УДК 004.056.55

Н.И. Алишов, А.Н. Мищенко

Варианты реализации шифрования потоковой информации в компьютерных системах и сетях методами косвенной стеганографии

Представлены концепции и основанные на них версии алгоритма шифрования потоковой информации методами косвенной стеганографии. Приведено сравнение версий в рамках каждой конкретной концепции.

The concepts and the based on them versions of an algorithm of the enciphering of a stream information by the methods of the indirect steganography are presented, a comparison of versions within the limits of each concept is given.

Представлено концепції та засновані на них версії алгоритму шифрування потокової інформації методами непрямої стеганографії. Наведено порівняння версій у межах кожної концепції.

Введение. Внедрение сетей связи нового поколения обусловливает создание информационных систем, способных предоставить пользователям более высокий уровень качества обслуживания. Среди множества требований, предъявляемых к свойствам подсистем качества обслуживания, наиболее важны требования по обеспечению конфиденциальности, целостности и доступности информационных ресурсов. С этой точки зрения разработка современных методов, алгоритмов и технологий обеспечения безопасности информационных ресурсов в компьютерных системах и сетях связи следующего поколения приобретает особую актуальность. В данной статье представлены результаты анализа, исследований и разработки вариантов реализации алгоритмов компьютерной косвенной стеганографии для потокового шифрования мультимедийной информации.

Постановка задачи

Предполагается, что между двумя информационными системами выполняется передача потока мультимедийной информации. Исходя из требований сетей связи нового поколения к параметрам соответствующих подсистем обеспечения качества обслуживания, ставится задача разработки методов и алгоритмов, способных обеспечить защиту передаваемого потока информации с требуемой криптографической стойкостью, определяемой ценностью потоковой информации.

Для решения поставленной задачи предлагается использовать метод косвенной стеганографии [1], представляющий собой развитие идей, заложенных в шифре Вернама, в одноразовых блокнотах и в «книжной» стеганографии, для современных компьютерных систем и сетей.

Анализ исследований и публикаций

Шифрование потоковой информации стало актуальным еще в начале прошлого века, с появлением средств для передачи сигналов по каналам электросвязи – телеграфов. Именно тогда (в 1917 г.) сотрудником *AT&T* Гильбертом Вернамом была изобретена система симметричного шифрования, получившая впоследствии название – *шифр Вернама*. В криптографии разновидность шифра Вернама известна также как *схема одноразовых блокнотов* (*one-time pad*) [2].

Большую популярность потоковым шифрам принесла работа Клода Шеннона «Теория связи в секретных системах» (1945 г.), которую рассекретили и опубликовали лишь в 1949 году. Исследуя шифр Вернама, Шеннон определил, что ключ имеет длину, равную длине передаваемого сообщения. Ключ используется в качестве гаммы, и если каждый бит ключа выбирается случайно, то вскрыть шифр невозможно (так как все открытые тексты будут равновероятны) [3].

Здесь уместно сослаться на известного современного специалиста в области прикладной криптографии Брюса Шнайера « …С помощью одноразовых блокнотов зашифрованы многие сообщения советских разведчиков. Эти сообщения не раскрыты до сих пор, и таковыми останутся навсегда. И эту задачу не решат никакие суперкомпьютеры. Даже когда чужаки из созвездия Андромеды приземлятся на нашей планете в своих огромных космических

кораблях с компьютерами невообразимой мощности, и они не смогут прочесть сообщения советских агентов… » [4].

Работа Шеннона послужила основой для обширных исследований в теории кодирования и передачи информации и, по всеобщему мнению, придала криптографии статус науки. Весомая заслуга Шеннона – исследование методов шифрования, доказательство существования абсолютно секретных систем и криптостойких шифров, выявление требуемых для этого условий. Шеннон также сформулировал основные требования, предъявляемые к надежным шифрам. Он ввел ставшие уже привычными понятия рассеивания и перемешивания, разработал методы создания криптостойких систем шифрования на основе простых операций [4].

