Содержание.

[Введение. 3](#_Toc263861733)

[1 Криптографические средства защиты. 8](#_Toc263861734)

[1.1 Принципы работы Криптосистемы. 8](#_Toc263861735)

[1.2 Управление криптографическими ключами. 11](#_Toc263861736)

[1.2 Алгоритмы шифрования 13](#_Toc263861737)

[2.2.1 Симметричные алгоритмы 13](#_Toc263861738)

[2.2.2 Асимметричные алгоритмы 16](#_Toc263861739)

[1.3 Хэш-функции 17](#_Toc263861740)

[1.4 Механизмы аутентификации 17](#_Toc263861741)

[1.5 Электронные подписи и временные метки 18](#_Toc263861742)

[1.6. Стойкость шифра. 19](#_Toc263861743)

[*2* Квантовая криптография. 22](#_Toc263861744)

[2.1. Природа секретности квантового канала связи. 23](#_Toc263861745)

[2.2.Принципы работы ККС и первая экспериментальная реализация. 23](#_Toc263861746)

[2.3.Современное состояние работ по созданию ККС 28](#_Toc263861747)

[2.4.Протоколы для квантово-криптографических систем распределения ключевой информации. 30](#_Toc263861748)

[Заключение. 34](#_Toc263861749)

[Литература. 37](#_Toc263861750)

# Введение.

Научно-техническая революция в последнее время приняла грандиозные масштабы в области информатизации общества на базе современных средств вычислительной техники, связи, а также современных методов автоматизированной обработки информации. Применение этих средств и методов приняло всеобщий характер, а создаваемые при этом информационно-вычислительные системы и сети становятся глобальными как в смысле территориальной распределенности, так и в смысле широты охвата в рамках единых технологий процессов сбора, передачи, накопления, хранения, поиска, переработки информации и выдачи ее для использования.

Информация в современном обществе – одна из самых ценных вещей в жизни, требующая защиты от несанкционированного проникновения лиц не имеющих к ней доступа.

Появление в середине двадцатого столетия первых электронно-вычислительных машин кардинально изменило ситуацию в области шифрования (криптографии). С проникновением компьютеров в различные сферы жизни возникла принципиально новая отрасль - информационная индустрия.

В 60-х и частично в 70-х годах проблема защиты информации решалась достаточно эффективно применением в основном организационных мер. К ним относились прежде всего режимные мероприятия, охрана, сигнализация и простейшие программные средства защиты информации. Эффективность использования указанных средств достигалась за счет концентрации информации на вычислительных центрах, как правило автономных, что способствовало обеспечению защиты относительно малыми средствами.

"Рассосредоточение" информации по местам ее хранения и обработки, чему в немалой степени способствовало появление в огромных количествах дешевых персональных компьютеров и построенных на их основе локальных и глобальных национальных и транснациональных сетей ЭВМ, использующих спутниковые каналы связи, создание высокоэффективных систем разведки и добычи информации, обострило ситуацию с защитой информации.

Проблема обеспечения необходимого уровня защиты информации оказалась (и это предметно подтверждено как теоретическими исследованиями, так и опытом практического решения) весьма сложной, требующей для своего решения не просто осуществления некоторой совокупности научных, научно-технических и организационных мероприятий и применения специфических средств и методов, а создания целостной системы организационных мероприятий и применения специфических средств и методов по защите информации.

Объем циркулирующей в обществе информации стабильно возрастает. Популярность всемирной сети Интренет в последние годы способствует удваиванию информации каждый год. Фактически, на пороге нового тысячелетия человечество создало информационную цивилизацию, в которой от успешной работы средств обработки информации зависит благополучие и даже выживание человечества в его нынешнем качестве. Произошедшие за этот период изменения можно охарактеризовать следующим образом:

1. объемы обрабатываемой информации возросли за полвека на несколько порядков;
2. доступ к определенным данным позволяет контролировать значительные материальные и финансовые ценности; информация приобрела стоимость, которую даже можно подсчитать;
3. характер обрабатываемых данных стал чрезвычайно многообразным и более не сводится к исключительно текстовым данным;
4. информация полностью "обезличилась", т.е. особенности ее материального представления потеряли свое значение - сравните письмо прошлого века и современное послание по электронной почте;
5. характер информационных взаимодействий чрезвычайно усложнился, и наряду с классической задачей защиты передаваемых текстовых сообщений от несанкционированного прочтения и искажения возникли новые задачи сферы защиты информации, ранее стоявшие и решавшиеся в рамках используемых "бумажных" технологий - например, подпись под электронным документом и вручение электронного документа "под расписку" - речь о подобных "новых" задачах криптографии еще впереди;
6. субъектами информационных процессов теперь являются не только люди, но и созданные ими автоматические системы, действующие по заложенной в них программе;
7. вычислительные "способности" современных компьютеров подняли на совершенно новый уровень как возможности по реализации шифров, ранее немыслимых из-за своей высокой сложности, так и возможности аналитиков по их взлому.

Перечисленные выше изменения привели к тому, что очень быстро после распространения компьютеров в деловой сфере практическая криптография сделала в своем развитии огромный скачок, причем сразу по нескольким направлениям:

1. во-первых, были разработаны стойкие блочные с секретным ключом, предназначенные для решения классической задачи - обеспечения секретности и целостности, передаваемых или хранимых данных, они до сих пор остаются "рабочей лошадкой" криптографии, наиболее часто используемыми средствами криптографической защиты;
2. во-вторых, были созданы методы решения новых, нетрадиционных задач сферы защиты информации, наиболее известными из которых являются задача подписи цифрового документа и открытого распределения ключей.

