***Реферат***

***по информатике и ИКТ на тему***

***«Защита информации»***

**Ученицы:** 10Б класса

МАОУ СОШ №68

с углубленным изучением отдельных предметов

Петушковой Татьяны

**Учитель:**

Ставрова Ольга Аркадьевна

***Оглавление***

[Введение 3](#_Toc435372249)

[Защита информации как закономерность развития компьютерных систем 4](#_Toc435372250)

[Объекты и элементы защиты в компьютерных системах обработки данных 5](#_Toc435372251)

[Виды угроз 7](#_Toc435372252)

[Средства опознания и разграничения доступа к информации 8](#_Toc435372253)

[Криптографический метод защиты информации 10](#_Toc435372254)

[Компьютерные вирусы 11](#_Toc435372255)

[Антивирусные программы 12](#_Toc435372256)

[Заключение 13](#_Toc435372257)

# **Введение**

С развитием техники и технологий окружающая нас информация стремительно возрастает, и человек уже не в силах хранить ее в собственной памяти. На помощь к нему приходят современные средства хранения информации, информационные системы. Но сохраняя информацию, на каком-либо носителе мы подвергаем себя опасности вероятного доступа третьих лиц. Много способов доступа к информации, большое количество квалифицированных специалистов, подавляющее использование специальных технических средств в общественном производстве позволяют нарушителям практически в любой момент и в любом месте проводить мероприятия, которые представляют собой угрозу для информационной безопасности. Поэтому информационная безопасность не только становится обязательной, но и выступает как одна из важнейших характеристик информационной системы. Большинство современных предприятий, занимающихся бизнесом в любом направлении, не могут вести нормальную деятельность без уверенности в обеспечении безопасности своей информацией. Нельзя забывать и про персональные компьютерные системы, связанные между собой сетью интернет, на которых и тренируются взломщики.

Человека, пытающегося нарушить работу информационной системы или получить неразрешенный доступ к информации, называют **взломщиком**, а иногда **«компьютерным пиратом» (хакером)**.

Термин «информация» сейчас больше используется для обозначения специального товара, который можно купить, продать, обменять на что-то другое и т.д. В общем смысле информация содержит сведения об окружающем нас мире, являющихся объектом хранения, передачи, преобразования и использования их для определенных целей. Исходя из этого человек размещается в постоянно изменяющемся информационном поле, влияющим на его действия и образ жизни. Информация по своему характеру может быть экономической, военной, политической, научно-технической, производственной или коммерческой. По степени секретности можно разделить информацию на **секретную (конфиденциальную)** или **несекретную**. К секретной (конфиденциальной) информации относят сведения, содержащие коммерческую тайну, некоторые виды служебной тайны, врачебную тайну, адвокатскую и следственную тайну, тайну переписки, почтовых и телеграфных отправлений, телефонных переговоров, а также сведения о частной жизни и деятельности граждан.

Защите подлежит только та информация, которая имеет цену. А ценной информация становится, когда ее обладатель может получить какую-либо выгоду: моральную, материальную или политическую.

С современным развитием информационного общества очень большое значение приобретают проблемы, связанные с защитой конфиденциальной информации. Информация как категория, имеющая стоимость, защищается ее собственником от лиц и организаций, пытающихся завладеть ее любыми способами. В связи с этим складывается тенденция, что чем выше уровень секретности информации, тем выше и уровень ее защиты, а значит, тем больше средств затрачивается на ее защиту.

Высокой эффективностью защиты информации можно определить, как совокупность следующих факторов: своевременность, активность, непрерывность и комплексность. Очень важно проводить профилактические защитные мероприятия комплексно, то есть гарантировать нейтрализацию всех опасных каналов утечки информации. Нельзя забывать, что один открытый канал утечки информации может свести на нет эффективность всей системы защиты.

# **Защита информации как закономерность развития компьютерных систем**

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Защита информации –** это применение различных средств и методов, использование мер и осуществление мероприятий для того, чтобы обеспечить систему надежности передаваемой, хранимой и обрабатываемой информации.

**Защита информации включает в себя:**

* обеспечение физической целостности информации, исключение искажений или уничтожения элементов информации;
* недопущение подмены элементов информации при сохранении ее целостности;
* отказ в несанкционированном доступе к информации лицам или процессам, которые не имеют на это соответствующих полномочий;
* приобретение уверенности в том, что передаваемые владельцем информационные ресурсы будут применяться только в соответствии с обговоренными сторонами условиями.

