МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Физико-технический факультет**

**Кафедра оптоэлектроники**

**КУРСОВОЙ ПРОЕКТ**

**МЕТОДЫ И СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В**

**ИНФОКОММУНИКАЦИОНЫХ КАНАЛАХ СВЯЗИ**

Работу выполнил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Пушистов Сергей Владимирович

Курс 2

Направление 11.03.02 Инфокоммуникационные технологии и системы связи

Научный руководитель

ст. преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Н.Р. Рудоман

Нормоконтролер

преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.Е. Лысенко

Краснодар 2018

**РЕФЕРАТ**

Курсовой проект 35 с., 8 рис., 2 табл., 9 источников.

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ КАНАЛАХ СВЯЗИ, СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ, ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Объектом исследования данного курсового проекта является информация, способы и методы её защиты.

Основной целью курсовой работы считается исследование способов защиты данных в инфокоммуникационных сетях.

В результате выполнения курсового проекта была проанализирована проблема защиты информации в информационных и в инфокоммуникационных сетях. Так же были определены угрозы информации и методы их влияний на объекты защиты информации. Были проанализированы способы защиты информации, в результате этого было выявлена теория информационной безопасности предприятий.

**СОДЕРЖАНИЕ**

Обозначения и сокращения……………………………………………………………………………….4

Введение… …………………………………………………….…………........…. 5

[1 Основные положения теории защиты информации](http://refeteka.ru/r-116718.html#_Toc198391314)……………………...…...7

[1.1 Сущность проблемы и задачи защиты информации в информационных и инфокоммуникационных сетях](http://refeteka.ru/r-116718.html#_Toc198391315)………………………...………....…7

[1.2 Угрозы информации. Способы их воздействия на объекты защиты информации](http://refeteka.ru/r-116718.html#_Toc198391316)………………………………………………….....…..………..8

[2 Методы и средства защиты информации](http://refeteka.ru/r-116718.html#_Toc198391317)………………………...………….13

[2.1 Традиционные меры и методы защиты информации](http://refeteka.ru/r-116718.html#_Toc198391318)….…………….13

[2.2 Криптографические методы и средства защиты информации](http://refeteka.ru/r-116718.html#_Toc198391319)….… 18

[2.3 Нетрадиционные методы защиты информации](http://refeteka.ru/r-116718.html#_Toc198391320)………………..….…23

[3. Информационная безопасность предприятия](http://refeteka.ru/r-116718.html#_Toc198391321)…………………………….…26

[3.1 Концепция информационной безопасности предприятия](http://refeteka.ru/r-116718.html#_Toc198391322)…………..26

[3.2 Методы защита информации в инфокоммуникационных сетях предприятия](http://refeteka.ru/r-116718.html#_Toc198391323)……………………………….....................................................…..29

[Заключение](http://refeteka.ru/r-116718.html#_Toc198391324)…………………………………………………………………….…33

Список использованных источников…………………………..……….………35

**Обозначения и сокращения**

|  |  |
| --- | --- |
| ВОЛС | волоконно-оптических линия связи |
| ОВ | оптическое волокно |
| A | мощность алфавита паролей |
| L | длина пароля |
| S | мощность пространства паролей |
| V | скорость подбора паролей |
| T | срок действия пароля |
| СБИС | сверхбольших интегральных системах |
| КА | криптографический алгоритм |
| ПО | программное обеспечение |
| ЭЦП | электронная цифровая подписи |
| МЭ | межсетевой экран |
| VPN | virtual private network |
| НСД | несанкционированный доступ |
| ПК | Персональный компьютер |

**ВВЕДЕНИЕ**

Использование вычислительных средств в системах управления государственных и коммерческих структур, привело к формированию общей инфраструктуры. Её применение разрешило людям, обладающим ПК и модемом, приобретать допуск к данным наикрупнейших библиотек и баз, незамедлительно осуществлять труднейшие расчёты, делиться данными с иными пользователями сети вне зависимости от расстояния и места проживания.

Но такие системы повлекли несколько трудностей, одна из таковых - защита обработки и передачи информации. Определенные проблемы связаны с разработкой новых технологий. С одной стороны, применение информационных технологий предоставляет несколько явных положительных сторон: увеличение эффективности процессов управления, обработки и передачи информации и т.п.

С другой стороны, процветание сетей, их усложнение, взаимная связь, приводят к возникновению новых угроз, увеличению злоумышленников, обладающих возможностью воздействовать на систему.

В настоящее время, одним из перспективных направлений развития сетей связи как в нашей стране, так и за рубежом является интенсивное внедрение в них волоконно-оптических линий связи (ВОЛС). Это объясняется тем, что они значительно превосходят проводные по таким показателям, как пропускная способность, длина участка регенерации, помехозащищенность, малые габаритные размеры и масса оптических кабелей, а также их относительно низкая стоимость. Считается, что ВОЛС, в силу особенностей распространения электромагнитной энергии в оптическом волокне (ОВ), обладают повышенной скрытностью. Однако, всегда существует принципиальная возможность съема информации с оптического кабеля. Поэтому для надежной защиты информации требуется не просто разработки частных механизмов защиты, а также систематического подхода, содержащего совокупность взаимосвязанных мер для защиты информации (нормативно-правовых актов, морально-этических мер противодействия и т.д.).

Основной целью курсовой работы считается исследование способов защиты информации в инфокоммуникационных сетях.

Для достижения этой цели необходимо решить следующие задачи:

1 отметить суть проблемы и проанализировать проблемы защиты информации в информационных и в инфокоммуникационных сетях.

2 определить угрозы данных и методы их влияний на объекты защиты информации.

3 проанализировать способы и средства защиты информации.

4 выявить теорию информационной безопасности предприятия.