Суть используемого Вернамом метода шифрования заключается в следующем: для создания шифротекста открытый текст объединяется операцией «исключающее ИЛИ» с ключом (называемым шифроблокнотом). При этом ключ должен обладать тремя критически необходимыми свойствами:

- быть истинно случайным;
- совпадать по размеру с заданным открытым текстом;
- применяться только один раз.

Задолго до появления компьютеров активно использовались потоковые шифры на базе сдвиговых регистров. Они были просты в проектировании и реализации. В 1965 г. Эрнст Селмер, главный криптограф норвежского правительства, разработал теорию последовательности сдвиговых регистров [5–7].

Для современной криптографии характерно применение известных алгоритмов шифрования, предполагающих сложные преобразования с использованием мощных вычислительных средств [8]. Известно более десятка проверенных алгоритмов шифрования, способных обеспечить высокий уровень криптографической стойкости генерируемых шифров [9, 10].

Существующие алгоритмы представлены тремя группами [11]:

- симметричные – *DES*, *AES*, ГОСТ 28147-89, *Camellia*, *Twofish*, *Blowfish*, *IDEA*, *RC*4 и др.;
- асимметричные – *RSA* и *Elgamal* (Эль-Гамаль) [11];
- хэш-функций – *MD*4, *MD*5, *SHA*-1, ГОСТ Р 34.11-94.

Что касается собственно идеи скрытия информации, то на данный момент известны два направления исследований, связанных с защитой компьютерной информации от несанкционированного использования.

1. *Компьютерная криптография* [12–14]. Информация, подлежащая защите, шифруется с помощью числовых ключей, причем с увеличением разрядности ключей возрастает вычислительная сложность преобразования. Существует множество вариантов реализации компьютерной криптографии. Общая схема такого шифрования представлена на рис. 1.

Рис. 1. Концепция компьютерной криптографии

2. *Компьютерная стеганография* [11]. Данные, подлежащие защите, смешиваются с определенным видом мультимедийной информации (аудио, видео, изображение и др.) и передаются законному пользователю. Разработано множество вариантов реализации этого метода. Общая схема стеганографического преобразования выглядит так (рис. 2).

Рис. 2. Концепция компьютерной стеганографии

Главный недостаток указанных методов состоит в том, что защищаемая информация (в зашифрованном или смешанном виде) передается по каналу, что позволяет криптоаналитику провести соответствующий анализ для взлома шифра и/или выделения полезных данных. К тому же при компьютерной стеганографии трудно реализовать передачу большого объема информации, а также передачу потоковых мультимедийных данных.

В данной статье основное внимание уделено потоковому шифрованию методом компьютерной косвенной стеганографии (рис. 3).

Рис. 3. Концепция косвенной стеганографии

Цель статьи – разработка различных версий реализации потокового шифрования информации методом косвенной стеганографии, а также последующее проведение предварительной оценки разработанных реализаций.

Дадим формальное определение косвенной стеганосистемы.

Совокупность $Œ = <C, @C, M, D, E>$, где C – множество контейнеров-ключей, $@C$ – множество параметров элементов множества C (множество косвенных контейнеров), M – множество секретных сообщений, $E_@$: $C \times M \rightarrow @C$, $D_@$: $C \times @C \rightarrow M$ − стеганографические преобразования со свойством $D_@(E_@(c, m), @c) = m$ для любых $m \in M$, $c \in C$ и $@c® \in @C$, представляет собой *косвенную стегосистему*.

Пусть

$M = \{♥_m, P_m, ®_m\}$; $C = \{H_c, □_c, ♥_m, D_c, \boldsymbol{P_c}, f_c, €_c, ®_c, G_{c...}\}$, $@C = \{@H_c{:}L, @□_c{:}S, @♥_m{:}\boldsymbol{A}, @D_c{:}⌘, @\boldsymbol{P_c}{:}⑨, @f_c{:}F, @€_c{:}t, @®_c{:}\boldsymbol{W}, @G_c{:}u...\}$.

В результате шифрования получаем $E_@$: $C \times M \rightarrow @C \rightarrow \{\boldsymbol{A}, ⑨, \boldsymbol{W}\}$ – образ исходного сообщения M, передаваемый по каналу связи.

