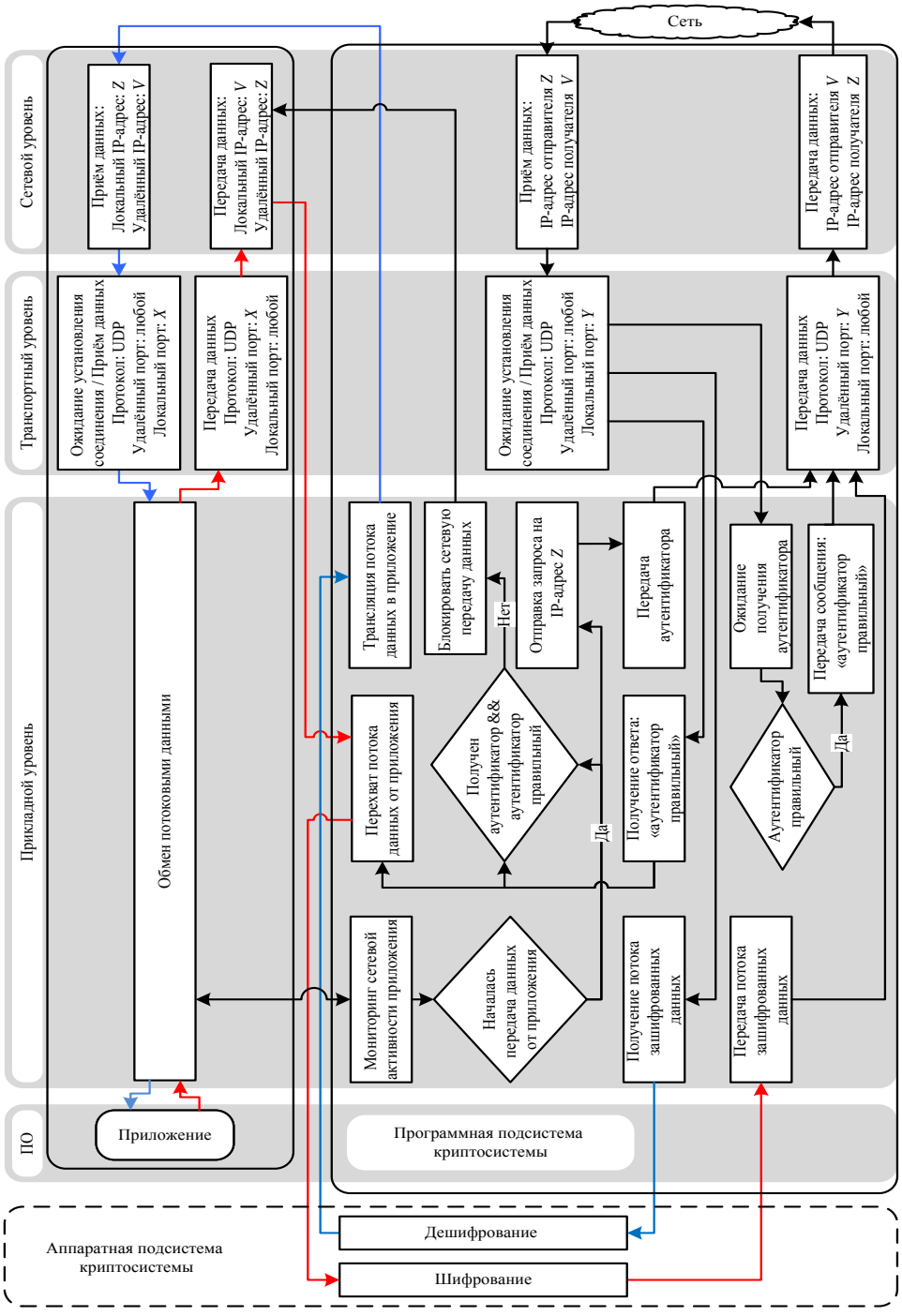

РИС. 3. Алгоритм работы тандема VoIP-приложения и криптосистемы

- VoIP-приложение инициализирует сетевое подключение к удалённой системе;
- криптосистема блокирует передачу информации от приложения в сеть, перенаправляет поток данных от VoIP-приложения на себя и выполняет подключение от своего имени к запрашиваемой удалённой системе. После установления соединения с удалённой криптосистемой начинается обмен потоками зашифрованной полезной информации. Таким образом, в такой реализации криптосистема сама обеспечивает передачу данных по сети и следит за корректностью передаваемой информации.

Аппаратная подсистема – выполняет шифрование/дешифрование в реальном времени получаемых от программной подсистемы потоков информации. Состоит из двух модулей, для выполнения: шифрования исходящего потока информации; дешифрования входящего потока информации.

Выводы. Применение предлагаемой криптосистемы, использующей для шифрования метод косвенного шифрования, позволяет реализовать качественно новый уровень безопасности, приближенный к абсолютной. 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 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.

1. *Шнайер Б.* Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 610 с.
2. *Rueppel R.A.* Analysis and Design of Stream Ciphers // Springer Communications And Control Engineering Series. – 1986. – N 1. – P. 244–260.
3. *Асосков А.В., Иванов М.А., Мирский А.А. и др.* 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. *Зубов А.Ю.* Совершенные шифры. – М.: Гелиос АРВ, 2003. – 159 с.
6. *Сборка* и перевод зарубежных исследований. Поточные шифры. Результаты зарубежной открытой криптологии. – М.: 1997. – 1059 с.
7. *Алишов Н.И.* Косвенная стеганография // Intern. Book Series "INFORMATION i SCIENCE & COMPUTING" (Sofia: ITHEA). – 2009. – N 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. – 2009. – № 8. – С. 105–112.

Получено 13.03.2011