В современном мире информационный ресурс стал одним из наиболее мощных рычагов экономического развития. Владение информацией необходимого качества в нужное время и в нужном месте является залогом успеха в любом виде хозяйственной деятельности. Монопольное обладание определенной информацией оказывается зачастую решающим преимуществом в конкурентной борьбе и предопределяет, тем самым, высокую цену "информационного фактора".

Широкое внедрение персональных ЭВМ вывело уровень "информатизации" деловой жизни на качественно новую ступень. Ныне трудно представить себе фирму или предприятие (включая самые мелкие), которые не были бы вооружены современными средствами обработки и передачи информации. В ЭВМ на носителях данных накапливаются значительные объемы информации, зачастую носящей конфиденциальный характер или представляющей большую ценность для ее владельца.

Задача криптографии, т.е. тайная передача, возникает только для информации, которая нуждается в защите. В таких случаях говорят, что информация содержит тайну или является защищаемой, приватной, конфиденциальной, секретной. Для наиболее типичных, часто встречающихся ситуаций такого типа введены даже специальные понятия:

* государственная тайна;
* военная тайна;
* коммерческая тайна;
* юридическая тайна;
* врачебная тайна и т. д.

Далее мы будем говорить о защищаемой информации, имея в виду следующие признаки такой информации:

* имеется какой-то определенный круг законных пользователей, которые имеют право владеть этой информацией;
* имеются незаконные пользователи, которые стремятся овладеть этой информацией с тем, чтобы обратить ее себе во благо, а законным пользователям во вред.

# 1 Криптографические средства защиты.

Криптографическими средствами защиты называются специальные средства и методы преобразования информации, в результате которых маскируется ее содержание. Основными видами криптографического закрытия являются шифрование и кодирование защищаемых данных. При этом шифрование есть такой вид закрытия, при котором самостоятельному преобразованию подвергается каждый символ закрываемых данных; при кодировании защищаемые данные делятся на блоки, имеющие смысловое значение, и каждый такой блок заменяется цифровым, буквенным или комбинированным кодом. При этом используется несколько различных систем шифрования: заменой, перестановкой, гаммированием, аналитическим преобразованием шифруемых данных. Широкое распространение получили комбинированные шифры, когда исходный текст последовательно преобразуется с использованием двух или даже трех различных шифров.

## **1.1 Принципы работы Криптосистемы.**

Типичный пример изображения ситуации, в которой возникает задача криптографии (шифрования) изображён на рисунке №1:

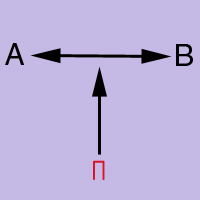


Рис. №1

На рисунке № 1 А и В - законные пользователи защищённой информации, они хотят обмениваться информацией по общедоступному каналу связи.  
П - незаконный пользователь (противник, хакер), который хочет перехватывать передаваемые по каналу связи сообщения и попытаться извлечь из них интересную для него информацию. Эту простую схему можно считать моделью типичной ситуации, в которой применяются криптографические методы защиты информации или просто шифрование.

Исторически в криптографии закрепились некоторые военные слова (противник, атака на шифр и др.). Они наиболее точно отражают смысл соответствующих криптографических понятий. Вместе с тем широко известная военная терминология, основанная на понятии кода (военно-морские коды, коды Генерального штаба, кодовые книги, кодобозначения и т. п.), уже не применяется в теоретической криптографии. Дело в том, что за последние десятилетия сформировалась теория кодирования - большое научное направление, которое разрабатывает и изучает методы защиты информации от случайных искажений в каналах связи.

Криптография занимается методами преобразования информации, которые бы не позволили противнику извлечь ее из перехватываемых сообщений. При этом по каналу связи передается уже не сама защищаемая информация, а результат ее преобразования с помощью шифра, и для противника возникает сложная задача вскрытия шифра. Вскрытие (взламывание) шифра - процесс получения защищаемой информации из шифрованного сообщения без знания примененного шифра. Противник может пытаться не получить, а уничтожить или модифицировать защищаемую информацию в процессе ее передачи. Это - совсем другой тип угроз для информация, отличный от перехвата и вскрытия шифра. Для защиты от таких угроз разрабатываются свои специфические методы. Следовательно, на пути от одного законного пользователя к другому информация должна защищаться различными способами, противостоящими различным угрозам. Возникает ситуация цепи из разнотипных звеньев, которая защищает информацию. Естественно, противник будет стремиться найти самое слабое звено, чтобы с наименьшими затратами добраться до информации. А значит, и законные пользователи должны учитывать это обстоятельство в своей стратегии защиты: бессмысленно делать какое-то звено очень прочным, если есть заведомо более слабые звенья ("принцип равнопрочности защиты").

Придумывание хорошего шифра дело трудоемкое. Поэтому желательно увеличить время жизни хорошего шифра и использовать его для шифрования как можно большего количества сообщений. Но при этом возникает опасность, что противник уже разгадал (вскрыл) шифр и читает защищаемую информацию. Если же в шифре сеть сменный ключ то, заменив ключ, можно сделать так, что разработанные противником методы уже не дают эффекта.

## **1.2 Управление криптографическими ключами.**

Под ключом в криптографии понимают сменный элемент шифра, который применяется для шифрования конкретного сообщения. В последнее время безопасность защищаемой информации стала определяться в первую очередь ключом. Сам шифр, шифрмашина или принцип шифрования стали считать известными противнику и доступными для предварительного изучения, но в них появился неизвестный для противника ключ, от которого существенно зависят применяемые преобразования информации. Теперь законные пользователи, прежде чем обмениваться шифрованными сообщениями, должны тайно от противника обменяться ключами или установить одинаковый ключ на обоих концах канала связи. А для противника появилась новая задача - определить ключ, после чего можно легко прочитать зашифрованные на этом ключе сообщения.