Проблема защиты информации в системах электронной обработки данных возникла практически одновременно с их созданием. Ее вызвали конкретные факты злоумышленных действий над информацией.

Важность проблемы по предоставлению надежности информации подтверждается затратами на защитные мероприятия. Для обеспечения надежной системы защиты необходимы значительные материальные и финансовые затраты. Перед построением системы защиты должна быть разработана оптимизационная модель, позволяющая достичь максимального результата при заданном или минимальном расходовании ресурсов.

Если в первые десятилетия активного использования ПК основную опасность представляли хакеры, подключившиеся к компьютерам в основном через телефонную сеть, то в последнее десятилетие нарушение надежности информации прогрессирует через программы, компьютерные вирусы, глобальную сеть Интернет.

**Способы несанкционированного доступа к информации:**

* просмотр;
* копирование и подмена данных;
* ввод ложных программ и сообщений в результате подключения к каналам связи;
* чтение остатков информации на ее носителях;
* прием сигналов электромагнитного излучения и волнового характера;
* использование специальных программ.

Для борьбы со всеми этими способами несанкционированного доступа необходимо разрабатывать, создавать и внедрять многоступенчатую непрерывную и управляемую архитектуру безопасности информации.Защищать следует не только информацию конфиденциального содержания. Для того чтобы обеспечить достаточно высокий уровень безопасности данных, надо найти компромисс между стоимостью защитных мероприятий, неудобствами при использовании мер защиты и важностью защищаемой информации.

# **Объекты и элементы защиты в компьютерных системах обработки данных**

**Объект защиты** – это такой компонент системы, в котором находится защищаемая информация.

**Основными объектами информации являются:**

* **Информационные ресурсы**, содержащие сведения, связанные с конфиденциальной информацией и государственной тайной;
* **Технические средства приёма, обработки и хранения информации (ТСПИ)**;
  + **Информационные системы** (сети и системы, средства вычислительной техники);
  + **Программные средства** (операционные системы, системы управления базами данных, прикладное программное обеспечение);
  + **Технические средства приёма, автоматизированные системы управления, системы связи и передачи данных, передачи и обработки информации ограниченного доступа** (звукозапись, звукоусиление, звуковоспроизведение, переговорные и телевизионные устройства, средства тиражирование и изготовления документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации).
* **Вспомогательные технические средства и системы (ВТСС)**.
  + **Системы пожарной и охранной сигнализации**;
  + **Технические средства телефонной, громкоговорящей связи, радиотрансляции, часофикации**;
  + **Контрольно-измерительная аппаратура**;
  + **Средства и системы передачи данных в системе радиосвязи**;
  + **Электробытовые приборы**;
  + **Помещения, предназначенные для обработки данной информации, имеющей ограниченное распространение**.
* ТСПИ можно рассматривать как систему, включающую в себя **стационарное оборудование, соединительные линии, периферийные устройства, системы электропитания, распределительные и коммуникационные устройства и системы заземления**.

**Элемент защиты** – это совокупность данных, которая может содержать необходимые защите сведения.

**При деятельности компьютерных систем могут возникать:**

* отказы и сбои аппаратуры;
* системные и системотехнические ошибки;
* программные ошибки;
* ошибки человека при работе с компьютером.

Для обеспечения безопасности проводятся разные мероприятия, которые объединены понятием «система защиты информации».

**Система защиты информации** – это совокупность организационных (административных) и технологических мер, программно-технических средств, правовых и морально-этических норм, которые применяются для предотвращения угрозы нарушителей с целью сведения до минимума возможного ущерба пользователям и владельцам системы.

**Организационно-административными средствами защиты** называется регламентация доступа к информационным и вычислительным ресурсам, а также функциональным процессам систем обработки данных. Эти средства защиты применяются для затруднения или исключения возможности реализации угроз безопасности.

**Типичные организационно-административные средства:**

* допуск к обработке и передаче охраняемой информации только проверенных должностных лиц;
* хранение носителей информации, которые представляют определенную тайну, а также регистрационных журналов в сейфах, недоступных для посторонних лиц;
* учет применения и уничтожения документов (носителей) с охраняемой информацией;
* разделение доступа к информационным и вычислительным ресурсам должностных лиц в соответствии с их функциональными обязанностями.