**1 Основные положения теории защиты информации.**

**1.1 Сущность проблемы и задачи защиты информации в информационных и инфокоммуникационных сетях.**

Широкое использование компьютерных технологий в автоматизированных методах обработки данных, находящихся в компьютерных системах, привело к обострению проблемы защиты от несанкционированного допуска. Защита данных в компьютерных системах обладает рядом своеобразных особенностей, сопряженных с тем, то, что они могут свободно и быстро копироваться и распространяться согласно каналам связи. Установлено огромное количество угроз, которые могут быть выполнены с внешних и внутренних сторон.

В виде стандартной модели информационной безопасности зачастую приводят модель, состоящую из трех различных категорий [1]::

- конфиденциальность – представляет собой состояние информации, при котором допуск к ней осуществляют лишь субъекты, которые имеют такое право;

- целостность – представляет собой избежание несанкционированных изменений информации;

- доступность – представляет собой избежание постоянного или временного сокрытия информации от юзеров, которые получили права доступа.

Также нельзя забывать, что всегда существует принципиальная возможность съема информации с ОВ оптического кабеля. Несанкционированный доступ к ВОЛС, несмотря на сложность и дороговизну, все-таки возможен.

В результате этого, безопасность информации представляет систему, защищающую секретность информации при ее вводе (выводе), обрабатывании, передаче и сохранении, а также того, что противодействует их разрушению и хищению.

Что качается задач обеспечения безопасности, то они разделяются на виды [2]:

- защита данных в каналах связи криптографическими способами;

- доказательство подлинности объектов информации и пользователей;

- выявление нарушений целостности информации;

- предоставление защиты от внедрения программных вирусов;

- обеспечение сохранности секретной информации.

**1.2 Угрозы информации. Способы их воздействия на объекты защиты информации**

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации, её отождествляют, как правило, либо с характером (типом, методом) дестабилизирующего влияния на данные, либо с последствиями (итогами) подобного воздействия. Угрозы систематизируются по показателям вреда субъекту при несоблюдении мер безопасности. Угроз на самом деле большое количество. При обеспечении регистрации данных это может быть кражей (копирование) данных и средств ее обрабатывания, а кроме того ее потеря (рисунок 1).



Рисунок 1 – Угрозы информационной безопасности

Что касается основных типов угроз, то к ним относят:

1 Угрозы конфиденциальности – несанкционированный доступ к данным (например, получение посторонними лицами сведений о состоянии счетов клиентов банка).

2 Угрозы целостности – несанкционированная модификация, дополнение или уничтожение данных (например, внесение изменений в бухгалтерские проводки с целью хищения денежных средств).

3 Угрозы доступности – ограничение или блокирование доступа к данным (например, невозможность подключится к серверу с базой данных в результате атаки типа «отказ в обслуживании»).

К источникам угроз безопасности информации можно отнести внешние и внутренние источники, которые мы можем наблюдать в таблице 1.

Таблица 1 - Источники угроз безопасности информации

|  |  |
| --- | --- |
| Внешние источники | компьютерные вирусы и иные вредоносные программы |
| работа зарубежных финансовых структур, направленная против интересов России |
| несанкционированный доступ к информации со стороны заинтересованных организаций и отдельных лиц |
| стихийные катастрофы |
| Внутренние источники | ошибки пользователей и сисадминов |
| ошибки в работе ПО |
| нарушение сотрудниками компании регламентов по работе с информацией |
| незаконные действия разных структур и ведомств, приводящие к нарушению законных прав сотрудников в информационной сфере |
| преступная деятельность общественно-политических, экономических и криминальных структур и отдельных лиц в сфере развития, распространения и применения данных, нацеленная на причинение экономического вреда государству |

К способам воздействия угроз на объекты защиты информации можно отнести аппаратно-программные, информационные, организационно-правовые, физические, радиоэлектронные, последствия которых написаны в таблице 2.

Таблица 2 - способы воздействия угроз на объекты защиты информации

|  |  |
| --- | --- |
| Аппаратно-программные: | уничтожение / модификация информации в информационных системах |
| установку программных и аппаратных закладных устройств |
| внедрение программных вирусов |
| Информационные: | кража данных из баз данных и банков |
| несоблюдение технологии обработки данных |
| запрещенный допуск к информационным ресурсам |
| противозаконное копирование информации в информационных системах |
| несоблюдение адресности и своевременности информационного обмена |
| Организационно-правовые: | невыполнение условий законодательства в информационной сфере |
| закупка устарелых информационных технологий |
| незаконное ограничение допуска к документам, содержащим немаловажную для людей информацию |
| Физические: | разрушение либо кража машинных, либо других оригиналов носителей информации |
| кража аппаратных или программных ключей, а так же средств криптографической защиты информации |
| разрушение средств обрабатывания данных |
| поставку "зараженных" компонентов |
| Радиоэлектронными: | перехватывание данных в технических каналах утечки |
| влияние на парольно-ключевые системы |
| перехватывание, дешифрование и введение неверных данных в сетях передачи информации |
| введение электронных устройств перехвата данных |

Можно сказать, что надежная защита вероятна только лишь при единой системе безопасности информации в абсолютно во всех стадиях разработки, при модернизации аппаратно-программных средств, а кроме того при обработке, сохранении и передаче по каналам связи информацию с обширным использованием нынешних средств криптографической защиты, которая содержит в себе меры разных степеней защиты.

**2 Методы и средства защиты информации**

**2.1 Традиционные меры и методы защиты информации**

С целью обеспечения сохранности данных в инфокоммуникационных сетях ведутся разнообразные мероприятия, под названием «система защиты данных». Система защиты данных – это совокупность мер, программно-технических средств, законных и морально-этических общественных норм, нацеленных на противодействие угрозам нарушителей с целью сведения вплоть до минимального количества вреда пользователям и собственникам системы.

