УДК 621.391

В.В. Васильев, Г.Г. Гроздов

СОВРЕМЕННЫЕ АЛГОРИТМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Введение

Обеспечение собственной безопасности – задача первостепенной важности для любой системы независимо от ее сложности и назначения, будь то социальное образование, биологический организм или система обработки информации.

Применительно к информационным технологиям в настоящее время особую значимость приобретает проблема безопасности этих технологий. Широкое внедрение популярных дешевых компьютерных систем массового применения спроса делает их чрезвычайно уязвимыми к деструктивным воздействиям. Главная тенденция, характеризующая развитие современных информационных технологий – рост числа компьютерных преступлений и связанных с ними хищений конфиденциальной и иной информации, а также материальных потерь [3,4,25].

Проблемой обеспечения секретности информации занимается криптология. Криптология состоит из двух разделов: криптографии и криптоанализа. Цели этих направлений противоположны: криптография занимается разработкой способов преобразования информации для ее засекречивания, а криптоанализ – для прочтения засекреченной информации.

Данная работа посвящена рассмотрению вопросов криптографии.

Классификация современных методов криптографической защиты информации

В настоящее время определены требования к методам криптографической защиты информации [6, 14,16,17,19,20].

Все существующие на сегодня методы криптографической защиты информации можно разделить на такие группы методов [7,8]:

- методы хеширования;
- методы кодирования;[1]
- методы шифрования;
- комбинированные методы.

Методы *хеширования* представляют собой одностороннее преобразование данных. Под односторонним преобразованием будем понимать такие действия над входными данными, чтобы из шифрованного текста было невозможно получить исходный текст.

По соотношению размеров открытого и шифрованного текстов все методы криптографической защиты информации можно разделить на методы кодирования и методы шифрования.

Методами *кодирования* будем называть такое преобразование данных, при котором длина выходной последовательности отличается от длины входной последовательности.

Методы *шифрования* представляют такое преобразование данных, при котором длина входной последовательности равна длине выходной последовательности.

Комбинированные методы преобразования данных могут включать несколько перечисленных выше методов. Например, входная последовательность сначала кодируется, а затем шифруется.

Классификация методов шифрования

К основным характеристикам современных методов шифрования можно отнести:

длину ключа;

---

[1] В эту статью не входит рассмотрение и классификация современных методов кодирования данных

- сложность алгоритма преобразования данных;
- размер обрабатываемых данных;
- способ работы с ключами и т.д.

Ввиду вышеизложенного, существующие методы шифрования можн классифицировать по следующим признакам:

По размерам обрабатываемых данных:

- блочные методы шифрования;
- поточные методы шифрования.

По способу работы с ключами:

- симметричные методы шифрования;
- асимметричные методы шифрования.

Рассмотрим более подробно перечисленные классы методов.

Если для прямой и обратной операции преобразования информации применяет один и тот же ключ, то алгоритм шифрования называется *симметричным* (или алгоритмо шифрования с секретным ключом). В качестве наиболее популярных на сегодняшний де симметричных методов шифрования назовем DES, Triple DES,RC2, RC5, BLOWFISH, IDE ГОСТ 28147-89 и др.

Довольно популярны также методы асимметричного шифрования или шифрования открытым ключом. В этих методах используются два неодинаковых ключа, приче сообщение, зашифрованное одним ключом из пары, расшифровывается только други ключом из этой же пары и наоборот. Применяя такие алгоритмы, удается избежа начального обмена секретными ключами, поэтому они более удобны для обмена секретно информацией между пользователями компьютерной сети.

Кроме методов использования ключей, алгоритмы различаются также и способам обработки исходной информации. В так называемых *блочных алгоритмах* данны преобразуются блоками определенного размера (обычно 64 бита и более). Другие алгоритм предназначены для *поточного шифрования* – побайтового или побитового – передаваемо информации и обычно работают очень быстро (заметно быстрее алгоритмов блочно шифрования).

Перейдем к подробному рассмотрению особенностей методов криптографическо защиты информации.