**Технические средства защиты** применяются для создания некоторой физически замкнутой среды вокруг объекта и элементов защиты.

**При этом используются такие мероприятия, как:**

* ограничение электромагнитного излучения через экранирование помещений, в которых осуществляется обработка информации;
* реализация электропитания оборудования, отрабатывающего ценную информацию, от автономного источника питания или общей электросети через специальные сетевые фильтры.

**Программные средства и методы защиты** являются более активными, чем другие применяемые для защиты информации в ПК и компьютерных сетях. **Реализуются с помощью различных программ:** операционных систем, программ обслуживания, антивирусных пакетов, инструментальных систем (СУБД, электронных таблиц, текстовых процессоров, систем программирования и т. д.).

**Они реализуют следующие функции защиты:**

* разграничение и контроль доступа к ресурсам;
* регистрация и изучение протекающих процессов;
* предотвращение возможных разрушительных воздействий на ресурсы;
* криптографическая защита информации.

Под **технологическими средствами защиты информации** понимаются ряд мероприятий, органично встраиваемых в технологические процессы преобразования данных.

**В них также входят:**

* создание архивных копий носителей;
* ручное или автоматическое сохранение обрабатываемых файлов во внешней памяти компьютера;
* автоматическая регистрация доступа пользователей к различным ресурсам;
* выработка специальных инструкций по выполнению всех технологических процедур и др.

**Правовые и морально-этические меры и средства защиты включают:**

* действующие в стране законы;
* действующие нормативные акты;
* регламентирующие правила;

# **Виды угроз**

Исследования случаев воздействия на информацию и несанкционированного доступа к ней показывают, что их можно разделить на **случайные** и **преднамеренные**.

1. **Случайные угрозы**

Основными причинами случайных воздействий на автоматизированные системы при их эксплуатации могут быть:

* сбои и отказы аппаратуры;
* помехи на линиях связи от воздействия внешней среды;
* ошибки человека как звена системы;
* системотехнические и схемные ошибки разработчиков;
* алгоритмические, структурные и программные ошибки;
* аварийные ситуации.

При выборе и проектировании системы, слабой в отношении надежности функционирования аппаратуры, частота отказов и сбоев аппаратуры увеличивается.

1. **Преднамеренные угрозы**

Преднамеренные угрозы обычно связаны с действиями, какого-либо человека, причинами которых могут выступать определенное недовольство своей жизненной ситуацией, а именно материальный интерес или простое развлечение с самоутверждением своих способностей, как у хакеров.

**Преднамеренные угрозы можно разделить на:**

* **Пассивные угрозы** – предназначены в основном на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на нормальную работу самой системы. К пассивным угрозам можно отнести несанкционированный доступ к базам данных, прослушивание каналов связи.
* **Активные угрозы** – имеют цель нарушения нормальной работы системы, путем целенаправленного воздействия на ее компоненты. К активным угрозам можно отнести, например, вывод из строя операционной системы компьютера, разрушение ПО компьютеров, нарушение работы линий связи и т.д.

**Преднамеренные угрозы так же могут быть:**

* **Внутренние угрозы** - возникающие внутри самой управляемой организации;
* **Внешние угрозы** – возникающие из вне, как правило, обусловленные действиями конкурентов.

**К основным угрозам безопасности информации от разрушения, модификации и ознакомления с ней третьих лиц относятся:**

* утечка конфиденциальной информации;
* компрометация информации;
* ошибочное использование информационных ресурсов;
* нарушение информационного обслуживания;
* несанкционированный обмен информацией между абонентами;
* несанкционированное использование информационных ресурсов;
* незаконное использование привилегий.

**Утечка конфиденциальной информации** — это бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны или круга лиц, которым она была доверена по службе или стала известна в процессе работы.

# **Средства опознания и разграничения доступа к информации**

**Идентификация** – это присвоение тому или иному объекту или субъекту уникального имени или образа.

**Аутентификация** – это установление подлинности объекта или субъекта, т. е. проверка, является ли объект (субъект) тем, за кого он себя выдает.

Конечная цель процедур идентификации и аутентификации объекта (субъекта) заключается в допуске его к информации ограниченного пользования в случае положительной проверки либо отказе в допуске при отрицательном результате проверки.

**Объекты идентификации и аутентификации включают в себя:**

* людей (пользователей, операторов);
* технические средства (мониторы, рабочие станции, абонентские пункты);
* документы (ручные, распечатки);
* магнитные носители информации;
* информацию на экране монитора.

