**МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**КАФЕДРА ИНФОРМАЦИОННЫЕ**

**СИСТЕМЫ В ЭКОНОМИКЕ**

**РЕФЕРАТ НА ТЕМУ:**

“ПРИНЦИПЫ ЗАЩИТЫ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ”

|  |
| --- |
| **Выполнила** |
| **Студент Мухина Е.В.** |
| **Группы Э-253** |
| **Проверил Шахов А.Н.** |

**ВОЛГОГРАД, 2000г.**

**Содержание**

1. Введение 4

2. Меры информационной безопасности. 5

3. Технические меры защиты информации. 6

4. Аппаратные средства защиты. 7

4.1. защита от сбоев в электропитании 7

4.2. защита от сбоев процессоров 7

4.3. защита от сбоев устройств для хранения информации. 8

4.4. защита от утечек информации электромагнитных излучений. 8

5. Программные средства защиты информации 9

5.1. Средства архивации информации. 9

5.2. Антивирусные программы. 10

5.2.1. Классификация компьютерных вирусов 10

5.2.1.1. Резидентные вирусы 11

5.2.1.2. Нерезидентные вирусы. 11

5.2.1.3. Стелс-вирусы 11

5.2.1.4. Полиморфик-вирусы 11

5.2.1.5. Файловые вирусы 12

5.2.1.6. Загрузочные вирусы 12

5.2.1.7. Макро-вирусы 13

5.2.1.8. Сетевые вирусы 13

5.2.1.9. Троянские кони (логические бомбы или временные бомбы) 14

5.2.2. Методы обнаружения и удаления компьютерных вирусов. 14

5.2.2.1. Профилактика заражения компьютера 14

5.2.2.2. Восстановление пораженных объектов 15

5.2.2.3. Классификация антивирусных программ. 15

5.2.2.4. Сканеры 15

5.2.2.5. CRC-сканеры 16

5.2.2.6. Блокировщики 16

5.2.2.7. Иммунизаторы 17

5.2.2.8. Перспективы борьбы с вирусами. 17

5.3. Криптографические методы защиты 18

5.3.1. Требования к криптосистемам. 19

5.3.2. Симметричные криптосистемы 20

5.3.3. Системы с открытым ключом 20

5.3.4. Электронная подпись. 21

5.3.5. Управление ключами. 22

5.3.5.1. Генерация ключей. 22

5.3.5.2. Накопление ключей. 22

5.3.5.3. Распределение ключей. 23

5.3.6. Реализация криптографических методов. 23

5.4. Идентификация и аутентификация 24

5.5. Управление доступом 26

5.6. Протоколирование и аудит 26

6. Безопасность баз данных 27

6.1. Управление доступом в базах данных 28

6.2. Управление целостностью данных 28

6.3. Управление параллелизмом 28

6.4. Восстановление данных 29

6.4.1. Транзакция и восстановление 30

6.4.2. Откат и раскрутка транзакции 30

7. Защита информации при работе в сетях 31

7.1. межсетевые экраны и требования к ним. 31

7.2. Использование электронной почты 33

7.2.1. Защита от фальшивых адресов 33

7.2.2. Защита от перехвата 33

8. Заключение. 34

9. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ. 35

# Введение

В последнее время все чаще стал встречаться термин - "информационное общество". С точки зрения анализа изменения производительных сил и производственных отношений, "информационное общество" может быть определено как общество, в котором основным предметом труда большей части людей являются информация и знания, а орудием труда - информационные технологии. Информационные технологии, основанные на новейших достижениях электронно-вычислительной техники, которые получили название новых информационных технологий (НИТ), находят все большее применение в различных сферах деятельности. Новые информационные технологии создают новое информационное пространство и открывают совершенно новые, ранее неизвестные и недоступные возможности, которые коренным образом меняют представления о существовавших ранее технологиях получения и обработки информации. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Все больше и больше отраслей человеческой деятельности становятся настолько сильно пронизаны этими новыми информационными технологиями, насколько и зависимы от них. Предоставляя огромные возможности, информационные технологии, вместе с тем, несут в себе и большую опасность, создавая совершенно новую, мало изученную область для возможных угроз, реализация которых может приводить к непредсказуемым и даже катастрофическим последствиям. Все увеличивается число компьютерных преступлений, что может привести в конечном счете к подрыву экономики. Сбой в информационных технологиях применяемых в управлении атомными станциями или химическими предприятиями может привести к экологическим катастрофам. И поэтому должно быть ясно, что информация - это ресурс, который надо защищать. Ущерб от возможной реализации угроз можно свести к минимуму, только приняв меры, которые способствуют обеспечению информации. Под угрозой безопасности понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети, включая хранимую, обрабатываемую информацию, а также программные и аппаратные средства.