Хеш-функции

Алгоритм хеширования – это последовательность математических преобразований, результате которых из некоторой двоичной последовательности переменной длин получается уникальная двоичная последовательность фиксированной длины. Функци реализующая такой алгоритм, называется *хеш-функцией*.

Чтобы преобразование данных можно было назвать хеш-функцией, оно должн одновременно удовлетворять следующим условиям [13,21]:

- обрабатывать последовательности различной длины;
- выдавать в качестве результата битовую последовательность фиксированно длины;
- достаточно просто вычисляться при любой входной информации;
- обладать свойством необратимости, когда для полученного результат невозможно получить входное значение;
- быть однозначной (т.е. для различных входных последовательностей н должны быть построены одинаковые хеш-образы).

С криптографической точки зрения, последние два свойства хеш-функции наиболе важны, так как обеспечивают несовпадение хешированных форм, например паролей разны пользователей, и усложняют задачу вскрытия этих паролей. Поэтому такого рода функци

довольно широко применяются в компьютерных системах для обеспечения безопасности при передаче и хранении информации.

Они могут применяться, в частности, в приложениях, обеспечивающих электронную подпись. В таких приложениях текст сообщения обычно обрабатывается с помощью хеш-функции, а результат последней шифруется по какому-либо алгоритму, что и дает цифровую подпись. Этот подход позволяет ускорить вычисление цифровой подписи, поскольку она вычисляется не для всего сообщения, а для его хеш-образа фиксированной длины.

Кроме того, в информационных системах может использоваться хранение хеш-образов паролей [20].

Перейдем к сравнению наиболее популярных в настоящее время алгоритмов хеширования.

Для сравнения алгоритмов хеширования использовались такие показатели, как размер выходного блока, сложность алгоритма преобразования и стойкость к криптоатакам[2]. В таблице 1 приведены параметры наиболее распространенных алгоритмов хеширования.

Таблица 1

Параметры алгоритмов хеширования

Алгоритм хеширования	Размер выходного блока (бит)	Количество циклов преобразования в алгоритме	Стойкость к криптоатакам
MD2	128	2	5
MD4	128	3	4
MD5	128	4	3
SHA-1	160	4	2
ГОСТ Р34.11-94	256	6	1

Из таблицы сравнения можно сделать следующие выводы.

Самым медленным алгоритмом является MD2. Это вызвано тем, что он ориентирован на 8-разрядную архитектуру. Кроме того, в алгоритме невысокая однозначность.

Что касается алгоритма MD4, он оптимизирован для 32-разрядной архитектуры. Однако, как показали исследования, он недостаточно устойчив к криптоатакам.

Алгоритм MD5 очень похож на MD4. Входное сообщение подвергается не 3, а 4 циклам преобразования. Ввиду этого алгоритм выполняется дольше, зато обладает большей стойкостью к различного рода криптоатакам.

Алгоритм SHA-1 опубликован как федеральный стандарт США. Последовательность преобразований входного сообщения аналогична алгоритмам MD4 и MD5. Однако больший размер получаемого результата (160 бит) обеспечивает алгоритму более высокую устойчивость к взломам методом перебора.

По мнению автора, наилучшим алгоритмом хеширования является ГОСТ Р34.11-94. Вызвано это следующими обстоятельствами: в алгоритме используется 256-битный вектор инициализации (аналог ключа шифрования). Кроме того, в алгоритме преобразования обладает большей вычислительной сложностью из рассмотренных алгоритмов.

Криптографические системы с секретными ключами

Любая криптографическая система с секретными ключами состоит из следующих частей: источника сообщений, шифратора, дешифратора, и получателя сообщений. Важнейшей частью таких систем является "защищенный канал", по которому источник сообщает получателю сообщений ключ преобразования данных.

[2] Стойкость оценивается по 5-бальной шкале: 1- максимальная , 5- минимальная оценки

Для шифрования и дешифрования данных используется один и тот же ключ, поэтому подобные системы называют также *симметричными* криптосистемами.