К наиболее распространенным методам аутентификации относятся присвоение лицу или другому имени пароля и хранение его значения в вычислительной системе.

**Пароль** – этосовокупность символов, которая определяет объект (субъект).

Пароль как средство обеспечения безопасности способен использоваться для идентификации и установления подлинности терминала, с которого входит в систему пользователь, а также для обратного установления подлинности компьютера по отношению к пользователю.

С учетом важности пароля как средства повышения безопасности информации от несанкционированного использования необходимо **соблюдать следующие меры предосторожности:**

1. Не хранить пароли в вычислительной системе в незашифрованном месте;
2. Не печатать и не отображать пароли в открытом виде на терминале пользователя;
3. Не применять в качестве пароля свое имя или имена родственников, а также личную информацию (дата рождения, номер домашнего или служебного телефона, название улицы);
4. Не применять реальные слова из энциклопедии или толкового словаря;
5. Использовать длинные пароли;
6. Применять смесь символов верхнего и нижнего регистров клавиатуры;
7. Применять комбинации из двух простых слов, соединенных специальными символами (например, +, =, <);
8. Использовать несуществующие новые слова (абсурдные или даже бредового содержания);
9. Как можно чаще менять пароль.

Для идентификации пользователей могут использоваться сложные в плане технической реализации системы, которые обеспечивают **установление подлинности пользователя на основе анализа его индивидуальных параметров:**

* отпечатков пальцев;
* рисунка линий руки;
* радужной оболочки глаз;
* тембра голоса.

Наиболее широкое применение имеют физические методы идентификации, которые используют носители кодов паролей.

**Такими носителями могут быть:**

* пропуск в контрольно-пропускных системах;
* пластиковые карты с именем владельца, его кодом, подписью;
* пластиковые карточки с магнитной полосой, которая считывается специальным считывающим устройством;
* пластиковые карты, содержащие встроенную микросхему;
* карты оптической памяти.

Одним из наиболее интенсивно разрабатываемых направлений по обеспечению безопасности информации является идентификация и определение подлинности документов на основе электронной цифровой подписи. При передаче информации по каналам связи используется факсимильная аппаратура, но при этом к получателю приходит не подлинник, а только копия документа с копией подписи, которая в процессе передачи может быть подвергнута повторному копированию для использования ложного документа.

**Электронная цифровая подпись** представляет собой способ шифрования с использованием криптографического преобразования и является паролем, зависящим от отправителя, получателя и содержания передаваемого сообщения.

**Существует несколько схем построения цифровой подписи:**

1. На основе алгоритмов **симметричного шифрования**.

Данная схема предусматривает **наличие в системе третьего лица — арбитра**, пользующегося доверием обеих сторон. Авторизацией документа является сам факт его шифрования секретным ключом, и передача его арбитру.

1. На основе алгоритмов **асимметричного шифрования**.

На данный момент такие схемы ЭП наиболее распространены и находят широкое применение.

Кроме этого, существуют другие разновидности цифровых подписей (групповая подпись, неоспоримая подпись, доверенная подпись), которые являются модификациями описанных выше схем. Их появление обусловлено разнообразием задач, решаемых с помощью ЭП.

Для того чтобы предупредить повторное использование подписи, ее необходимо менять от сообщения к сообщению.

В методах цифровой подписи часто используются алгоритмы шифрования с открытым ключом, но несколько иначе, чем обычно, а именно: закрытый ключ применяется для шифрования, а открытый — для дешифрования.

Наличие цифровой подписи свидетельствует о том, что ее владелец подтвердил подлинность содержимого переданного сообщения.

**Цифровой сертификат** — это сообщение, подписанное полномочным органом сертификации, который подтверждает, что открытый ключ действительно относится к владельцу подписи и может быть использован для дешифрования.

# **Криптографический метод защиты информации**

Наиболее эффективным средством повышения безопасности является **криптографическое преобразование. Для того чтобы повысить безопасность, осуществляется одно из следующих действий:**

* передача данных в компьютерных сетях;
* передача данных, которые хранятся в удаленных устройствах памяти;
* передача информации при обмене между удаленными объектами.

Защита информации методом криптографического преобразования состоит в приведении ее к неявному виду через преобразование составных частей информации (букв, цифр, слогов, слов) с применением специальных алгоритмов либо аппаратных средств и кодов ключей.