После обратного преобразования (дешифрования) получим:

$D_@$: $C \times @C \rightarrow M = \{♥_m, P_m, ®_m, \}$.

Причем после шифрования $@C = \{@H_c{:}L, @□_c{:}S, @♥_m{:}⊙, @D_c{:}⌘, @\boldsymbol{P_c}{:}⊙, @f_c{:}F, @€_c{:}t, @®_c{:}⊙, @G_c{:}u... @♥_m{:}5, \ldots, \boldsymbol{P_c}{:}★, \ldots, @®_c{:}\boldsymbol{L}, \ldots\}$, где знак ⊙ означает «пусто».

Таким образом, если шифровать $M = \{♥_m, P_m, ®_m\}$ еще раз, шифр, передаваемый по каналу связи, будет представляться в следующем виде: $E_@$: $C \times M \rightarrow @C \rightarrow \{5, ★, \boldsymbol{L}\}$.

Следует оговорить, что в данной статье детально не рассматриваются:

- методы и алгоритмы передачи и синхронизации первичных ключей [15, 16];
- коллизии в канале передачи [17] и устойчивость к возможной модификации передаваемой информации (предполагается, что отправляемая информация в точности соответствует получаемой адресатом).

Методы решения задачи

Значительным преимуществом косвенной стеганографии является то, что открытая информация вообще не передается по каналу, вместо нее передается образ полезной информации. Выглядит это следующим образом. У отправителя и получателя имеются одинаковые секретные контейнеры-ключи. Поток информации, подлежащей защите, условно делится на сегменты, после чего проводится замена (по определенному алгоритму) сегментов полезной информации сегментами секретного контейнера-ключа. В результате получается образ исходной информации, как правило, такого же размера. Сегменты образа полезной информации можно в реальном времени передавать по каналу связи. При получении адресатом образ подвергается обратному преобразованию: его сегменты заменяются сегментами секретного контейнера–ключа, т.е. выполняется зеркальный алгоритм.

В зависимости от вида шифруемой информации могут быть реализованы различные версии рассматриваемого метода, а именно:

- наиболее ресурсоемкие – шифрование в реальном масштабе времени больших объемов информации в единицу времени, крайне критичное к скорости обработки, где не допускается промедление или отставание одной из взаимодействующих сторон (например, потоковое видео высокого разрешения);
- умеренно ресурсоемкие – шифрование небольших потоков информации в единице времени (например, голос) либо некритичные ко времени шифрование и передача потоковых данных (например, *WEB*-страницы).

В отличие от версии с умеренным потреблением системных ресурсов, для которой возможна реализация программным способом, в высокотребовательной версии реального времени необходимую производительность может обеспечить только аппаратно реализованная

криптосистема. В общем случае такая аппаратная реализация должна состоять из:

- цифрового сигнального процессора [18] – для выполнения вычислений в реальном масштабе времени;
- ассоциативной памяти [19], содержащей контейнер-ключ, для очень быстрого сопоставления сегментов (байтов) потока информации с содержимым контейнера–ключа;
- программируемой логической интегральной схемы [20], в которой заложена вся логика процесса обработки потока информации.

Основным элементом для шифрования методом косвенной стеганографии является секретный контейнер-ключ, который может:

- быть файлом, хранящимся во внешней памяти;
- быть массивом в оперативной памяти;
- генерироваться в реальном времени.

Контейнер-ключ может использоваться:

- циклически – после того как все элементы контейнера-ключа были использованы, начинается их повторное использование по циклу (это очень простая, но ненадежная реализация, так как не соответствует требованию о неповторяемости ключа);
- циклически со случайно выбранной позиции;
- одноразово – после того как все элементы контейнера-ключа были использованы, генерируется новый (следующий) контейнер-ключ. Такой подход может обеспечить требуемый уровень криптозащиты, но его реализация связана с рядом сложностей.

Контейнер-ключ может заполняться:

1. Истинно случайными числами, источниками которых могут служить:

- *физические шумы* – детекторы событий ионизирующей радиации, шум в резисторе, космическое излучение и др.;
- *бинарные файлы*, мультимедиа-файлы, системные библиотеки;
- содержимое дорожек жесткого диска со случайно выбранных позиций.