Подобная схема была рассмотрена Шенноном в работе [22].Шеннон рассматривал вопрос о стойкости подобных систем. Вначале он поставил вопрос о теоретической стойкости: насколько надежна система, если криптоаналитик противника не ограничен временем и обладает средствами для анализа шифрованных сообщений ? Вопрос был решен, однако Шеннон пришел к такому выводу: объем секретного ключа для построения теоретически стойкого шифра будет таким большим, что его невозможно будет реализовать практически.

Поэтому Шеннон рассмотрел также вопрос практической стойкости: надежна ли система, если криптоаналитик располагает ограниченным временем и вычислительными возможностями для анализа перехваченных сообщений ?

Шеннон показал, что для решения задачи практической стойкости криптосистем необходимо учитывать следующие обстоятельства [23]:

- необходимо периодически менять секретные ключи (в противном случае криптоаналитику противника рано или поздно удастся определить закон преобразования сообщений, и все шифрованные сообщения могут быть прочитаны им);
- необходимо также уделять внимание длине используемых ключей (при использовании секретного ключа малой длины сообщение может быть расшифровано методом полного перебора ключей).

Перейдем к сравнению наиболее популярных криптографических алгоритмов с секретными ключами. Каждый алгоритм оценивается по следующим параметрам: размеры входного и выходного блоков, размер ключа, сложность алгоритма преобразования данных, скорость преобразования данных и стойкость к криптоатакам. Результаты сравнения представлены в Таблице 2[3].

Таблица 2

Параметры современных криптографических систем с секретными ключами

Алгоритм	Размер входного блока (бит)	Размер выходного блока (бит)	Размер ключа (бит)	Количество циклов преобразования в алгоритме	Стойкость	Скорость
BLOWFISH	64	64	448	16	2	3
DES	64	64	56	16	3	5
FEAL	64	64	64	от 4 до 32	4	4
IDEA	64	64	128	12	5	2
RC5	32 или 64 или 128	32 или 64 или 128	от 0 до 2040	от 0 до 255	6	1
ГОСТ 28147-89	64	64	256	32	1	6

Стойкость алгоритмов шифрования с секретными ключами рассматривалась по следующим критериям:

- размер ключа;
- сложность преобразования данных;

---

3 Стойкость алгоритма и скорость преобразования данных оценивались по 6-бальной шкале (1-максимальная, 6- минимальная оценка)

- время существования алгоритма.

С точки зрения криптоанализа немаловажную роль играет время существования алгоритма. Так, если алгоритм шифрования используется достаточно длительное время и становится популярным, то он становится привлекательной целью для криптоаналитиков. Так как при раскрытии такого алгоритма противник сможет получить большую прибыль, то на раскрытие алгоритма шифрования будут выделены большие вычислительные ресурсы. Если закон преобразования, используемый в алгоритме, не является секретным, шансы противника на успех возрастают.

Ярким примером распространенного алгоритма шифрования может выступать алгоритм DES [11]. В [16] приведены доводы против использования стандарта шифрования.

В современных информационных системах методы симметричного шифрования могут применяться для защиты данных, передаваемым по открытым каналам связи, для хранения информации на дисках в шифрованном виде и т.д.

По мнению автора, наиболее стойким к криптоатакам противника является алгоритм шифрования ГОСТ 28147-89. Однако этот алгоритм преобразования является самым "медленным" среди рассмотренных.

Криптография с открытым ключом

С развитием сетевых компьютерных технологий и их внедрением, возникла потребность в новых подходах к криптографическому закрытию данных.

Первой встала проблема рассылки ключей в сети. Если два человека, которые никогда ранее не встречались, должны передать друг другу секретные данные, используя классические средства криптографии, то им необходимо каким-то образом заранее договориться о ключе, который будет известен только им обоим и никому более.

Второй проблемой была проблема электронной подписи. Существует ли метод, который бы позволял получателю цифрового электронного сообщения демонстрировать другим людям, что оно пришло от конкретного лица ?

На первый взгляд, эти две проблемы требуют невозможного.

В первом случае, если два человека, не встречаясь, могут как-то передать друг другу секретный ключ, то почему они не могут передать друг другу сообщение ? Вторая проблема не легче. Подпись будет эффективной только тогда, когда ее трудно подделать. Может ли тогда цифровое сообщение, которое легко скопировать, нести подпись ?