**Ключ** является изменяемой частью криптографической системы, хранящейся в тайне и определяющей, какое шифрующее преобразование из возможных выполняется в данном случае.

Для изменения (шифрования) используется некоторый алгоритм или устройство, реализующее заданный алгоритм. Алгоритмы могут быть известны широкому кругу лиц. Управление процессом шифрования происходит с помощью периодически меняющегося кода ключа, который обеспечивает каждый раз оригинальное представление информации в случае применения одного и того же алгоритма или устройства. При известном ключе можно относительно быстро, просто и надежно расшифровать текст. Без знания ключа эта процедура может стать практически невыполнимой даже при использовании компьютера.

**Методы, предназначенные для защитных преобразований, подразделяют на четыре основные группы:** перестановки, замены (подстановки), аддитивные и комбинированные методы.

Методы перестановки и замены (подстановки) характеризуются коротким ключей, а надежность защиты определяется сложностью алгоритмов преобразования. Для аддитивных методов, наоборот, свойственны простые алгоритмы и длинные ключи. Комбинированные методы являются более надежными. Они чаще всего сочетают в себе достоинства используемых компонентов.

Упомянутые четыре метода криптографического преобразования относятся к методам симметричного шифрования. Один ключ используется и для шифрования, и для дешифрования.

**Основными методами криптографического преобразования являются методы перестановки и замены.**

Основа метода перестановки состоит в разбиении исходного текста на блоки, а затем в записи этих блоков и чтении шифрованного текста по разным путям геометрической фигуры.

Шифрование методом замены заключается в том, что символы исходного текста (блока), записанные в одном алфавите, заменяются символами другого алфавита в соответствии с используемым ключом преобразования.

Комбинация этих методов привела к образованию метода производного шифра, который обладает сильными криптографическими возможностями. Алгоритм метода реализуется как аппаратно, так и программно, но рассчитан на реализацию с помощью электронных устройств специального назначения, что позволяет достичь высокой производительности и упрощенной организации обработки информации.

# **Компьютерные вирусы**

**Компьютерный вирус** – это специально написанная программа, способная самопроизвольно присоединяться к другим программам (заражать их), создавать свои копии и внедрять их в файлы, системные области компьютера и другие объединенные с ним компьютеры в целях нарушения нормальной работы программ, порчи файлов и каталогов, а также создания разных помех при работе на компьютере.

**Основными путями заражения компьютеров вирусами обычно служат съемные диски (дискеты и CD-ROM) и компьютерные сети.**

**По тому, какой вид среды обитания имеют вирусы, их классифицируют на:**

* **загрузочные** (внедряются в загрузочный сектор диска или в сектор, который содержит программу загрузки системного диска);
* **файловые** (помещаются в основном в исполняемых файлах с расширением СОМ и ЕХЕ);
* **системные** (внедряются в системные модули и драйверы периферийных устройств, таблицы размещения файлов и таблицы разделов);
* **сетевые** (находятся в компьютерных сетях);
* **файлово – загрузочные** (заражают загрузочные секторы дисков и файлы прикладных программ).

**По пути заражения среды обитания вирусы разделяются на:**

* **резидентные (**при заражении компьютера оставляют в ОП свою резидентную часть, которая после заражения перехватывает обращение ОС к другим объектам заражения, внедряется в них и выполняет свои разрушительные действия, которые могут привести к выключению или перезагрузке компьютера);
* **нерезидентные** (не заражают ОП компьютера и проявляют активность ограниченное время)

**Логическая бомба** является программой, которая встраивается в большой программный комплекс. Она безвредна до наступления определенного события, после которого реализуется ее логический механизм. **Программы-мутанты**, самовоспроизводясь, создают копии, явно отличающиеся от оригинала. **Вирусы-невидимки**, или **стелс-вирусы**, перехватывают обращения ОС к пораженным файлам и секторам дисков и подставляют вместо себя незараженные объекты. Эти вирусы при обращении к файлам применяют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы. **Макровирусы** используют возможности макроязыков, которые встроены в офисные программы обработки данных (текстовые редакторы, электронные таблицы).

**По степени воздействия на ресурсы компьютерных систем и сетей, или по деструктивным возможностям, выделяют:**

* **безвредные** (не оказывают влияния на работу компьютера);
* **неопасные** (не разрушают файлы, однако уменьшают свободную дисковую память, выводят на экран графические эффекты);
* **опасные** (вызывают значительные нарушения в работе компьютера);
* **разрушительные вирусы** (могут привести к стиранию информации, полному или частичному нарушению работы прикладных программ).