Традиционные меры в целях противодействия утечкам данных разделяются на организационные и технологические. [3]

К *технологическим* мерам можно причислить защиту от несанкционированного допуска к системе, сохранение наиболее значимых компьютерных подсистем, организацию вычислительных сетей с перераспределением ресурсов в случае не работоспособности отдельных звеньев, установку разного рода приборов для обнаружения и тушения пожара, утверждение конструкционных мер защиты оборудования и информации от хищений, саботажа, диверсий, оснащение помещений замками и сигнализациями и т.д.

К *организационным* мерам относится служба охраны серверов, собеседование и отбор персонала, присутствие плана восстановления работы сервера при его сбоях, универсальность средств охраны информации от людей (в том числе все руководство).

Несанкционированный допуск к информации способен совершаться в период профилактики либо ремонтных работ оборудования за счет чтения остаточных данных на носителях, невзирая на удаление их пользователем. Другой способ – чтение данных с носителя в период его транспортировки в отсутствии защиты внутри объекта либо региона.

Современные компьютерные ресурсы созданы на интегральных схемах. Работа таких схем заключается в высокочастотных изменениях уровней напряжения и токов, то, что приводит к появлению в цепях питания у рядом стоящей техники и т.п. электромагнитных полей, которые при помощи специальных средств (называемых "шпионскими") возможно трансформировать в обработанные данные. С уменьшением дистанции от приемника нарушителя и аппаратными средствами возможность подобного рода съема и расшифровки данных возрастает. Несанкционированный взлом данных возможен также при прямом подсоединении нарушителя к каналам связи и к различным сетевым оборудованиям.

Традиционными способами защиты данных от несанкционированного допуска считаются идентификация, аутентификация и защита пользователя паролями. [4]

В компьютерных системах находится информация, право на использование которой могут только конкретные личности либо группа лиц, действующих в результате индивидуальной инициативы либо в соответствии со своими обязанностями.

Для того, чтобы гарантировать безопасность информационных ресурсов и ликвидировать вероятность несанкционированного допуска вводятся разнообразные системы опознавания, определения подлинности объекта (субъекта).

Ключевыми понятиями защиты информации являются идентификация и аутентификация. Идентификация – это присвоение предмету (субъекту) уникального имени. Аутентификация (установление подлинности) - это контроль, при котором проверяется объект (субъект), является ли он тем, за кого себя выдает.

Под идентификацией принято понимать присвоение субъектам доступа уникальных идентификаторов и сравнение таких идентификаторов с перечнем возможных. В свою очередь, аутентификация понимается как проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Тем самым, задача идентификации – ответить на вопрос «кто это?», а аутентификации – «а он ли это на самом деле?».

Для того чтобы наглядно представить базовую схему идентификации и аутентификации рассмотрим рисунок 2.

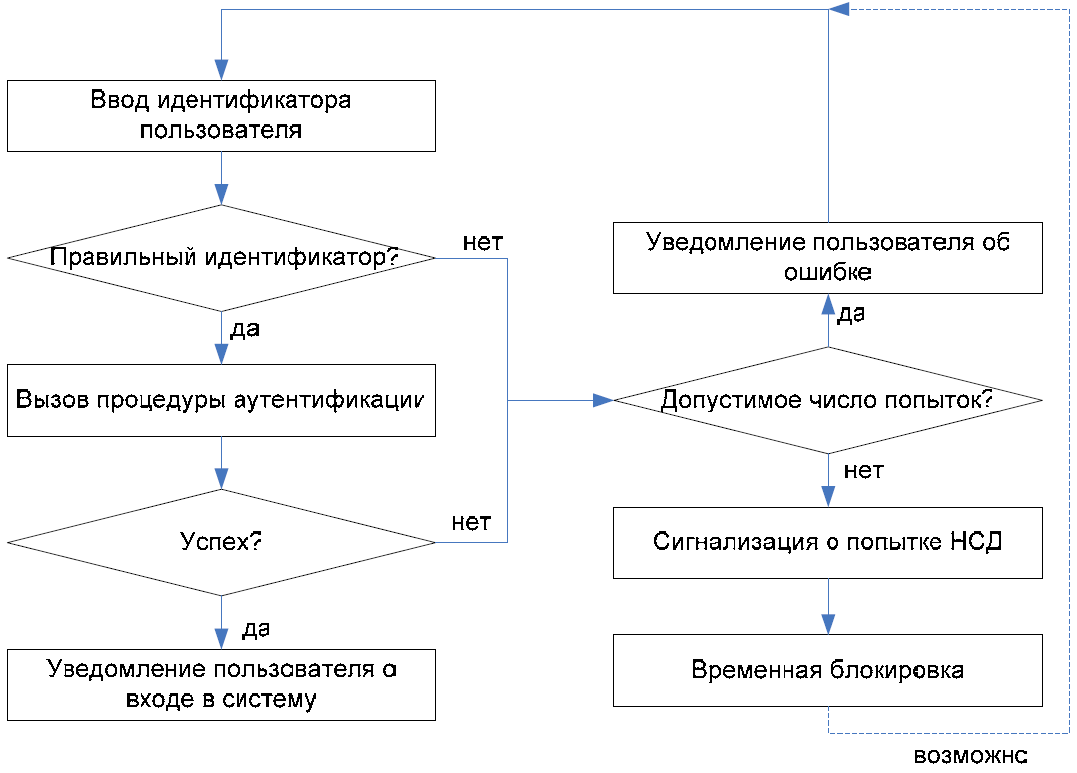


Рисунок 2 - Базовая схема идентификации и аутентификации

Приведённая схема учитывает возможные ошибки оператора при проведении процедуры аутентификации: если аутентификация не выполнена, но допустимое число попыток не превышено, пользователю предлагается пройти процедуру идентификации и аутентификации еще раз.