2. Псевдослучайными числами [21], для получения которых используются детерминированные алгоритмы. Возможны следующие варианты реализации:

- отправителю и получателю *задана формула*, согласно которой выполняется генерация псевдослучайных чисел, но *не заданы начальные значения* (параметры формулы); эти параметры будут генерироваться и передаваться от отправителя к получателю в шифрованном виде при каждой инициализации процесса заполнения контейнера-ключа;
- отправителю и получателю заранее *заданы начальные значения* (параметры формулы), но *не задана формула*, согласно которой будет выполняться процесс заполнения контейнера–ключа; эта формула, выбранная из заданного списка, будет передаваться в шифрованном виде адресату при инициализации процесса заполнения контейнера-ключа;
- отправителю и получателю *не заданы формула и начальные значения* (параметры формулы); при каждой инициализации процесса заполнения контейнера-ключа на первой системе из заданного списка будет выбрана формула и передана на вторую систему в шифрованном виде; при этом на второй системе будут сгенерированы параметры формулы и переданы на первую систему.

В зависимости от требований к криптоустойчивости и вычислительной мощности оборудования, выполняющего шифрование/дешифрование, выбирается метод генерации контейнера-ключа (рис. 4).

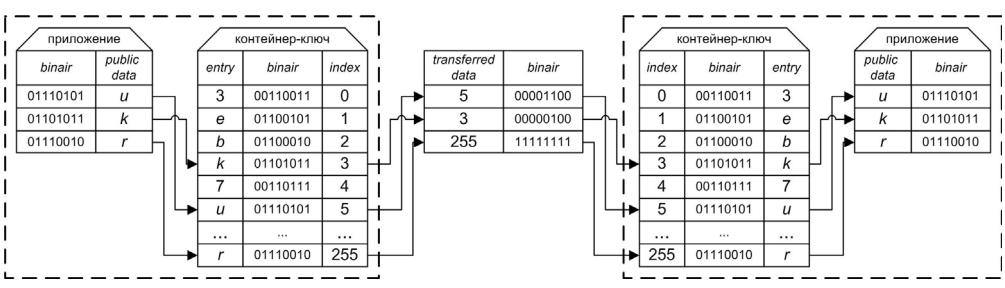

Рис. 4. Общий алгоритм использования контейнера-ключа

В процессе работы с контейнером-ключом после нахождения совпадения текущий элемент помечается в контейнере-ключе как уже использованный либо удаляется, что исключает повторное его использование.

Потоковые контейнеры-ключи могут быть двух видов:

- сгенерированные по детерминированному алгоритму [6];
- получаемые при использовании *online*-вещания.

Поиск совпадений при этом будет проводиться в реальном времени, по мере поступления потока открытой информации.

Рассматриваемые алгоритмы рассчитаны на использование в устанавливаемой на ЭВМ криптосистеме с клиент-серверной архитектурой (рис. 5).

Далее будут представлены отдельные варианты реализации рассматриваемого алгоритма и дана предварительная оценка их достоинств и недостатков. Каждая из версий базируется на определенной концепции (генератор псевдослучайных чисел [21], бинарные файлы, *online*-потоковое вещание) и использовании определенного контейнера-ключа.

Представленные концепции и основанные на них версии алгоритма различаются настолько, что проведение объективного сравнения практически невозможно. Поэтому сравнение версий алгоритма будет выполнено отдельно в рамках каждой конкретной концепции (табл. 1–3).