Угрозы подразделяются на случайные (непреднамеренные) и умышленные. Источником первых могут быть ошибочные действия пользователей, выход из строя аппаратных средств и другие.

Умышленные угрозы подразделяются на пассивные и активные. Пассивные угрозы не разрушают информационные ресурсы. Их задача - несанкционированно получить информацию. Активные угрозы преследуют цель нарушать нормальный процесс функционирования систем обработки информации, путем разрушения или радиоэлектронного подавления линий, сетей, вывода из строя компьютеров, искажения баз данных и т.д. Источниками активных угроз могут быть непосредственные действия физических лиц, программные вирусы и т.д.

# Меры информационной безопасности.

Информационная безопасность подчеркивает важность информации в современном обществе - понимание того, что информация - это ценный ресурс, нечто большее, чем отдельные элементы данных. Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода. Целью информационной безопасности является обезопасить ценности системы, защитить и гарантировать точность и целостность информации, и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, к ней обеспечивается доступ или она распространяется

Можно выделить следующие направления мер информационной безопасности.

1. правовые
2. организационные
3. технические

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашение

К организационным мерам отнесу охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра, после выхода его из строя, организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.

К техническим мерам можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое. Более подробно эти меры будут рассмотрены в последующих разделах этого реферата.

# Технические меры защиты информации.

Можно так классифицировать потенциальные угрозы, против которых направлены технические меры защиты информации:

1. Потери информации из-за сбоев оборудования:

1. перебои электропитания;
2. сбои дисковых систем;
3. сбои работы серверов, рабочих станций, сетевых карт и т.д.

2. Потери информации из-за некорректной работы программ:

1. потеря или изменение данных при ошибках ПО;
2. потери при заражении системы компьютерными вирусами;

3. Потери, связанные с несанкционированным доступом:

1. несанкционированное копирование, уничтожение или подделка информации;
2. ознакомление с конфиденциальной информацией

4. Ошибки обслуживающего персонала и пользователей:

1. случайное уничтожение или изменение данных;
2. некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных

Сами технические меры защиты можно разделить на:

:

- средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания, и т.д.

- программные средства защиты, в том числе: криптография, антивирусные программы, системы разграничения полномочий, средства контроля доступа и т.д..

- административные меры защиты, включающие подготовку и обучение персонала, организацию тестирования и приема в эксплуатацию программ, контроль доступа в помещения и т.д.

Следует отметить, что подобное деление достаточно условно, поскольку современные технологии развиваются в направлении сочетания программных и аппаратных средств защиты. Наибольшее распространение такие программно-аппаратные средства получили, в частности, в области контроля доступа, защиты от вирусов и т.д..

# Аппаратные средства защиты.

Под аппаратными средствами защиты понимаются специальные средства, непосредственно входящие в состав технического обеспечения и выполняющие функции защиты как самостоятельно, так и в комплексе с другими средствами, например с программными. Можно выделить некоторые наиболее важные элементы аппаратной защиты:

1. защита от сбоев в электропитании;
2. защита от сбоев серверов, рабочих станций и локальных компьютеров;
3. защита от сбоев устройств для хранения информации;
4. защита от утечек информации электромагнитных излучений.

Рассмотрю их подробнее.

## защита от сбоев в электропитании

Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии в настоящее время является установка источников бесперебойного питания (UPS). Различные по своим техническим и потребительским характеристикам, подобные устройства могут обеспечить питание всей локальной сети или отдельной компьютера в течение какого-то промежутка времени, достаточного для восстановления подачи напряжения или для сохранения информации на магнитные носители. В противном случае используется следующая функция подобных устройств – компьютер получает сигнал, что UPS перешел на работу от собственных аккумуляторов и время такой автономной работы ограничено. Тогда компьютер выполняет действия по корректному завершению всех выполняющихся программ и отключается (команда SHUTDOWN). Большинство источников бесперебойного питания одновременно выполняет функции и стабилизатора напряжения, является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства - серверы, концентраторы, мосты и т.д. - оснащены собственными дублированными системами электропитания.