Вернемся к формальному описанию основного объекта криптографии   
(рис. №1). Теперь в него необходимо внести существенное изменение - добавить недоступный для противника секретный канал связи для обмена ключами (см. рис. №2).

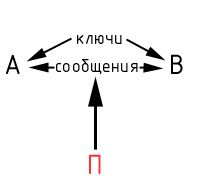


Рис. №2

Создать такой канал связи вполне реально, поскольку нагрузка на него, вообще говоря, небольшая. Отметим теперь, что не существует единого шифра, подходящего для всех случаев. Выбор способа шифрования зависит от особенностей информации, ее ценности и возможностей владельцев по защите своей информации. Прежде всего подчеркнем большое разнообразие видов защищаемой информации: документальная, телефонная, телевизионная, компьютерная и т.д. Каждый вид информации имеет свои специфические особенности, и эти особенности сильно влияют на выбор методов шифрования информации. Большое значение имеют объемы и требуемая скорость передачи шифрованной информации. Выбор вида шифра и его параметров существенно зависит от характера защищаемых секретов или тайны. Некоторые тайны (например, государственные, военные и др.) должны сохраняться десятилетиями, а некоторые (например, биржевые) - уже через несколько часов можно разгласить. Необходимо учитывать также и возможности того противника, от которого защищается данная информация. Одно дело - противостоять одиночке или даже банде уголовников, а другое дело - мощной государственной структуре.

Любая современная криптографическая система основана (построена) на использо­вании криптографических ключей. Она работает по определенной методологии (процедуре), состоящей из: одного или более алгоритмов шифрования (математических формул); ключей, используемых этими алгоритмами шифрования; системы управления ключами; незашифрованного текста; и зашифрованного текста (шифртекста).

## **1.2 Алгоритмы шифрования**

Алгоритмы шифрования с использованием ключей предполагают, что данные не сможет прочитать никто, кто не обладает ключом для их расшифровки. Они могут быть разделены на два класса, в зависимости от того, какая методология криптосистем напрямую поддерживается ими.

### 2.2.1 Симметричные алгоритмы

Для шифрования и расшифровки используются одни и те же алгоритмы. Один и тот же секретный ключ используется для шифрования и расшифровки. Этот тип алгоритмов используется как симметричными, так и асимметричными криптосистемами.

Таблица № 2.

|  |  |
| --- | --- |
| Тип | Описание |
| DES (Data Encryption  Standard) | Популярный алгоритм шифрования, используемый как стандарт шифрования данных правительством США.  Шифруется блок из 64 бит, используется 64-битовый ключ (требуется только 56 бит), 16 проходов  Может работать в 4 режимах:   1. Электронная кодовая книга (ECB-Electronic Code Book ) - обычный DES, использует два различных алгоритма. 2. Цепочечный режим (CBC-Cipher Block Chaining), в котором шифрование шифрование блока данных зависит от результатов шифрования предыдущих блоков данных. 3. Обратная связь по выходу (OFB-Output Feedback), используется как генератор случайных чисел. 4. Обратная связь по шифратору (CFB-Cipher Feedback), используется для получения кодов аутентификации сообщений. |
| 3-DES или  тройной DES | 64-битный блочный шифратор, использует DES 3 раза с тремя различными 56-битными ключами.  Достаточно стоек ко всем атакам |
| Каскадный 3-DES | Стандартный тройной DES, к которому добавлен механизм обратной связи, такой как CBC, OFB или CFB  Очень стоек ко всем атакам. |
| FEAL (быстрый  алгоритм шифрования) | Блочный шифратор, используемый как альтернатива DES  Вскрыт, хотя после этого были предложены новые версии. |
| IDEA (международный  алгоритм шифрования) | 64-битный блочный шифратор, 128-битовый ключ, 8 проходов  Предложен недавно; хотя до сих пор не прошел полной проверки, чтобы считаться надежным, считается более лучшим, чем DES |
| Skipjack | Разработано АНБ в ходе проектов правительства США "Clipper" и "Capstone".  До недавнего времени был секретным, но его стойкость не зависела только от того, что он был секретным.  64-битный блочный шифратор, 80-битовые ключи используются в режимах ECB, CFB, OFB или CBC, 32 прохода |
| RC2 | 64-битный блочный шифратор, ключ переменного размера  Приблизительно в 2 раза быстрее, чем DES  Может использоваться в тех же режимах, что и DES, включая тройное шифрование.  Конфиденциальный алгоритм, владельцем которого является RSA Data Security |
| RC4 | Потоковый шифр, байт-ориентированный, с ключом переменного размера.  Приблизительно в 10 раз быстрее DES.  Конфиденциальный алгоритм, которым владеет RSA Data Security |
| RC5 | Имеет размер блока 32, 64 или 128 бит, ключ с длиной от 0 до 2048 бит, от 0 до 255 проходов  Быстрый блочный шифр  Алгоритм, которым владеет RSA Data Security |
| CAST | 64-битный блочный шифратор, ключи длиной от 40 до 64 бит, 8 проходов  Неизвестно способов вскрыть его иначе как путем прямого перебора. |
| Blowfish. | 64-битный блочный шифратор, ключ переменного размера до 448 бит, 16 проходов, на каждом проходе выполняются перестановки, зависящие от ключа, и подстановки, зависящие от ключа и данных.  Быстрее, чем DES  Разработан для 32-битных машин |
| Устройство с  одноразовыми ключами | Шифратор, который нельзя вскрыть.  Ключом (который имеет ту же длину, что и шифруемые данные) являются следующие 'n' бит из массива случайно созданных бит, хранящихся в этом устройстве. У отправителя и получателя имеются одинаковые устройства. После использования биты разрушаются, и в следующий раз используются другие биты. |
| Поточные шифры | Быстрые алгоритмы симметричного шифрования, обычно оперирующие битами (а не блоками бит).  Разработаны как аналог устройства с одноразовыми ключами, и хотя не являются такими же безопасными, как оно, по крайней мере практичны. |

### 2.2.2 Асимметричные алгоритмы

Асимметричные алгоритмы используются в асимметричных криптосистемах для шифрования симметричных сеансовых ключей (которые используются для шифрования самих данных).