Таблица 1. Концепция 1: шифрование на основе генератора псевдослучайных чисел [21]

Версии	Используются заранее заполненные массивы в качестве контейнера–ключа	Генерируется потоковый контейнер-ключ по мере поступления потока информации
Достоинства	✓ Меньше нагрузка на вычислительную подсистему (нет необходимости генерировать контейнер-ключ в реальном времени) ✓ Автономность (независимость от возможных внешних источников контейнера-ключа)	✓ Упрощенная реализация (нет необходимости в промежуточном контейнере–ключе) ✓ Автономность (независимость от возможных внешних источников контейнера-ключа)
Недостатки	✓ Ограниченная длина ключа (как любой детерминированный алгоритм, имеет ограниченную длину периода) ✓ Сложность реализации (для обеспечения высокой производительности необходима полностью аппаратная реализация)	

Для реализации третьей концепции необходимо соблюдение следующих ключевых условий:

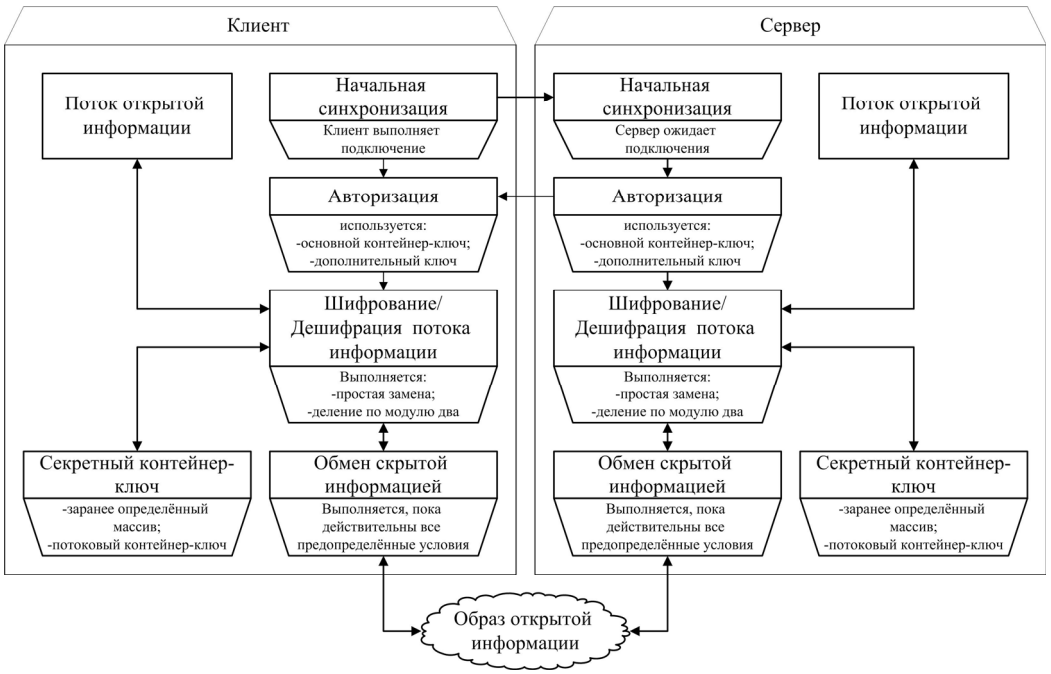

Рис. 5. Взаимодействие ЭВМ с установленными криптосистемами

- передача видеопотока должна вестись в режиме *multicast* [22] для гарантирования получения обеими взаимодействующими системами одинаковой информации.
- для передачи *online*-потока следует использовать транспортный протокол *TCP*, чтобы гарантировать целостность получения данных [23].

Заключение. Поскольку передача

потоковой информации является неотъемлемой частью практически любой информационной системы, появление предлагаемой криптосистемы с высокими показателями криптоустойчивости и скорости обработки информации можно оценивать как развитую систему при передаче защищенной потоковой информации, что, безусловно, вызовет интерес потенциальных потребителей.