Крупные организации имеют собственные аварийные электрогенераторы или резервные линии электропитания. Эти линии подключены к разным подстанциям, и при выходе из строя одной них электроснабжение осуществляется с резервной подстанции.

## защита от сбоев процессоров

Один из методов такой защиты - это резервирование особо важных компьютерных подсистем. Пример – симметричное мультипроцессирование. В системе используется более двух процессоров, и в случае сбоя одного из них, второй продолжает работу так, что пользователи вычислительной системы даже ничего не замечают. Естественно на такую защиту требуется гораздо больше средств.

## защита от сбоев устройств для хранения информации.

Организация надежной и эффективной системы резервного копирования и дублирования данных является одной из важнейших задач по обеспечению сохранности информации. В небольших сетях, где установлены один-два сервера, чаще всего применяется установка системы резервного копирования непосредственно в свободные слоты серверов. Это могут быть устройства записи на магнитные ленты (стример), на компакт-диски многоразового использования, на оптические диски и т.д. В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер. Специалисты рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании, на случай пожара или стихийного бедствия. В некоторых случаях, когда подобные сбои и потеря информации могут привести к неприемлемой остановке работы - применяются система зеркальных винчестеров. Резервная копия информации формируется в реальном времени, то есть в любой момент времени при выходе из строя одного винчестера система сразу же начинает работать с другим.

В месте с тем, кроме аппаратных средств резервного копирования данных существуют и чисто программные средства архивации, о которых будет упомянуто в последующих разделах реферата.

## защита от утечек информации электромагнитных излучений.

Прохождение электрических сигналов по цепям ПК и соединительным кабелям сопровождается возникновением побочных электромагнитных излучений (ПЭМИ) в окружающей среде. Распространение побочных электромагнитных излучений за пределы контролируемой территории на десятки, сотни, а иногда и тысячи метров, создает предпосылки для утечки информации, так как возможен ее перехват с помощью специальных технических средств контроля. В персональном компьютере кроме проводных линий связи также основными источниками электромагнитных излучений являются мониторы, принтеры, накопители на магнитных дисках, а также центральный процессор. Исследования показывают, что излучение видеосигнала монитора является достаточно мощным, широкополосным и охватывает диапазон метровых и дециметровых волн. Для уменьшения уровня побочных электромагнитных излучений применяют специальные средства защиты информации: экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений и наводок при помощи различных резистивных и поглощающих согласованных нагрузок.

При контроле защиты информации ПК используются специально разработанные тестовые программы, а также специальная аппаратура контроля уровня излучения, которые определяют режим работы ПК, обеспечивающий совместно с другими техническими средствами скрытый режим работы для различных средств разведки.

# Программные средства защиты информации

Программными называются средства защиты данных, функционирующие в составе программного обеспечения. Среди них можно выделить и подробнее рассмотреть следующие;

1. средства архивации данных
2. антивирусные программы
3. криптографические средства
4. средства идентификации и аутентификации пользователей
5. средства управления доступом
6. протоколирование и аудит

Как примеры комбинаций вышеперечисленных мер можно привести:

1. защиту баз данных
2. защиту информации при работе в компьютерных сетях.

## Средства архивации информации.

Иногда резервные копии информации приходится выполнять при общей ограниченности ресурсов размещения данных, например владельцам персональных компьютеров. В этих случаях используют программную архивацию. Архивация это слияние нескольких файлов и даже каталогов в единый файл — архив, одновременно с сокращением общего объема исходных файлов путем устранения избыточности, но без потерь информации, т. е. с возможностью точного восстановления исходных файлов. Действие большинства средств архивации основано на использовании алгоритмов сжатия, предложенных в 80-х гг. Абрахамом Лемпелем и Якобом Зивом. Наиболее известны и популярны следующие архивные форматы;