При всём многообразии существующих механизмов аутентификации, наиболее распространённым из них остаётся парольная защита. Для этого есть несколько причин, из которых мы отметим следующие:

- относительная простота реализации. Действительно, реализация механизма парольной защиты обычно не требует привлечения дополнительных аппаратных средств.

- традиционность. Механизмы парольной защиты являются привычными для большинства пользователей автоматизированных систем и не вызывают психологического отторжения – в отличие, например, от сканеров рисунка сетчатки глаза.

Подлинность объекта может производиться аппаратным устройством, программой, пользователем и т.д. Для этого используют пароли.

Пароль – совокупность знаков (символов), характеризующая объект (субъекта). При подборе пароля возникают проблемы с его объемом, стойкости к несанкционированному подбору, методам его использования. Безусловно, чем длиннее пароль, тем лучше будет защищен, поскольку понадобятся огромные усилия для его отгадывания. Например, оценим элементарные взаимосвязи между основными параметрами парольных систем. Введём следующие обозначения:

- A – мощность алфавита паролей;

- L – длина пароля;

- S= AL – мощность пространства паролей;

- V – скорость подбора паролей;

- T – срок действия пароля;

- P – вероятность подбора пароля в течение его срока действия.

Очевидно, что справедливо следующее соотношение:



Обычно скорость подбора паролей V и срок действия пароля T можно считать известными. В этом случае, задав допустимое значение вероятности P подбора пароля в течение его срока действия, можно определить требуемую мощность пространства паролей S. Заметим, что уменьшение скорости подбора паролей *V* уменьшает вероятность подбора пароля.

Так же стоит отметить, что выбор длины пароля в существенной степени формируется развитием технического оборудования, их элементной базой и быстродействием. В случае использования пароля следует время от времени его менять, для того, чтобы уменьшить возможность его перехвата путем прямого хищения носителя, снятия его копии и в том числе и физического принуждения лица. Пароль вводится пользователем в начале взаимодействия с компьютерной системой, в некоторых случаях и в завершении сеанса (в наиболее ответственных случаях пароль стандартного выхода может различаться от входного).

Так же существуют средства защиты информации, которые согласно способам осуществления, возможно, разбить на 3 категории:

- программные;

- программно-аппаратные;

- аппаратные.

Программными средствами защиты информации называют намеренно созданные программы, которые выполняют функции безопасности вычислительной системы, реализовывают функцию ограничения допуска пользователей согласно паролям, ключам, многоуровневому доступу и т.д. Эти программы имеют все шансы быть выполнены почти в каждой операционной системе, комфортной для пользователя, эти программные ресурсы обеспечивают довольно высокий уровень защиты системы и являются недорогими. При подсоединении такого рода системы в всемирную сеть возможность взлома защиты увеличивается. Таким образом, этот метод защиты применим для локальных закрытых сетей, никак не имеющих выход в глобальную сеть.

Программно-аппаратными средствами называют устройства, реализованные на многоцелевых или специализированных микропроцессорах, никак не требующие модификаций в схемотехнике при изменении метода функционирования. Данные устройства приспосабливаются к каждой операционной системе, так как они имеют большей уровень защиты. Они обойдутся немного дороже (их стоимость находится в зависимости от вида операторной системы). При этом такие устройства считаются наиболее гибким инструментом, позволяющим вносить изменения в конфигурацию при необходимости пользователя. Программно-аппаратные ресурсы гарантируют значительно высокий уровень защиты локальной сети, подключенной к всемирной.

Аппаратными средствами называют устройства, в которых функциональные узлы реализуются в сверхбольших интегральных системах (СБИС) с неизменяемым методом функционирования. Данный вид приборов приспосабливается в каждой операционной системе, считается наиболее дорогостоящим в разработке, предъявляет высокие технологические требования при изготовлении. В то же время данные устройства владеют наиболее значительным уровнем защиты, в них нереально проникнуть и внести конструктивные либо программные изменения. Использование аппаратных средств затруднено в связи их большой цены и статичности алгоритма. Программно-аппаратные средства, уступают аппаратным по скорости, но предоставляют возможность в любое время свободно изменить алгоритм функционирования и никак не обладают недостатками программных способов.

Так же существуют программы выявления нарушений в режиме реального времени, которые относятся к отдельной группе мер по обеспечению безопасности информации.

**2.2 Криптографические методы и средства защиты информации.**

Криптографические методы защиты необходимы во всех случаях обеспечения безопасности (независимо от того, применяются они в сети или вне ее) и основаны на шифровании информации и программ. Шифрование программ гарантирует невозможность внесения в них изменений. Криптографическая защита данных осуществляется как при их хранении, так и при передаче по сети. В настоящее время доступны как программная, так и высокопроизводительная аппаратная реализация средств криптографии.

Известны несколько классификаций криптографических алгоритмов (КА). Одна из них подразделяет КА в зависимости от числа ключей, применяемых в конкретном алгоритме :

- бесключевые КА — не используют в вычислениях никаких ключей;

- одноключевые КА — работают с одним ключевым параметром (секретным ключом);

- двухключевые КА — на различных стадиях работы в них применяются два ключевых параметра: секретный и открытый ключи. [5]

Интерес к изучению адаптации алгоритмов к разным аппаратным и программным платформам обусловлен формированием кроссплатформенных инфокоммуникационных систем на основе единых стандартов. Один и тот метод обязан продуктивно выполняться в разных аппаратных и программных платформах с мобильного телефона вплоть до маршрутизатора, от сим-карты до персонального компьютера.

Существующие ресурсы защиты информации в инфокоммуникационных сетях, возможно разбить на 2 категории: симметричные криптосистемы и асимметричные криптосистемы.