Открытие новых методов состояло не в решении этих проблем, а в признании того, что эти две проблемы, каждая из которых казалась неразрешимой по определению, могут быть в принципе разрешены, и что решения входят в один пакет.

Новые методы были основаны на применении NP - полных задач [1,10]. Функции, основанные на NP - полных задачах вычисляются достаточно легко, но обратное преобразование невозможно или требует огромное числа вычислений. Таким образом, криптоаналитик будет поставлен в затруднительную ситуацию: владея перехваченным сообщением и даже зная метод преобразования данных, он не сможет расшифровать сообщение за требуемое время.

В результате проведенных исследований были выбраны такие примеры NP - полных задач для построения асимметрических методов шифрования:

- дискретное возведение в степень;
- разложение чисел на простые множители;
- другие задачи (задача об укладке ранца [1]);

Новые методы шифрования стали использовать два ключа: секретный и открытый. Поэтому новые методы шифрования получили название *асимметричных* или *криптографии с открытым ключом*.

Наличие двух ключей упрощает установление сеанса связи между сторонами. В рамках метода шифрования с асимметричными ключами отправитель и получатель

информации сначала обмениваются своими открытыми ключами. Отправитель шифрует сообщение с помощью *открытого ключа* получателя, а получатель может расшифровать это сообщение, используя свой *закрытый ключ*, который известен только его владельцу. Получатель сообщения также может использовать открытый ключ отправителя, чтобы зашифровать пересылаемое тому сообщение. Расшифровать его можно только с помощью парного закрытого ключа. Самой популярной системой шифрования с открытым ключом является RSA.

Цифровая подпись строится следующим образом: по заранее известному алгоритму формируется дайджест передаваемого сообщения, далее с помощью секретного ключа отправителя асимметричный алгоритм генерирует цифровую подпись сообщения. Получатель проверяет валидность сообщения с помощью открытого ключа отправителя.

В задачу публикации не входит описание асимметричных методов шифрования, они достаточно подробно изложены в [5, 12, 14]. Перейдем к сравнению алгоритмов. Оценка проводится по следующим критериям: используемые NP-полные задачи и скорость работы алгоритмов. Результаты сравнения приведены в таблице 3[4].

Таблица 3

Сравнение асимметричных методов шифрования

Алгоритм	Используемые NP-полные задачи	Скорость работы
Месси-Омуры	Дискретное возведение в степень	4
Диффи-Хеллмана	Дискретное возведение в степень	2
Эль-Гамаля	Дискретное возведение в степень	3
RSA	Дискретное возведение в степень, разложение числа на множители	5
Ранцевая система	Задача укладки ранца	1

Самым стойким из существующих алгоритмов считается RSA. В 1995 году лишь однажды удалось раскрыть шифр RSA для 500-значного ключа. Для этих целей было задействовано 1600 компьютеров добровольцев на протяжении 5 месяцев непрерывной работы. Следует отметить, что при использовании системы RSA с ключами длиной 512-1024 бит взломать шифры будет практически невозможно.

В качестве примера, подтверждающего тезис о большой важности выбранной NP-полной задачи для построения асимметричного алгоритма, может быть ранцевая система. Как оказалось, за два года использования ранцевых систем криптоаналитикам удалось разработать методику решения подобных задач. Поэтому подобные системы в настоящее время не используются.

Алгоритмы асимметричного шифрования применяются для решения многих задач: аутентификация пользователей и сообщений, генерация сеансовых ключей в информационных системах, для систем опознавания "свой-чужой" и т.д.

Ввиду того, что асимметричные алгоритмы обладают большой вычислительной сложностью, в современных информационных системах их применяют для генерации и распространения сеансовых ключей. Для шифрования передаваемых сообщений используют симметричные алгоритмы шифрования.

В настоящее время в странах Западной Европы и США ведется поиск новых NP - полных задач для использования в асимметричных криптоалгоритмах [9].