Используется два разных ключа - один известен всем, а другой держится в тайне. Обычно для шифрования и расшифровки используется оба этих ключа. Но данные, зашифрованные одним ключом, можно расшифровать только с помощью другого ключа.

Таблица № 3.

|  |  |
| --- | --- |
| Тип | Описание |
| RSA | Популярный алгоритм асимметричного шифрования, стойкость которого зависит от сложности факторизации больших целых чисел. |
| ECC (криптосистема  на основе  эллиптических кривых) | Использует алгебраическую систему, которая описывается в терминах точек эллиптических кривых, для реализации асимметричного алгоритма шифрования.  Является конкурентом по отношению к другим асимметричным алгоритмам шифрования, так как при эквивалентной стойкости использует ключи меньшей длины и имеет большую производительность.  Современные его реализации показывают, что эта система гораздо более эффективна, чем другие системы с открытыми ключами. Его производительность приблизительно на порядок выше, чем производительность RSA, Диффи-Хеллмана и DSA. |
| Эль-Гамаль. | Вариант Диффи-Хеллмана, который может быть использован как для шифрования, так и для электронной подписи. |

## **1.3 Хэш-функции**

Хэш-функции являются одним из важных элементов криптосистем на основе ключей. Их относительно легко вычислить, но почти невозможно расшифровать. Хэш-функция имеет исходные данные переменной длины и возвращает строку фиксированного размера (иногда называемую дайджестом сообщения - MD), обычно 128 бит. Хэш-функции используются для обнаружения модификации сообщения (то есть для электронной подписи).

Таблица № 4.

|  |  |
| --- | --- |
| Тип | Описание |
| MD2 | Самая медленная, оптимизирована для 8-битовых машин |
| MD4 | Самая быстрая, оптимизирована для 32-битных машин  Не так давно взломана |
| MD5 | Наиболее распространенная из семейства MD-функций.  Похожа на MD4, но средства повышения безопасности делают ее на 33% медленнее, чем MD4  Обеспечивает целостность данных  Считается безопасной |
| SHA (Secure  Hash Algorithm) | Создает 160-битное значение хэш-функции из исходных данных переменного размера.  Предложена NIST и принята правительством США как стандарт  Предназначена для использования в стандарте DSS |

## **1.4 Механизмы аутентификации**

Эти механизмы позволяют проверить подлинность личности участника взаимодействия безопасным и надежным способом.

Таблица № 5.

|  |  |
| --- | --- |
| Тип | Описание |
| Пароли или PIN-коды  (персональные  идентификационные  номера) | Что-то, что знает пользователь и что также знает другой участник взаимодействия.  Обычно аутентификация производится в 2 этапа.  Может организовываться обмен паролями для взаимной аутентификации. |
| Одноразовый пароль | Пароль, который никогда больше не используется.  Часто используется постоянно меняющееся значение, которое базируется на постоянном пароле. |
| CHAP (протокол  аутентификации  запрос-ответ) | Одна из сторон инициирует аутентификацию с помощью посылки уникального и непредсказуемого значения "запрос" другой стороне, а другая сторона посылает вычисленный с помощью "запроса" и секрета ответ. Так как обе стороны владеют секретом, то первая сторона может проверить правильность ответа второй стороны. |
| Встречная проверка  (Callback) | Телефонный звонок серверу и указание имени пользователя приводит к тому, что сервер затем сам звонит по номеру, который указан для этого имени пользователя в его конфигурационных данных. |

## **1.5 Электронные подписи и временные метки**

Электронная подпись позволяет проверять целостность данных, но не обеспечивает их конфиденциальность. Электронная подпись добавляется к сообщению и может шифроваться вместе с ним при необходимости сохранения данных в тайне. Добавление временных меток к электронной подписи позволяет обеспечить ограниченную форму контроля участников взаимодействия.

Таблица № 6.

|  |  |
| --- | --- |
| Тип | Комментарии |
| DSA (Digital  Signature Authorization) | Алгоритм с использованием открытого ключа для создания электронной подписи, но не для шифрования.  Секретное создание хэш-значения и публичная проверка ее - только один человек может создать хэш-значение сообщения, но любой может проверить ее корректность.  Основан на вычислительной сложности взятия логарифмов в конечных полях. |
| RSA | Запатентованная RSA электронная подпись, которая позволяет проверить целостность сообщения и личность лица, создавшего электронную подпись.  Отправитель создает хэш-функцию сообщения, а затем шифрует ее с использованием своего секретного ключа. Получатель использует открытый ключ отправителя для расшифровки хэша, сам рассчитывает хэш для сообщения, и сравнивает эти два хэша. |
| MAC (код  аутентификации сообщения) | Электронная подпись, использующая схемы хэширования, аналогичные MD или SHA, но хэш-значение вычисляется с использованием как данных сообщения, так и секретного ключа. |
| DTS (служба  электронных временных  меток) | Выдает пользователям временные метки, связанные с данными документа |