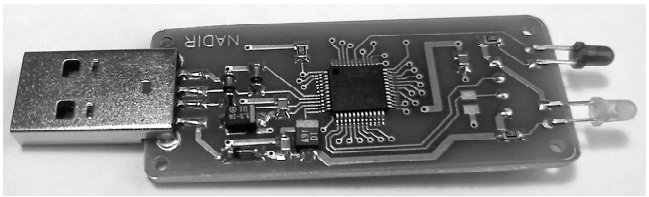

Рис. 6. Опытный образец косвенного стеганографа

Таблица 2. Концепция 2: шифрование на основе бинарных файлов

Версии	В качестве контейнера–ключа используются любые файлы, доступные для свободной загрузки из Интернета	В качестве контейнера-ключа используются системные бинарные файлы
Достоинства	✓ Контейнер-ключ содержит истинно случайные числа ✓ Файлы, используемые в качестве контейнера-ключа, доступны для загрузки всех криптосистем	✓ Контейнер-ключ содержит истинно случайные числа ✓ Файлы, используемые в качестве контейнера-ключа, одинаковы в соответствующих ОС
Недостатки	✓ Небезопасность (файлы, используемые в качестве контейнера-ключа, доступны для загрузки на всех системах, в том числе и на системе возможного злоумышленника) ✓ Сложность реализации (для обеспечения высокой производительности необходима полностью аппаратная реализация) ✓ Медлительность (для работы с файлами необходимо обращение к внешней памяти) ✓ Повышенная нагрузка на канал связи (при загрузке файлов, используемых в качестве контейнера-ключа)	✓ Небезопасность (файлы, используемые в качестве контейнера-ключа, одинаковы в соответствующих ОС, в том числе и на системе возможного злоумышленника) ✓ Сложность реализации (для обеспечения высокой производительности необходима полностью аппаратная реализация) ✓ Медлительность (для работы с файлами необходимо обращение к внешней памяти)

Для выполнения операций шифрования/дешифрования в реальном масштабе времени больших объемов информации (потоковое видео высокого разрешения и др.) в состав такой системы необходимо включить аппаратные средства, реализующие рассмотренные версии алгоритма. В перспективе планируется спроектировать и изготовить такую криптосистему на базе процессора цифровой обработки сигналов.

Таблица 3. Концепция 3: шифрование на основе *online*-потокового вещания

Версии	Используется цифровое *online*-вещание телевидения	Используется цифровой *online*-сигнал от *WEB*-камер реального времени
Достоинства	✓ Нет необходимости в промежуточном контейнере-ключе ✓ *Online*-поток содержит истинно случайные числа ✓ *Online* -поток имеет неограниченную длину	✓ Нет необходимости в промежуточном контейнере-ключе ✓ *Online* -поток содержит истинно случайные числа ✓ *Online* -поток имеет неограниченную длину
Недостатки	✓ Небезопасность (*online*-поток можно получать на всех системах, в том числе и на системе злоумышленника) ✓ Автономность (независимость от возможных внешних источников контейнера-ключа) ✓ Повышенная нагрузка на канал связи (при получении *online*-потока) ✓ Сложность реализации (для обеспечения высокой производительности необходима полностью аппаратная реализация) ✓ В случае большого количества ошибок при соединении/подтверждении получаемой информации передаваемые данные могут утратить актуальность. Возможны значительные задержки при передаче информации на время, затраченное на пересылку поврежденных данных	✓ Небезопасность (*online* -поток можно получать на всех системах, в том числе и на системе злоумышленника) ✓ Необходим промежуточный сервер для ретрансляции в режиме *multicast* и трансляции из *UDP* в *TCP* [24, 25] ✓ Автономность (независимость от возможных внешних источников контейнера-ключа) ✓ Повышенная нагрузка на канал связи (при получении *online* -потока) ✓ Сложность реализации (для обеспечения высокой производительности необходима полностью аппаратная реализация) ✓ В случае большого количества ошибок при соединении/подтверждении получаемой информации передаваемые данные могут утратить актуальность. Возможны значительные задержки при передаче информации на время, затраченное на пересылку поврежденных данных

С точки зрения авторов, наилучшей реализацией методов косвенной стеганографии явля-

ются аппаратные средства, работающие с массивами истинно случайных последовательностей, генерируемыми в реальном масштабе времени.

Безусловно, все это требует дополнительных как научных, так и прикладных исследований. Однако опыт авторов, полученный в результате интеграции аппаратных и программных средств, показывает, что это позволит на практике достичь высокого уровня криптоустойчивости, предъявляемого бесчисленными бизнес-приложениями.