[4] Скорость преобразования данных оценивались по 5-бальной шкале (1-максимальная, 5- минимальная оценка)

Проблемы и перспективы развития криптографических систем

По мнению автора, в настоящий момент существуют следующие проблемы криптографических систем:

- преобразование сообщений большого объема;
- применение методов сжатия и кодирования данных;
- распределение сеансовых ключей;
- нахождение способов решения существующих NP-полных задач.

Перейдем к рассмотрению сути проблемы.

Преобразование сообщений большого объема

Развитие сетей передачи данных и мультимедийных средств остро поставило вопрос защиты сообщений большого объема.

До сих пор речь шла о криптографическом преобразовании текстовых сообщений. В настоящее время начинают применяться информационные технологии, при которых происходит передача больших объемов данных в реальном масштабе времени. К таким технологиям можно отнести системы видеоконференций, видео- и голосовую почту, факсимильную и модемную почту.

В подобных системах необходимо обеспечить надежную защиту передаваемой информации с одной стороны, и высокую скорость преобразования и передачи – с другой.

Решением подобной проблемы может быть применение поточных методов шифрования данных. Эти методы обладают рядом преимуществ.

Во-первых, они могут работать с блоками данных любых размеров. При использовании блочных методов шифрования могла возникнуть искусственная задержка, вызванная необходимостью ожидания заполнения блока перед началом его преобразования.

Во-вторых, поточные методы шифрования обладают высокой скоростью преобразования данных.

Применение методов сжатия и кодирования данных

При рассмотрении вопросов теоретической и практической стойкости криптосистем Шеннон показал [22,23], что чем выше избыточность текста, тем выше вероятность того, что он будет раскрыт криптоаналитиком противника.

Известно, что любой язык обладает определенной избыточностью. Например, русский язык менее избыточен, чем английский. Заранее зная частоту появления отдельных символов в открытом тексте, криптоаналитик сможет прочесть шифрованный текст достаточно большого объема.

Для решения этой проблемы необходимо использовать в комплексе с методами шифрования данных также методы сжатия и кодирования. Перечисленные методы преобразования данных эффективно дополнят друг друга, и их совместное применение позволит использовать открытые каналы связи для передачи сообщений.

Методы сжатия позволят значительно уменьшить объем передаваемых или хранимых данных, методы кодирования – защитят передаваемую информацию от помех и ошибок в каналах связи. Шифрование защитит информацию от прочтения ее посторонними.

Таким образом, сначала открытый текст должен подвергаться сжатию, затем его необходимо зашифровать, затем кодировать.

Кроме того, применение подобного подхода способно решить проблему криптографического преобразования сообщений большого объема.

Распределение сеансовых ключей

В крупных информационных системах на сегодняшний день высокую актуальность приобрела проблема распределения сеансовых ключей. Частично эта проблема может быть решена за счет использования криптосистем с открытыми ключами. Однако современные асимметричные алгоритмы обладают большой вычислительной сложностью и их применение не всегда оправдано.

В настоящее время существует два подхода к решению данной проблемы: использование центра распределения ключей (далее - ЦРК) и использование "блуждающих ключей". Каждый из подходов имеет свои преимущества и недостатки. Перейдем к их рассмотрению.

Первый подход предполагает наличие в составе информационной системы отдельного компонента (центра распределения ключей), отвечающего за генерацию и выдачу ключей сеанса каждому абоненту. Перед началом сеанса работ две стороны обращаются к такому компоненту за ключами, необходимыми для работы.

Преимущества подобного подхода состоят в следующем: сосредоточение способов генерации сеансовых ключей в одном месте, упрощение администрирования работы системы.

Недостатками являются высокая уязвимость системы в случае выхода из строя ЦРК. Кроме того, злоумышленник может создать средство, которое имитирует работу ЦРК.

Второй подход предполагает замену ключей взаимодействия по некоторому правилу, которое известно двум обменивающимся сторонам. Ключи могут изменяться как в начале нового сеанса, так и периодически в течении одного сеанса.

Преимуществом данного подхода является более простой способ установления связи между сторонами.