*Симметричные криптосистемы* построены на основе сохранения в тайне ключа шифрования. Процессы зашифрования и расшифрования используют один и тот же ключ (рисунок 3). Секретность ключа является постулатом. Основная проблема при применении симметричных криптосистем для связи заключается в сложности передачи обоим сторонам секретного ключа. Однако данные системы обладают высоким быстродействием. Раскрытие ключа злоумышленником грозит раскрытием только той информации, что была зашифрована на этом ключе.

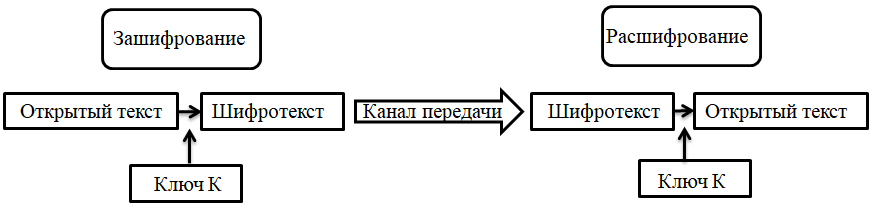


Рисунок 3 - Структура симметричной криптосистемы

Что касается *асимметричных криптосистем*, то они считаются наиболее перспективными системами криптографической защиты данных, называемые также системами с открытым ключом. Их суть состоит в том, что ключ, используемый асимметричных для зашифровывания, отличен от ключа расшифровывания (рисунок 4). При этом ключ зашифровывания не секретен и может быть известен всем пользователям системы. Однако расшифровывание с помощью известного ключа зашифровывания невозможно. Для расшифровывания используется специальный, секретный ключ. При этом знание открытого ключа не позволяет определить секретный ключ. Таким образом, расшифровать сообщение может только его получатель, владеющий этим секретным ключом.

Суть криптографических систем с открытым ключом сводится к тому, что в них используются так называемые необратимые функции (иногда их называют односторонними или однонаправленными), которые характеризуются следующим свойством: для данного исходного значения с помощью некоторой известной функции довольно легко вычислить результат, но рассчитать по этому результату исходное значение чрезвычайно сложно.

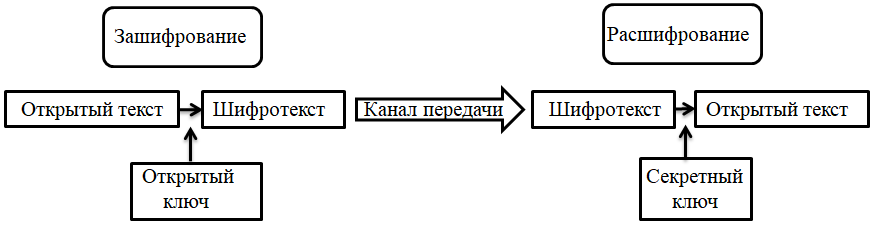


Рисунок 4 - Структура асимметричной криптосистемы

Кроме этого, имеется вероятность кодирования данных и наиболее простым методом — с применением генератора псевдослучайных чисел. Применение генератора псевдослучайных чисел состоит в генерации гаммы шифра с поддержкой генератора псевдослучайных чисел при конкретном ключе и наложении полученной гаммы на открытые данные обратимым способом. Данный способ шифровальной защиты реализуется довольно свободно и гарантирует достаточно большую быстроту кодирования.

Так же различают два способа шифрования: канальное и оконечное (абонентское) (рисунок5).



Рисунок 5 – Особенности способов шифрования

Таким образом, любая криптографическая система шифрования надежна лишь настолько, насколько полно она отвечает следующим требованиям:

- Невозможность ее раскрытия даже при известном тексте, а в случае раскрытия сообщения - гарантия безопасности сообщений, которые были переданы ранее, и тех, которые будут переданы в дальнейшем;

- Достаточно большое число вариантов шифрования, не позволяющее раскрыть истинное содержание информации даже с использованием современных вычислительных средств;

- Высокая сложность шифра, не позволяющая раскрыть его с применением различных математических методов;

- Гарантированная надежность хранения ключа и алгоритма шифрования, а также самих шифровальных устройств.

В развитых странах прослеживается широкий диапазон суждений по вопросу, о регламентации использования алгоритмов шифрования. Высказываются предложения от абсолютного запрета обширного использования шифровальных способов вплоть до абсолютной независимости их применения. Некоторые предложения относятся к разрешению использования только лишь ослабленных алгоритмов либо к установлению режима обязательной регистрации ключей кодирования.

Из всего изложенного следует, что надежная криптографическая система должна удовлетворять таким требованиям: [6]

- процедуры зашифровывания и расшифровывания должны быть "прозрачны" для пользователя;

- дешифрование закрытой информации должно быть максимально затруднено;

- содержание передаваемой информации не должно сказываться на эффективности криптографического алгоритма;

- надежность криптозащиты не должна зависеть от содержания в секрете самого алгоритма шифрования.

В заключении можно сказать, то, что криптография гарантирует безопасность информации в интернете и в настоящее время стремительно развивается.

**2.3 Нетрадиционные методы защиты информации**

Для нетрадиционных задач защиты электронной информации, одной из которых является аутентификация электронной информации в условиях, не доверительного обмена информацией между пользователями, приобрело название системы электрической цифровой подписи (ЭЦП).

Электронно-цифровая подпись (ЭЦП) - это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. Федеральные органы государственной власти и все организации, участвующие в документообороте, применяют её для подписания своих электронных документов. [7]

Существует три вида электронной цифровой подписи:

- простая электронно-цифровая подпись;

- усиленная неквалифицированная электронно-цифровая подпись;

- усиленная квалифицированная электронно-цифровая подпись.