1. ZIP, ARJ для операционных систем DOS. и Windows
2. TAR для операционной системы Unix
3. межплатформный формат JAR (Java ARchive)
4. RAR (все время растет популярность этого нового формата, так как разработаны программы позволяющие использовать его в операционных системах DOS, Windows и Unix),

Пользователю следует лишь выбрать для себя подходящую программу, обеспечивающую работу с выбранным форматом, путем оценки ее характеристик – быстродействия, степени сжатия, совместимости с большим количеством форматов, удобности интерфейса, выбора операционной системы и т.д.. Список таких программ очень велик – PKZIP, PKUNZIP, ARJ, RAR, WinZip, WinArj, ZipMagic, WinRar и много других. Большинство из этих программ не надо специально покупать, так как они предлагаются как программы условно-бесплатные (Shareware) или свободного распространения (Freeware). Также очень важно установить постоянный график проведения таких работ по архивации данных или выполнять их после большого обновления данных.

## Антивирусные программы.

Это программы разработанные для защиты информации от вирусов. Неискушенные пользователи обычно считают, что компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять нежелательные различные действия на компьютере. Специалисты по компьютерной вирусологии определяют, что ОБЯЗАТЕЛЬНЫМ (НЕОБХОДИМЫМ) СВОЙСТВОМ КОМПЬЮТЕРНОГО ВИРУСА является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению. Следует отметить, что это условие не является достаточным т.е. окончательным. Вот почему точного определения вируса нет до сих пор, и вряд ли оно появится в обозримом будущем. Следовательно, нет точно определенного закона, по которому «хорошие» файлы можно отличить от «вирусов». Более того, иногда даже для конкретного файла довольно сложно определить, является он вирусом или нет.

### Классификация компьютерных вирусов

Вирусы можно разделить на классы по следующим основным признакам:

1. деструктивные возможности
2. особенности алгоритма работы;
3. среда обитания;

По ДЕСТРУКТИВНЫМ ВОЗМОЖНОСТЯМ вирусы можно разделить на:

1. безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
2. неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами;
3. опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
4. очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти

ОСОБЕННОСТИ АЛГОРИТМА РАБОТЫ вирусов можно охарактеризовать следующими свойствами:

1. резидентность;
2. использование стелс-алгоритмов;
3. самошифрование и полиморфичность;

#### Резидентные вирусы

Под термином "резидентность" (DOS'овский термин TSR - Terminate and Stay Resident) понимается способность вирусов оставлять свои копии в системной памяти, перехватывать некоторые события (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов). Таким образом, резидентные вирусы активны не только в момент работы зараженной программы, но и после того, как программа закончила свою работу. Резидентные копии таких вирусов остаются жизнеспособными вплоть до очередной перезагрузки, даже если на диске уничтожены все зараженные файлы. Часто от таких вирусов невозможно избавиться восстановлением всек копий файлов с дистрибутивных дисков или backup-копий. Резидентная копия вируса остается активной и заражает вновь создаваемые файлы. То же верно и для загрузочных вирусов — форматирование диска при наличии в памяти резидентного вируса не всегда вылечивает диск, поскольку многие резидентные вирусы заражает диск повторно после того, как он отформатирован.

#### Нерезидентные вирусы.

Нерезидентные вирусы, напротив, активны довольно непродолжительное время — только в момент запуска зараженной программы. Для своего распространения они ищут на диске незараженные файлы и записываются в них. После того, как код вируса передает управление программе-носителю, влияние вируса на работу операционной системы сводится к нулю вплоть до очередного запуска какой-либо зараженной программы. Поэтому файлы, зараженные нерезидентными вирусами значительно проще удалить с диска и при этом не позволить вирусу заразить их повторно.

#### Стелс-вирусы

Стелс-вирусы теми или иными способами скрывают факт своего присутствия в системе..