Недостатки – в случае нарушения правила замены ключей на одной из сторон взаимодействие сторон будет прервано. Кроме того, правила замены ключей хранятся во многих местах и могут быть вычислены криптоаналитиком противника.

Нахождение способов решения существующих NP-полных задач

За последнее десятилетие криптография с открытым ключом превратилась из новой концепции в опору криптографической технологии. В ближайшее время асимметричных алгоритмов преобразования приобретут большую популярность, что привлечет к ним внимание многих криптоаналитиков.

К сожалению, технологическая база криптографии с открытым ключом является недостаточно развитой. За исключением схемы Макэлиса [25], которая была разработана с целью противостояния известным методам криптоанализа, фактически все алгоритмы цифровой подписи и криптографии с открытым ключом в качестве NP-полной задачи используют операцию возведения в степень по модулю произведения простых чисел.

Таким образом, учитывая большие достижения в решении задач разложения и вычисления дискретных алгоритмов, они становятся все более уязвимыми.

Из вышеизложенного следует, что при разработке новых криптосистем большое значение следует уделять выбору NP-полной задачи [9,14].

Заключение

На сегодняшний день существуют апробированные и хорошо зарекомендовавшие себя методы криптографической защиты данных. Их стойкость к атакам доказана математически либо сводится к решению сложной математической задачи. Казалось бы, применение подобных методов в информационных системах должно обеспечить конфиденциальность защищаемой информации.

Тем не менее, в средствах массовой информации периодически появляются сообщения о найденных "дырах" в системах защиты информации или о фактах "взлома" подобных систем.

Попытаемся объяснить данное противоречие.

Как было отмечено в предыдущих разделах, методы криптографической защиты являются лишь *малой частью* систем защиты информации. Использование в таких системах криптографически стойких методов вовсе не гарантирует того, что подобная система не может быть взломана нарушителем.

Приложение 1Терминология

В приложении приведены термины, которые использованы в работе.

Алфавит - конечное множество используемых для преобразования информации знаков.

Дешифрование - обратный шифрованию процесс, при котором на основе ключа шифрованный текст преобразуется в исходный.

Ключ - информация, необходимая для беспрепятственного криптографического преобразования текстов. Обычно представляет собой последовательный ряд символов того же алфавита, в котором набрано информационное сообщение.

Криптоанализ- процесс получения исходного теста без знания ключа.

Криптостойкость - характеристика метода преобразования данных, определяющая его стойкость к криптоанализу. Измеряется в MIPS-часах или MIPS-годах.

Пространство ключей - набор всех возможных значений ключа.

Текст - набор элементов алфавита, имеющих определенный смысл.

Криптографическое преобразование - преобразовательный процесс, при котором исходный текст заменяется шифрованным текстом.

Эффективность криптоалгоритма - отношение временных затрат критоаналитика на вскрытие шифрованного текста к временных затратам на создание шифрованного текста.

Хеширование - одностороннее преобразование данных.

Кодирование - криптографическое преобразование данных, при котором длина входной последовательности отличается от длины выходной последовательности.

Шифрование - криптографическое преобразование данных, при котором длина входной последовательности равна длине выходной последовательности.

Список литературы

1. Ахо А., Хопрокфт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М: Мир, 1979.-536 с.

2. Беляев В.И. Безопасность в распределенных системах. Открытые системы. 1995, №3, сс 36-39.

3. Ведев Д.Л. Защита данных в компьютерных сетях. Открытые системы. 1995, №3, сс 12-16.

4. Вехов В.Б. Преступления в сфере высоких технологий. Десять лет - это только начало.Конфидент.2000, №6,

5. Герасименко В.А, Размахнин М.К, Диев С.А. Новые данные о защите информации в автоматизированных системах обработки данных. Зарубежная радиоэлектроника . 1987 .№ 9. с 48-75 .

6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Книги 1,2. М.: Энергоатомиздат, 1994.- 400 с. и 176 с.

7. Герасименко В.А. , Размахнин М.К. Криптографические методы защиты информации. Зарубежная радиоэлектроника . 1982 , № 5 , с 97-123.