Электронная цифровая подпись во многом является аналогом

рукописной подписи – в частности, к ней предъявляются практически аналогичные требования:

1 Цифровая подпись должна позволять доказать, что именно законный автор, и никто другой, сознательно подписал документ.

2 Цифровая подпись должна представлять собой неотъемлемую часть документа. Должно быть невозможно отделить подпись от документа и использовать её для подписывания других документов.

3 Цифровая подпись должна обеспечивать невозможность изменения

подписанного документа (в том числе и для самого автора!).

4 Факт подписывания документа должен быть юридически доказуемым. Должен быть невозможным отказ от авторства подписанного документа.

В простейшем случае для реализации цифровой подписи может быть использован механизм, аналогичный асимметричной криптосистеме. Разница будет состоять в том, что для зашифровки (являющегося в данном случае подписыванием) будет использован секретный ключ, а для расшифровки , играющего роль проверки подписи, - общеизвестный открытый ключ (рисунок 6), таким образом, после процесса передачи, подпись будет верна тогда когда M=M’.

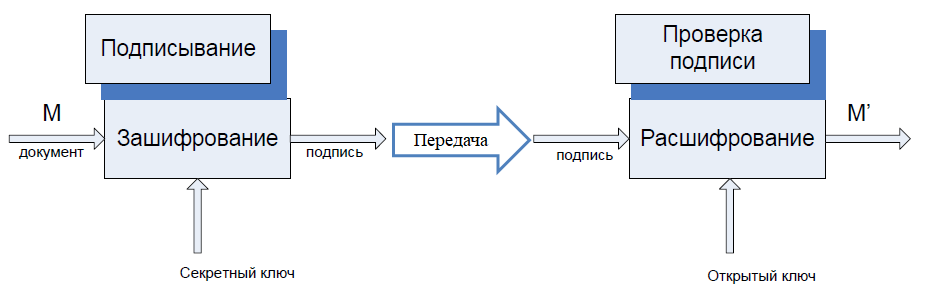


Рисунок 6 - Реализация механизма цифровой подписи

Электронная цифровая подпись на сегодняшний день в большей мере используется в работе юридических лиц. Особенно ее применение актуально для организаций, имеющих большое количество подразделений или заключающих сделки с контрагентами, находящимися от них на значительном расстоянии.

**3 Информационная безопасность предприятия.**

**3.1 Концепция информационной безопасности предприятия**

Характерным показателем коммерческой деятельности считается стремление к получению максимальной прибыли. Помимо этого, одной из характерных отличительных черт коммерческой деятельности является то, то, что она осуществляется в условиях жесткой конкуренции.

Конкурентное соперничество это двигатель коммерческой деятельности, а кроме того условие выживания коммерческих предприятий. Отсюда их стремление сберечь в тайне от соперника способы и особенности личной работы, которые обеспечивают им превосходство над соперником. Защищаемые тайны коммерческой деятельности приобрели наименование коммерческой тайны. Под коммерческой тайной предприятия понимаются не являющиеся государственными тайнами данные, связанные с производством, финансами и иной работой компании, разглашение которых способно причинить вред предприятию.

Уязвимость информации выражается в разных конфигурациях. К подобным конфигурациям, выражающим результаты дестабилизирующего влияния на информацию, относятся:

- кража носителя информации либо кража информации с самого носителя (хищение);

- утрата носителя данных (потеря);

- неразрешенное уничтожение носителя информации;

- изменение информации (несанкционированное изменение, фальсификация);

- блокировка данных;

- разглашение информации (распространение).

Та либо другая модель уязвимости информации может осуществляться вследствие намеренного либо ненамеренного дестабилизирующего воздействия различными способами на носитель информации либо на саму информацию со стороны источников воздействия, которыми могут быть: общество, технические средства обрабатывания и передачи информации, ресурсы связи, стихийные бедствия и др.

Способами дестабилизирующего воздействия на информацию считаются: копирование, записывание, передача, нарушение технологии обрабатывания и сохранения информации, физическое воздействие на данные и др.

Реализация форм проявления уязвимости данных приводит или может привести к двум типам уязвимости - утрате либо утечке данных.

Утечка информации в компьютерных системах может быть допущена как случайно, так и умышленно, с применением технических средств съема данных.

К утрате информации приводит кража и потеря носителей информации, неразрешенная порча носителей информации либо саму информацию на этих носителям, что подразумевает изменение и блокировку информации. Утрата может являться абсолютной либо частичной, безвозвратной либо временной, однако в каждом случае она причиняет вред владельцу данных.

Несанкционированный доступ – это беззаконное преднамеренное овладение секретной информации личностью, никак не имеющим права доступа к этой информации.

Наиболее популярными способами несанкционированного доступа к информации считаются:

- перехватывание электронных излучений;

- использование подслушивающих приборов (закладок);

- дистанционная фотосъемка;

- перехватывание звуковых излучений и восстановление текста принтера;

- копирование носителей данных с преодолением мер защиты;

- маскировка под зарегистрированного пользователя и требования концепции;

- применение программных ловушек;

- применение недостатков языков программирования и операционных систем;

- противозаконное подключение к технике и линиям связи

- расшифровка специальными программами зашифрованных данных;

- информационные вирусы.

Перечисленные пути несанкционированного доступа требуют довольно крупных технических знаний и соответствующих аппаратных и программных разработок со стороны взломщика. Причиной возникновения каналов утечки считаются конструктивные и технологические несовершенства схемных решений или эксплуатационный износ компонентов. Все это позволяет взломщикам создавать действующие на определенных физических принципах преобразователи, образующие путь передачи информации – канал утечки.