1. *Алишов Н.* Косвенная стеганография // INFORMATION SCIENCE&COMPUTING. − 2009. − N 11. − P. 53−58.
2. *Зубов А.Ю.* Совершенные шифры. – М.: Гелиос АРВ, 2003. – 159 с.
3. *Шеннон К.* Работы по теории информации и кибернетике. – М.: Иностр. лит., 1963. – 830 с.
4. *Ященко В.В.* Введение в криптографию. – М.: МЦНМО, 2000. – 288 с.
5. *Жельников В.* Криптография от папируса до компьютера. – М.: АВР, 1996. – 56 с.
6. *Сборка* и перевод зарубежных исследований. Поточные шифры. Результаты зарубежной открытой криптологии. – М.: 1997. – 390 с.
7. *Solomon Wolf Golomb*. Shift Register Sequences. – S. Francisco: Holden-Day, 1967. – 484 p.
8. *Серов Р.Е.*, *Баричев С.Г.* Основы современной криптографии. – М.: Горячая линия-Телеком, 2001. – 152 с.
9. *Гатчин Ю.А.*, *Коробейников А.Г.* Основы криптографических алгоритмов: Учеб. пособие. – СПб.: ИТМО, 2002. – 29 с.
10. *Грушо А.А.*, *Применко Э.А.*, *Тимонина Е.Е.* Анализ и синтез криптоалгоритмов: Курс лекций. – М.: СОЛОН-Р, 2000. – 110 с.
11. *Шнайер Б.* Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 610 с.
12. *Коутинхо С.* Введение в теорию чисел. Алгоритм RSA. – М.: Простмаркет, 2001. – 321 с.
13. *Баричев С.* Криптография без секретов. – М.: Новый изд. дом, 2005. – 43 с.
14. *Щербаков Л.Ю.*, *Домашев А.В.* Прикладная криптография. Использование и синтез криптографических интерфейсов. – М.: Русская редакция, 2003. – 405 с.
15. *Салоома А.* Криптография с открытым ключом. – М.: Мир, 1995. – 309 с.
16. *Сидельников В.М.* Алгоритм выработки общего ключа с помощью квантового канала связи // Проблемы передачи информации. – 1999. – Т. 35, **1**. – С. 100–109.
17. *Транников Ю.В.* О корреляционно-иммунных и устойчивых булевых функциях // Дискретная математика. – 2006. – Т. 18, **3**. – С. 120–137.
18. *Interfacing* Micron Â® MT9V022 Image Sensors to Blackfin Â® Processors. – http://www.analog.com/uploadedfiles/application_notes/213595899ee_258r262006.pdf
19. *Dan Ventura*, *Tony Martinez*. Quantum associative memory, 2000. – http://arxiv.org/pdf/quant-ph/9807053.pdf
20. Programmable Logic Devices. – http://cc.ee.ntu.edu.tw/~ywchang/Papers/pla.ps
21. *Иванов М.А.*, *Чугунков И.В.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: Кудиц-образ, 2003. – 229 с.
22. *Unicast-Based* Multicast Communication in Wormhole-Routed Networks / Philip K. Mckinley, Philip K. Mckinley, Hong Xu et. al. // Proc. of IEEE Transactions on Parallel and Distributed Systems, 1994. – ftp://ftp.cps.msu.edu/pub/acs/reports/msu-cps-acs-57.ps.Z
23. *Characterization* and Evaluation of TCP and UDP-Based Transport On Real Networks / R. Les Cottrell, Saad Ansari, Parakram Kh et. al., 2005. – http://www.slac.stanford.edu/cgi-wrap/getdoc/slac-pub-10996.pdf
24. *Ion Stoica*, *T.S. Eugene Ng*, *Hui Zhang*. REUNITE: A Recursive Unicast Approach to Multicast // Proc. of IEEE INFOCOM'00 (Tel-Avivu, 2000). – P. 10.
25. *Athina P.* Markopoulou, Fouad A. Tobagi. Hierarchical reliable multicast: Performance analysis and placement of proxies, 2000. – http://www.sprintlabs.com/People/amarko/./PAPERS/ngc00-corrected.ps

Поступила 30.03.2010

Тел. для справок: (044) 526-3427 (Киев)