## **1.6. Стойкость шифра.**

Способность шифра противостоять всевозможным атакам на него называют стойкостью шифра. Под атакой на шифр понимают попытку вскрытия этого шифра. Понятие стойкости шифра является центральным для криптографии. Хотя качественно понять его довольно легко, но получение строгих доказуемых оценок стойкости для каждого конкретного шифра - проблема нерешенная. Это объясняется тем, что до сих пор нет необходимых для решения такой проблемы математических результатов. Поэтому стойкость конкретного шифра оценивается только путем всевозможных попыток его вскрытия и зависит от квалификации криптоаналитиков, атакующих шифр. Такую процедуру иногда называют проверкой стойкости. Важным подготовительным этапом для проверки стойкости шифра является продумывание различных предполагаемых возможностей, с помощью которых противник может атаковать шифр. Появление таких возможностей у противника обычно не зависит от криптографии, это является некоторой внешней подсказкой и существенно влияет на стойкость шифра. Поэтому оценки стойкости шифра всегда содержат те предположения о целях и возможностях противника, в условиях которых эти оценки получены. Прежде всего, как это уже отмечалось выше, обычно считается, что противник знает сам шифр и имеет возможности для его предварительного изучения. Противник также знает некоторые характеристики открытых текстов, например, общую тематику сообщений, их стиль, некоторые стандарты, форматы и т.д.

Из более специфических приведем еще три примера возможностей противника:

* противник может перехватывать все шифрованные сообщения, но не имеет соответствующих им открытых текстов;
* противник может перехватывать все шифрованный сообщения и добывать соответствующие им открытые тексты;
* противник имеет доступ к шифру (но не к ключам!) и поэтому может зашифровывать и дешифровывать любую информацию;

Существуют различные криптографические системы защиты, которые мы можем разделить на две группы: c использованием ключа и без него. Криптосистемы без применения ключа в совремом мире не используються т.к. очень дорогостоющие и ненадёжные.

Были расмотренны основные методологии: семметричная и асиметричная. Обе методологии используют ключ (сменный элемент шифра).

Симметричные и асиметричные алгоритмы, описанные выше, сведены в таблицу, из которой можно понять какие алгоритмы наиболее подходят к той или иной задаче.

Остальная информация пердставленная во второй главе очень разнообразна. На её основе сложно сделать вывод, какие алгоритмы хеш-функций, механизмов аутетификации и электронных подписей наиболее продвинутые, все они в разной ситуации могут показать себя с лучшей стороны.

На протяжении многих веков среди специалистов не утихали споры о стойкости шифров и о возможности построения абсолютно стойкого шифра.

# *2* Квантовая криптография.

Один из надёжных способов сохранить в тайне телефонные переговоры или передаваемую по компьютерным сетям связи информацию – это использование квантовой криптографии.

Идея использовать для целей защиты информации природу объектов микромира - квантов света (фотонов), поведение которых подчиняется законам квантовой физики, стала наиболее актуальной.

Наибольшее практическое применение квантовой криптографии находит сегодня в сфере защиты информации, передаваемой по волоконно-оптическим линиям связи. Это объясняется тем, что оптические волокна ВОЛС позволяют обеспечить передачу фотонов на большие расстояния с минимальными искажениями. В качестве источников фотонов применяются лазерные диоды передающих модулей ВОЛС; далее происходит существенное ослабление мощности светового сигнала – до уровня, когда среднее число фотонов на один импульс становится много меньше единицы. Системы передачи информации по ВОЛС, в приемном модуле которых применяются лавинные фотодиоды в режиме счета фотонов, называются квантовыми оптическими каналами связи (КОКС).

Вследствие малой энергетики сигналов скорости передачи информации в КОКС по сравнению с возможностями современных ВОЛС не слишком высоки (от килобит до мегабит в секунду, в зависимости от применения). Поэтому в большинстве случаев квантовые криптографические системы (ККС) применяются для распределения ключей, которые затем используются средствами шифрования высокоскоростного потока данных. Важно отметить, что квантово-криптографическое оборудование пока серийно не выпускается. Однако по мере совершенствования и удешевления применяемой элементной базы можно ожидать появления ККС на рынке телекоммуникаций в качестве, например, дополнительной услуги при построении корпоративных волоконно-оптических сетей.

## **2.1. Природа секретности квантового канала связи.**

При переходе от сигналов, где информация кодируется импульсами, содержащими тысячи фотонов, к сигналам, где среднее число фотонов, приходящихся на один импульс, много меньше единицы (порядка 0,1), вступают в действие законы квантовой физики. Именно на использовании этих законов в сочетании с процедурами классической криптографии основана природа секретности ККС. Здесь непосредственно применяется принцип неопределенности Гейзенберга, согласно которому попытка произвести измерения в квантовой системе искажает ее состояние, и полученная в результате такого измерения информация не полностью соответствует состоянию до начала измерений. Попытка перехвата информации из квантового канала связи неизбежно приводит к внесению в него помех, обнаруживаемых легальными пользователями. КК используют этот факт для обеспечения возможности двум сторонам, которые ранее не встречались и предварительно не обменивались никакой секретной информацией, осуществлять между собой связь в обстановке полной секретности без боязни быть подслушанными.

## **2.2.Принципы работы ККС и первая экспериментальная реализация.**

В 1984 году Ч. Беннетт (фирма IBM) и Ж. Брассард (Монреальский университет) предложили простую схему защищенного квантового распределения ключей шифрования. Эта схема использует квантовый канал, по которому пользователи А и Б обмениваются сообщениями, передавая их в виде поляризованных фотонов. Подслушивающий их злоумышленник П может попытаться производить измерения этих фотонов, но он не может сделать это, не внося в них искажения. А и Б используют открытый канал для обсуждения и сравнения сигналов, передаваемых по квантовому каналу, проверяя их на возможность перехвата. Если при этом они не выявят искажений в процессе свыязи, они могут извлечь из полученных данных информацию, которая надежно распределена, случайна и секретна, несмотря на все технические ухищрения и вычислительные возможности, которыми располагает П.