8. Герасименко В.А. ,Размахнин М.К. Программные средства защиты информации в вычислительных, информационных и управляющих системах и сетях. Зарубежная радиоэлектроника . 1986 .№ 5. с 73-91 .

9. Горша Л. Эллиптические кривые.Computer World. 1998, №34.

10. Гэри М.,Джонсон Д. Вычислительные машины и труднорешаемые задачи.М.: Мир , 1982.-416 с.

11. Дейтел Г. Введение в Операционные системы. Т.2. М.: Мир , 1987. – 398 с.

12. Диффи У. Первые десять лет криптографии с открытым ключом Малый тематический выпуск " Защита информации ". ТИИЭР , 1988 , № 5.

13. Люцарев В.С. и др. Безопасность компьютерных сетей на основе Windows NT.М.: Русская редакция,1998. - 279 с.

14. Месси Дж. Л. Введение в современную криптологию.Малый тематический выпуск " Защита информации ".ТИИЭР , 1988 , № 5.

15. Рааб М. Защита сетей: наконец-то в центре внимания. ComputerWorld - Москва.1994, №29.

16. Смид Э.,Бранстед Д. Стандарт шифрования данных: прошлое и будущее.Малый тематический выпуск " Защита информации ".ТИИЭР , 1988 , № 5.

17. Спесивцев, Вегнер и др. Защита информации в ПЭВМ.М.: Радио и связь ,1992, - 192 с.

18. Сухова С.В. Система безопасности NetWare. Сети. 1995, №4,сс. 60-70.

19. Сяо Д., Керр, Мэдник С. Защита ЭВМ. М.: Мир , 1982.-264 с.

20. Уолкер Б.Дж., Блейк М.Ф. Безопасность ЭВМ и организация их защиты. М.: Связь, 1980.-112 с.

21. Хоффман Л.Дж. Современные методы защиты информации. М.: Советское радио , 1980.-264 с.

22. Шеннон К.Э. "Теория связи в секретных системах".В кн : Шеннон К.Э. Работы по теории информации и кибернетике. М.: Иностранная Литература .1963 ,с 332 – 402,-829 с.

23. Шеннон К.Э. "Математическая теория связи". В кн : Шеннон К.Э. Работы по теории информации и кибернетике. М.: Иностранная Литература .1963 ,с 243-322,-829 с.

24. Шнейер Б. Компьютерная безопасность: мы научимся чему-нибудь или нет? www.counterprane.com.

25. Chor B.,Rivest L. A knapsack type public-key cryptosystem based on arithmetic in finite fields. In Crypto`84 pp.54-65.

26. Diffie W.,Hellman M. New directions in cryptography IEEE Trans. Informat.Theory, Vol.IT-22,pp.644-654, Nov 1976.

27. Vernan G.S. Cipher printing telegraph systems for secret wire and radio telegraphic communications.Amer. Inst.Elec. Eng., vol. 55, pp. 109-115, 1926.

Поступила 1.11.2001

УДК 681.3

Стишенко И.К.

ВОЛС И МОНИТОРИНГ ОПТИЧЕСКИХ КАБЕЛЕЙ

Согласно мировой статистике объем передаваемой информации и оказываемых услуг связи увеличивается по экспоненциальному закону, при этом реальный спрос постоянно превышает прогнозируемый. Очевидно, что сложившаяся ситуация эффективно стимулирует исследования и разработки по совершенствованию систем связи и телекоммуникаций, приводя к появлению новых технологий, направленных на возможность передачи больших объемов различной информации с более высоким качеством. Одной из таких технологий, наиболее перспективных в аспекте обеспечения высокой пропускной способности, является передача информации в микроволновом диапазоне по оптическому волокну.

1. Предпосылки создания системы мониторинга волоконно-оптического кабеля.

Задача повышения надежности ВОЛС охватывает широкий круг вопросов и по своей сути является комплексной. Ее решение требует применения соответствующих методик оценки, расчета и контроля различных параметров волоконно-оптических кабелей (ВОК) и показателей надежности ВОЛС [1]. Надежность ВОЛС зависит от различных конструктивно-производственных и эксплуатационных факторов. К первым относят факторы, связанные с