Важно иметь в виду, что любой файл, способный к загрузке и выполнению кода программы, является потенциальным местом, где может помещаться вирус.

# **Антивирусные программы**

Широкое распространение компьютерных вирусов **привело к разработке антивирусных программ**, которые позволяют обнаруживать и уничтожать вирусы, «лечить» пораженные ресурсы. Основой работы большинства антивирусных программ является принцип поиска сигнатуры вирусов.

**Вирусной сигнатурой** называют некоторую уникальную характеристику вирусной программы, выдающую присутствие вируса в компьютерной системе.

Чаще всего в антивирусные программы включается периодически обновляемая база данных сигнатур вирусов. Антивирусная программа изучает и анализирует компьютерную систему, а также проводит сравнение, отыскивая соответствие с сигнатурами в базе данных. Если программа находит соответствие, она старается вычистить обнаруженный вирус.

**По способу работы антивирусные программы можно разделить на:**

* **Фильтры**

Это «сторожа», которые постоянно находятся в ОП. Они являются резидентными и перехватывают все запросы к ОС на выполнение подозрительных действий, т. е. операций, которые используют вирусы для своего размножения и порчи информационных и программных ресурсов в компьютере, в том числе для переформатирования жесткого диска. Постоянное нахождение программ - «сторожей» в ОП существенно уменьшает ее объем, что является основным недостатком этих программ. К тому же программы-фильтры не способны «лечить» файлы или диски.

* **Ревизоры**

Они запоминают исходное состояние программ, каталогов и системных областей диска при условии, что компьютер еще не был заражен вирусом. Впоследствии программа периодически сравнивает текущее состояние с исходным. При обнаружении несоответствий (по длине файла, дате модификации, коду циклического контроля файла) сообщение об этом появляется на экране компьютера. **Среди программ-ревизоров можно выделить программу Adinf и дополнение к ней в виде Adinf cure Module.**

* **Доктора**

Способны не только обнаруживать, но и «лечить» зараженные программы или диски. При этом она уничтожает зараженные программы тела вируса. **Программы данного типа можно разделить на:**

* + **Фаги** – это программы, с помощью которых отыскиваются вирусы определенного вида.
  + **Полифаги** предназначены для обнаружения и уничтожения большого числа разнообразных вирусов. В нашей стране наиболее часто используются такие полифаги, как MS Antivirus, Aidstest, Doctor Web.
* **Детекторы** (способны обнаруживать файлы, зараженные одним или несколькими известными разработчикам программ вирусами);
* **Вакцины**

Они модифицируют программы и диски так, что это не отражается на их работе. Однако вирус, от которого производится вакцинация, считает их уже зараженными и не внедряется в них.

В настоящий момент разработано множество антивирусных программ, получивших широкое признание и постоянно пополняющихся новыми средствами для борьбы с вирусами.

# **Заключение**

Нужно четко представлять себе, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в любой организации. В то же время можно существенно уменьшить риск потерь при комплексном подходе к вопросам безопасности. Средства защиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока специалистами не произведен соответствующий анализ. Анализ должен дать объективную оценку многих факторов (подверженность появлению нарушения работы, вероятность появления нарушения работы, ущерб от коммерческих потерь и др.) и предоставить информацию для определения подходящих средств защиты – административных, аппаратных, программных и прочих.

Однако обеспечение безопасности информации - дорогое дело. Большая концентрация защитных средств в информационной системе может привести не только к тому, что система окажется очень дорогостоящей и потому нерентабельной, и неконкурентоспособной, но и к тому, что у нее произойдет существенное снижение коэффициента готовности. Например, если такие ресурсы системы, как время центрального процессора будут постоянно тратиться на работу антивирусных программ, шифрование, резервное архивирование, протоколирование и тому подобное, скорость работы пользователей в такой системе может упасть до нуля.

Так же стоит большое внимание уделять и внутренним угрозам. Даже самый честный и преданный сотрудник может оказаться средством утечки информации.

Главное при определении мер и принципов защиты информации – это квалифицированно определить границы разумной безопасности и затрат на средства защиты с одной стороны и поддержания системы в работоспособном состоянии и приемлемого риска с другой.