Схема работает следующим образом. Сначала А генерирует и посылает Б последовательность фотонов, поляризация которых выбрана случайным образом и может составлять 0°, 45°, 90° или 135°. Б принимает эти фотоны и для каждого из них случайным образом решает, замерять ли его поляризацию как перпендикулярную или диагональную. Затем по открытому каналу Б объявляет для каждого фотона, какой тип измерений им был сделан (перпендикулярный или диагональный), но не сообщает результат этих измерений, например, 0°, 45°, 90° или 135°. По этому же открытому каналу А сообщает ему, правильный ли вид измерений был выбран для каждого фотона. Затем А и Б отбрасывают все случаи, когда Б сделал неправильные замеры или когда произошли сбои в его детекторах. Если квантовый канал не перехватывался, оставшиеся виды поляризаций, которые затем переводятся в биты, составят в совокупности поделенную между А и Б секретную информацию.

Следующее испытание на возможность перехвата может производиться пользователями А и Б по открытому каналу путем сравнения и отбрасывания случайно выбранных ими подмножеств полученных данных. Если такое сравнение выявит наличие перехвата, А и Б отбрасывают все свои данные и начинают с новой группы фотонов. В противном случае они оставляют прежнюю поляризацию, о которой не упоминалось по открытому каналу, в качестве секретной информации о битах, известных только им, принимая фотоны с горизонтальной или 45-градусной поляризацией за двоичный ноль, а с вертикальной или 135-градусной поляризацией - за двоичную единицу.

Согласно принципу неопределенности, П не может замерить как прямоугольную, так и диагональную поляризации одного и того же фотона. Даже если он для какого-либо фотона произведет неправильное измерение и перешлет Б этот фотон в соответствии с результатом своих измерений, это неизбежно внесет случайность в первоначальную поляризацию, с которой он посылался А. В результате появятся ошибки в одной четвертой части битов, составляющих данные Б, которые были подвергнуты перехвату.

Более эффективной проверкой для А и Б является проверка на четность, осуществляемая по открытому каналу. Например, А может сообщить: "Я просмотрел 1-й, 4-й, 5-й, 8-й, ... и 998-й из моих 1000 битов данных, и они содержат четное число единиц. Тогда Б подсчитывает число единиц на тех же самых позициях. Можно показать, что если данные у Б и А отличаются, проверка на четность случайного подмножества этих данных выявит этот факт с вероятностью 0,5 независимо от числа и местоположения ошибок. Достаточно повторить такой тест 20 раз с 20 различными случайными подмножествами, чтобы сделать вероятность необнаруженной ошибки очень малой.

А и Б могут также использовать для коррекции ошибок коды, исправляющие ошибки, обсуждая результаты кодирования по открытому каналу. Однако при этом часть информации может попасть к П. Тем не менее А и Б, зная интенсивность вспышек света и количество обнаруженных и исправленных ошибок, могут оценить количество информации, попадающей к П.

Знание П значительной части ключа может во многих случаях привести к вскрытию им сообщения. Беннетт и Брассард совместно с Ж. М. Робертом разработали математический метод, называемый усилением секретности. Он состоит в том, что при обсуждении по открытому каналу из части секретной битовой последовательности пользователи выделяют некоторое количество особо секретных данных, из которых перехватчик с большой вероятностью не в состоянии узнать даже значения одного бита. В частности, было предложено использовать некоторую функцию уменьшения длины (функцию хэширования). После применения этой функции пользователями А и Б к имеющимся у них последовательностям битов частичная информация перехватчика о массиве их данных преобразуется практически в отсутствие какой-либо информации о выходных данных функции.

Например, если входная последовательность состоит из 1000 бит, из которых П известно более 200, А и Б могут выделить около 800 особо секретных битов в качестве выходной последовательности. В качестве таковых они могут взять любое множество таких битов, которые с наибольшей достоверностью были идентичны при проведении ими измерений (при этом им следует сохранять в тайне это соответствие, а не обсуждать его по открытому каналу). Так, например, А и Б могут определить каждый выходной бит функции усиления секретности как четность независимого публично оговоренного случайного набора битов из полного массива.

Отметим, что в качестве открытого канала могут использоваться как обычные линии телефонной и радиосвязи или локальные вычислительные сети, так и волоконно-оптическая линия связи в стандартном режиме работы.

В 1989 году в Исследовательском центре фирмы IBM был построен первый прототип КОКС, содержащий передающий модуль пользователя А на одном конце и приемный модуль Б на другом. Эта система размещалась на оптической скамье длиной около 1 м в светонепроницаемом кожухе. Квантовый канал представлял собой свободное воздушное пространство длиной около 30 см. Во время функционирования макет управлялся от ПЭВМ, которая содержала программное представление пользователей А, Б и, кроме того, возможного злоумышленника П.

Левая сторона передающего модуля А состоит из диода, излучающего зеленый свет, линзы, булавочного отверстия и фильтров, которые обеспечивают пучок горизонтально поляризованного света. Получались импульсы с интенсивностью 0,1 фотона на импульс. Такая низкая интенсивность принята для сведения к минимуму возможности перехватчика разделить отдельный импульс на два или более фотонов. Затем располагаются электрооптические приборы, известные как камеры Поккельса, которые используются для изменения первоначальной горизонтальной поляризации в любое из четырех стандартных поляризационных состояний, выбором которых управляет пользователь А.

На противоположном конце в приемнике Б располагается аналогичная камера Поккельса, позволяющая ему изменять тип поляризации, которую приемник будет измерять. После прохождения через камеру Поккельса пучок света расщепляется кальцитовой призмой на два перпендикулярно поляризованных пучка, которые направляются на два фотоэлектронных умножителя с целью выделения отдельных фотонов.

**2.3.Современное состояние работ по созданию ККС**.

За десять лет, прошедших с момента создания первого прототипа КОКС, достигнут огромный прогресс. Сейчас квантовое распределение ключей по ВОЛС является возможным уже на расстояния в десятки километров.