Для предоставления эффективного использования системы защиты информации в инфокоммуникационной сети компании при её построении следует принимать во внимание следующие условия: [8]

- интегрируемость. Средства защиты информации обязаны подходящим способом внедряться в инфраструктуру инфокоммуникационной сети;

- сертифицируемость. Используемые при построении системы защиты средства обязаны удовлетворять определенным стандартам и требованиям;

- эшелонированность. Система защиты обязана складываться из нескольких уровней. Нарушение защиты на каком-либо уровне никак не обязано повлечь за собою ослабления других уровней или недееспособности системы защиты в целом;

- контролируемость. События, сопряженные с функционированием системы защиты, обязаны контролироваться средствами мониторинга безопасности;

- масштабируемость. При построении системы защиты обязана быть обеспечена возможность её развития с учетом развития инфокоммуникационных сетей предприятия.

**3.2 Методы защита информации в инфокоммуникационных сетях предприятия.**

Отраслевой стандарт согласно информационной безопасности устанавливает защиту данных как деятельность, нацеленную на устранение утечки информации, от несанкционированных и непреднамеренных воздействий на данные. И в случае если первое направление (предотвращение утечки) обязано предостерегать разглашение секретной информации, несанкционированный доступ к ней, в таком случае два других направления защищают от схожих угроз (искажение конфиденциальных данных, их уничтожение, блокировки доступа и подобные действия с носителем информации). Все отличие состоит в наличии либо отсутствии умысла в действиях с информацией (рисунок 7).



Рисунок 7 - Защита информации на предприятии.

Больше всего угроз всё также формируют компьютерные вирусы и атаки распространителей спама.

Многие сети годами остаются открытыми, и неизвестно, то что в данном случае опаснее — сознательный взлом злоумышленником корпоративной сети с целью съема секретных данных либо же осуществляемая дезорганизация деятельности сети с помощью атак типа «отказ в обслуживании». Так как для небольших и средних коммерческих предприятий формирование специально защищенных линий связи нереально, приходится применять открытые каналы связи для обмена информацией, а это опасно как перехватом этих данных, так и нарушением их целостности. Внутри локальной сети актуальна проблема надежной аутентификации пользователей: широко известный пример прикрепления к монитору бумажки с записанным логином и паролем.

Зачастую никак не придается значимости разделению допуска среди работников организации. Тут возможно привести подобную аналогию: иерархию кабинетов все работники придерживаются незыблемо, ни одному человеку не приходит в голову занять столик либо комнатку руководства, а вот по отношению к секретной информации действует, так сказать, правило «любому — согласно интересам», и информация, предназначенная двум-трем топ-менеджерам, становятся известна всей фирме.

В качестве ещё одного канала возможной утечки, возможно охарактеризовать, к примеру, сервис-центры, в которые поступают диски с не уничтоженными надлежащим способом информацией.

Таким образом, можно сделать вывод: защита информации – одно из основных направлений работы каждой успешной компании. Перед специально отобранным для этого сотрудником (либо подразделением) встают следующие задачи:

- анализ угроз секретной информации, а также уязвимых зон автоматизированной системы и их предотвращение;

- формирование системы защиты информации - приобретение и установление необходимых средств (профилактика, обслуживание);

- подготовка персонала к работе со средствами защиты, контроль за их соблюдением;

- разработка алгоритма действий в экстремальных ситуациях и проведение постоянных "учений";

- разработка и реализация программы постоянной работы автоматизированной системы и плана восстановительных мероприятий (в случае вирусной атаки, сбоя/ошибки/отказа технических средств и т. д.).

В результате того, что многие фирмы и организации не могут себе позволить надежную систему защиты информации, они очень часто сталкиваются с одними и теми же проблемами в её защите, например: [9]

- Метод заплаток. «Кусочное» обеспечение защиты информации только в отдельных направлениях. Результат - невозможность отражать атаки на незащищенных участках, вследствие этого возникает угроза на всю систему в целом.

- Синдром амебы. Фрагментарное реагирование на любой новый раздражитель; зачастую смешивается с использованием «метода заплаток». Результат - задержка с отражением новых угроз.

- Стремление к экономии. Стремление создать систему защиты на без затратной основе. Результат - использование проблематичных и/или нелицензионных средств защиты, отсутствие поддержки со стороны производителей, постоянные усилия разобраться в абсолютно всем без помощи других, приводит к безрезультатным результатам.

Таким образом, в любой организации обязан быть создан следующий набор средств и способов для защиты информации в сети. (рисунок 8)