Работы в области квантовой криптографии ведутся во многих странах. В России, например, этими вопросами активно занимаются в Государственном университете телекоммуникаций (Санкт-Петербург). В США в Лос-Аламосской национальной лаборатории создана линия связи общей длиной 48 км, в которой осуществляется распределение ключей со скоростью в несколько десятков Кбит/с, а в университете Дж. Хопкинса реализована локальная вычислительная сеть с квантовым каналом связи длиной 1 км, в которой достигнута скорость передачи 5 кбит/с. В Великобритании, в Оксфордском университете, реализован целый ряд макетов квантово-криптографических систем с использованием различных методов модуляции и детектирования оптических сигналов, а в лаборатории фирмы British Telecom получена наибольшая длина КОКС – 30 км при скорости передачи порядка 10 кбит/с. В 1997 году была доказана возможность существенного повышения скоростей передачи - до уровня 1 Мбит/с и более.

ККС поначалу использовались для связи отдельных пар пользователей, но практические применения требуют связей со многими пользователями. И не так давно были предложены реализации ККС для оптических сетей связи различной топологии.

Рассмотрим, как КК может применяться к случаю пассивной оптической сети, содержащей центральный сетевой контроллер А, связанный посредством пассивного оптического светоделителя со множеством сетевых пользователей (Бi). В этой схеме просто используется квантовое поведение оптического светоделителя. Одиночный фотон в светоделителе не может разделяться, а, напротив, направляется по одному (и только одному) из путей. Выбор пути для каждого отдельного фотона произволен и непредсказуем. Следовательно, если стандартный протокол квантовой передачи применяется в сети со светоделителями, то каждый пользователь будет обеспечен уникальным произвольно выбранным подмножеством битов. Из последовательности, которая передается в сети, центр А может, выполняя открытое обсуждение после передачи с каждым пользователем по очереди, идентифицировать, какие фотоны были разделены с каждым из них, и создать с каждым секретный и уникальный индивидуальный ключ. Таким образом, сеть может быть надежно защищена, потому что, хотя шифрованная информация передается открыто по сети, А и Бi могут быть уверены, что никакой другой сетевой пользователь или внешний злоумышленник не получил никаких сведений относительно их общего ключа. Эта схема распределения ключей полезна, например, для обеспечения работы пользователей с защищенной базой данных.

Основные усилия теперь направлены на то, чтобы сделать использование квантового канала экономически эффективным. Большинство схем КОКС требуют постоянной подстройки и управления на каждой стороне канала связи, что удорожает систему. Однако недавно в Женевском университете была предложена реализация КОКС, не требующая никакой подстройки, кроме синхронизации. Экспериментальные результаты подтверждают, что подобные схемы действительно многообещающи для практических реализаций квантового канала. Применение в них так называемых “зеркал Фарадея” приводит к тому, что все световые импульсы проходят одинаковый путь, поэтому, в отличие от обычных схем, не требуется никакой подстройки. Для организации квантового канала необходимо просто подключить приемный и передающий модули в конце ВОЛС, синхронизировать сигналы и начать передачу. Именно поэтому данную систему называют системой Plug and Play ("подключай и работай"). В эксперименте швейцарских исследователей каналом связи являлся подводный кабель длиной 23 км, используемый для передачи данных между Нионом и Женевой. Однако скорости передачи информации, полученные в данной системе, низки для практических приложений, и сейчас ведется доработка схемы, чтобы достичь более конкурентоспособных результатов.

## **2.4.Протоколы для квантово-криптографических систем распределения ключевой информации.**

Алгоритмическая часть ККС состоит из стека протоколов, реализация которого позволяет законным пользователям обеспечить формирование общего ключа при условии утечки к злоумышленнику не более заданного количества информации или отказ от данного сеанса при невыполнении этого условия.

В стек протоколов входят следующие элементы.

* Протокол первичной квантовой передачи.
* Протокол исправления ошибок в битовых последовательностях, полученных в результате квантовой передачи.
* Протокол оценки утечки к злоумышленнику информации о ключе.
* Протокол усиления секретности и формирования итогового ключа.

Шаги первичного протокола квантовой передачи зависят от типа оптической схемы, использованной для создания квантового оптического канала связи, и вида модуляции квантовых состояний. Пример протокола квантовой передачи для КОКС с модуляцией поляризации фотонов по четырем состояниям был кратко описан выше. После реализации такого протокола пользователи A и Б будут иметь в основном совпадающие последовательности, причем длины этих последовательностей будут близки к половине длины последовательности переданных фотонных импульсов.

Примером протокола исправления ошибок в битовых последовательностях, полученных после выполнения первичного протокола, является способ коррекции ошибок, состоящий в том, что блок данных, который должен быть согласован между пользователями, рассматривается как информационный блок некоторого кода. Проверочные символы этого кода могут быть переданы по открытому каналу связи и использованы для исправления или обнаружения ошибок в блоке. Для того чтобы злоумышленник не мог получить дополнительную информацию по проверочным символам, из информационного блока исключается несколько определенных битов. Коды и множества отбрасываемых битов должны быть выбраны так, чтобы выполнялось требование о невозрастании количества информации у злоумышленника. После применения протокола исправления ошибок легальные пользователи будут иметь одинаковые битовые последовательности и могут оценить степень вмешательства злоумышленника в квантовом канале связи.

Для этого реализуется протокол оценки утечки информации о ключе при перехвате данных в квантовом канале. В нем пользователь Б по заданной допустимой величине утечки информации к злоумышленнику определяет максимально возможную длину ключа, при которой хэширование данных после исправления в них ошибок к ключу требуемой длины обеспечит выполнение заданного требования стойкости. Если эта максимальная длина оказывается допустимой, то сеанс связи принимается для формирования ключа, в противном случае он отвергается.

В том случае, когда при реализации предыдущего протокола делается вывод о допустимости данного сеанса связи, выполняется протокол усиления секретности и формирования итогового ключа – оба пользователя применяют к согласованным после исправления ошибок данным хэширующую функцию (перемешивающее и сжимающее преобразование), которая отображает эти данные в ключ. Функция выбирается одним из пользователей случайным образом и передается другому по открытому каналу связи.

Осуществимость квантового распределения ключей по волоконно-оптическим сетям связи доказана, но насколько оно практично? Сейчас можно ответить на этот вопрос положительно.

Во-первых, потому, что современные схемы шифрования используют ключ порядка единиц килобит или меньше для шифрования достаточно больших объемов информации, и эффективный способ распределения ключа со скоростью порядка десятков килобит в секунду может быть более чем адекватен для многих потенциальных применений.

Во-вторых, потому, что создание защищенных с использованием методов квантовой криптографии оптических корпоративных и локальных сетей различных топологий является технически вполне выполнимой задачей.

Объективности ради отметим, что на сегодня при использовании методов криптографии имеется возможность защищенной от подслушивания передачи информации на расстояние в несколько десятков километров. При больших длинах линий связи классические методы распределения ключей и защиты информации оказываются пока более дешевыми и надежными.

В последнее время появились новые теоретические идеи для создания глобальных распределенных квантовых криптографических сетей. Они основаны на использовании безопасной передачи информации так называемых квантовых корреляций между двумя частицами, имеющими неклассические свойства, а также на использовании для хранения этих частиц квантовой памяти. Кроме того, появились сообщения об экспериментах по реализации ККС для защиты каналов связи между космическими аппаратами и земными станциями.

# Заключение.

Криптография сегодня - это важнейшая часть всех информационных систем: от электронной почты до сотовой связи, от доступа к сети Internet до электронной наличности. Криптография обеспечивает подотчетность, прозрачность, точность и конфиденциальность. Она предотвращает попытки мошенничества в электронной коммерции и обеспечивает юридическую силу финансовых транзакций. Криптография помогает установить вашу личность, но и обеспечивает вам анонимность. Она мешает хулиганам испортить сервер и не позволяет конкурентам залезть в ваши конфиденциальные документы. А в будущем, по мере того как коммерция и коммуникации будут все теснее связываться с компьютерными сетями, криптография станет жизненно важной.

Но присутствующие на рынке криптографические средства не обеспечивают того уровня защиты, который обещан в рекламе. Большинство продуктов разрабатывается и применяется отнюдь не в сотрудничестве с криптографами. Этим занимаются инженеры, для которых криптография - просто еще один компонент программы. Но криптография - это не компонент. Нельзя обеспечить безопасность системы, «вставляя» криптографию после ее разработки. На каждом этапе, от замысла до инсталляции, необходимо осознавать, что и зачем вы делаете.

Для того, чтобы грамотно реализовать собственную криптосистему, необходимо не только ознакомится с ошибками других и понять причины, по которым они произошли, но и, возможно, применять особые защитные приемы программирования и специализированные средства разработки.

На обеспечение компьютерной безопасности тратятся миллиарды долларов, причем большая часть денег выбрасывается на негодные продукты. К сожалению, коробка со слабым криптографическим продуктом выглядит так же, как коробка со стойким. Два криптопакета для электронной почты могут иметь схожий пользовательский интерфейс, но один обеспечит безопасность, а второй допустит подслушивание. Сравнение может указывать сходные черты двух программ, но в безопасности одной из них при этом зияют дыры, которых лишена другая система. Опытный криптограф сможет определить разницу между этими системами. То же самое может сделать и злоумышленник.

На сегодняшний день компьютерная безопасность - это карточный домик, который в любую минуту может рассыпаться. Очень многие слабые продукты до сих пор не были взломаны только потому, что они мало используются. Как только они приобретут широкое распространение, они станут притягивать к себе преступников. Пресса тут же придаст огласке эти атаки, подорвав доверие публики к этим криптосистемам. В конце концов, победу на рынке криптопродуктов определит степень безопасности этих продуктов.

# Литература.

1. А.Ю.Винокуров. ГОСТ не прост..,а очень прост, М., Монитор.–1995.–N1.
2. А.Ю.Винокуров. Еще раз про ГОСТ., М., Монитор.–1995.–N5.
3. А.Ю.Винокуров. Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы Intel x86., Рукопись, 1997.
4. А.Ю.Винокуров. Как устроен блочный шифр?, Рукопись, 1995.
5. М.Э.Смид, Д.К.Бранстед. Стандарт шифрования данных: прошлое и будущее. /пер. с англ./ М., Мир, ТИИЭР.–1988.–т.76.–N5.
6. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования ГОСТ 28147–89, М., Госстандарт, 1989.
7. Б.В.Березин, П.В.Дорошкевич. Цифровая подпись на основе традиционной криптографии//Защита информации, вып.2.,М.: МП "Ирбис-II",1992.
8. W.Diffie,M.E.Hellman. New Directions in cryptography// IEEE Trans. Inform. Theory, IT-22, vol 6 (Nov. 1976), pp. 644-654.
9. У.Диффи. Первые десять лет криптографии с открытым ключом. /пер. с англ./ М., Мир, ТИИЭР.–1988.–т.76.–N5.
10. Водолазкий В., "Стандарт шифрования ДЕС", Монитор 03-04 1992 г. С.
11. Воробьев, "Защита информации в персональных ЗВМ", изд. Мир, 1993 г.
12. Ковалевский В., "Криптографические методы", Компьютер Пресс 05.93 г.
13. Мафтик С., "Механизмы защиты в сетях ЭВМ", изд. Мир, 1993 г.