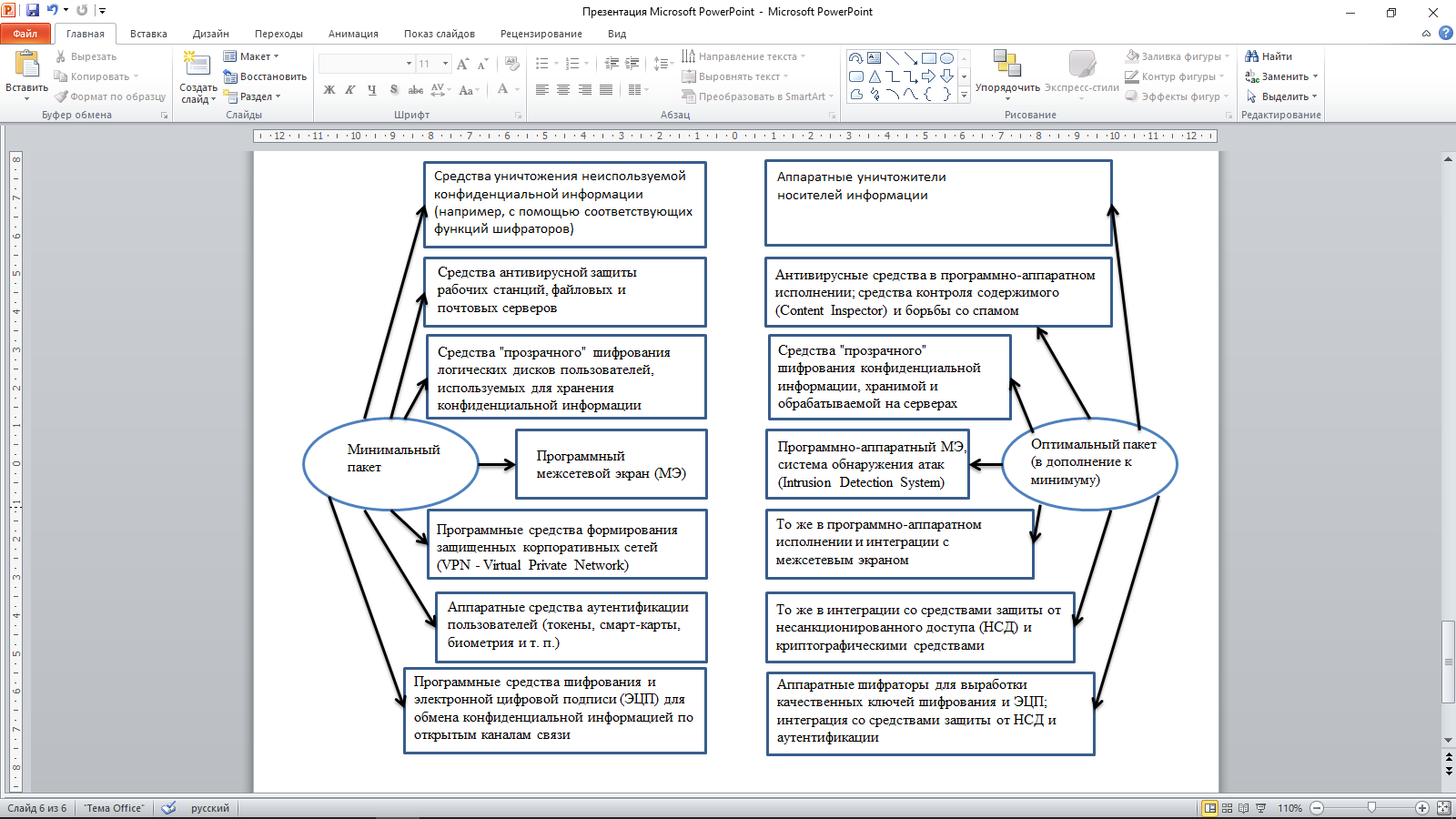


Рисунок 8 - Набор средств и методы защиты информации

**ЗАКЛЮЧЕНИЕ**

В результате проведённой работы по изучению проблем методов защиты информации в инфокоммуникационных сетях можно сделать несколько заключений: проблемы, сопряженные с повышением безопасности информационной сферы, считаются многоплановыми и сложными. Развитие информационных технологий способствует к совместным усилиям по совершенствованию методов, позволяющим оценивать угрозы безопасности информации и реагировать на них. Главной задачей обеспечения безопасности информации считается предотвращение несанкционированного доступа к секретной информации, находящейся в инфокоммуникационных сетях.

Для защиты информации нужно использовать различные средства и методы, для достижения надежной передачи, хранения и обработки информации, следует отметить ряд основных задач, решение которых в информационных системах и инфокоммуникационных сетях гарантируют защиту информации, например:

- организация доступа к данным только лишь допущенных к ней лиц;

- подтверждение истинности данных;

- защита от перехвата данных при передаче их по каналам связи;

- защита от искажений и ввода ложных данных.

Уберечь информацию – это означает:

- обеспечить физическую целостность информации, т.е. никак не позволить искажений либо порчи её элементов;

- не позволить подмены (изменения) элементов информации при сохранении ее целостности;

- не позволить несанкционированного получения информации лицами или процессами, не обладающими на это определенными полномочиями;

- быть уверенным в том, что передаваемая информация будет использоваться только в соответствии с обговоренными условиями.

Для решения проблем защиты электронной информации обязаны использоваться криптографические методы, которые дают возможность решить важнейшие проблемы защищённой автоматизированной обработки и передачи информации. Криптографические преобразования информации считаются более эффективным средством обеспечения конфиденциальности информации, её целостности и подлинности. Электронная цифровая подпись (ЭЦП) - вид аналога собственноручной подписи, являющийся средством защиты информации, которая используется для контроля целостности и подтверждения подлинности электронных документов.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Гмурман А.И. Информационная безопасность / А.И. Гмурман – М.: БИТ-М, 2004. – 23-35 c.

2. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян – СПб.: BHV, 2000. – С. 56.

3. Конахович Г. Ф. Защита информации в телекоммуникационных системах / Г. Ф. Конахович – М.: МК-Пресс,2005. – 123 c.

4. Коржов В. В. Стратегия и тактика защиты / В. В. Коржов // Compu-terworld Россия. – 2004. – №14. – 26 с.

5. Цирлов В. Л. Основы информационной безопасности автоматизированных систем / В. Л. Цирлов – М.: Изд-во Феникс, 2008. – 38 с.

6. Молдовян А. А. Криптография / А. А. Молдовян, Н. А. Молдовян, Б. Я. Советов – СПб.: Издательство “Лань”, 2001. – С. 56-76.

7. Семенов Г. Цифровая подпись. // Открытые системы.– 2002. – №07–08. – С. 67-78.

8. Биячуев Т.А. Безопасность корпоративных сетей / Т. А. Биячуев – СПб: СПбГУ ИТМО, 2004. – С.187.

9. Мельников В. Защита информации в компьютерных системах / В. Мельников. – М.: Финансы и статистика – Электронинформ, 1997. – 79-81 с.