Использование СТЕЛС-алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов OC на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. В случае макро-вирусов наиболее популярный способ — запрет вызовов меню просмотра макросов. Известны стелс-вирусы всех типов, за исключением Windows-вирусов — загрузочные вирусы, файловые DOS-вирусы и даже макро-вирусы. Появление стелс-вирусов, заражающих файлы Windows, является скорее всего делом времени

#### Полиморфик-вирусы

САМОШИФРОВАНИЕ и ПОЛИМОРФИЧНОСТЬ используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфик - вирусы (polymorphic) - это достаточно трудно обнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

К полиморфик-вирусам относятся те из них, детектирование которых невозможно (или крайне затруднительно) осуществить при помощи так называемых вирусных масок - участков постоянного кода, специфичных для конкретного вируса. Достигается это двумя основными способами - шифрованием основного кода вируса с непостоянным ключем и случаным набором команд расшифровщика или изменением самого выполняемого кода вируса. Полиморфизм различной степени сложности встречается в вирусах всех типов - от загрузочных и файловых DOS-вирусов до Windows-вирусов.

По СРЕДЕ ОБИТАНИЯ вирусы можно разделить на:

1. файловые;
2. загрузочные;
3. макровирусы;
4. сетевые.

#### Файловые вирусы

Файловые вирусы либо различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Внедрение файлового вируса возможно практически во все исполняемые файлы всех популярных ОС. На сегодняшний день известны вирусы, поражающие все типы выполняемых объектов стандартной DOS: командные файлы (BAT), загружаемые драйверы (SYS, в том числе специальные файлы IO.SYS и MSDOS.SYS) и выполняемые двоичные файлы (EXE, COM). Существуют вирусы, поражающие исполняемые файлы других операционных систем - Windows 3.x, Windows95/NT, OS/2, Macintosh, UNIX, включая VxD-драйвера Windows 3.x и Windows95.

Существуют вирусы, заражающие файлы, которые содержат исходные тексты программ, библиотечные или объектные модули. Возможна запись вируса и в файлы данных, но это случается либо в результате ошибки вируса, либо при проявлении его агрессивных свойств. Макро-вирусы также записывают свой код в файлы данных - документы или электронные таблицы, - однако эти вирусы настолько специфичны, что вынесены в отдельную группу.

#### Загрузочные вирусы

Загрузочные вирусы заражают загрузочный (boot) сектор флоппи-диска и boot-сектор или Master Boot Record (MBR) винчестера. Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера - после необходимых тестов установленного оборудования (памяти, дисков и т.д.) программа системной загрузки считывает первый физический сектор загрузочного диска (A:, C: или CD-ROM в зависимости от параметров, установленных в BIOS Setup) и передает на него управление.

В случае дискеты или компакт-диска управление получает boot-сектор, который анализирует таблицу параметров диска (BPB - BIOS Parameter Block) высчитывает адреса системных файлов операционной системы, считывает их в память и запускает на выполнение. Системными файлами обычно являются MSDOS.SYS и IO.SYS, либо IBMDOS.COM и IBMBIO.COM, либо других в зависимости от установленной версии DOS, Windows или других операционных систем. Если же на загрузочном диске отсутствуют файлы операционной системы, программа, расположенная в boot-секторе диска выдает сообщение об ошибке и предлагает заменить загрузочный диск.

В случае винчестера управление получает программа, расположенная в MBR винчестера. Эта программа анализирует таблицу разбиения диска (Disk Partition Table), вычисляет адрес активного boot-сектора (обычно этим сектором является boot-сектор диска C:), загружает его в память и передает на него управление. Получив управление, активный boot-сектор винчестера проделывает те же действия, что и boot-сектор дискеты.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, одинаков во всех описанных выше способах: вирус "заставляет" систему при ее перезапуске считать в память и отдать управление не оригинальному коду загрузчика, но коду вируса.

Заражение дискет производится единственным известным способом — вирус записывает свой код вместо оригинального кода boot-сектора дискеты. Винчестер заражается тремя возможными способами - вирус записывается либо вместо кода MBR, либо вместо кода boot-сектора загрузочного диска (обычно диска C:), либо модифицирует адрес активного boot-сектора в Disk Partition Table, расположенной в MBR винчестера.

#### Макро-вирусы

Макро-вирусы заражают файлы-документы и электронные таблицы нескольких популярных редакторов. Макро-вирусы (macro viruses) являются программами на языках (макро-языках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие. Наибольшее распространение получили макро-вирусы для Microsoft Word, Excel и Office97. Существуют также макро-вирусы, заражающие документы Ami Pro и базы данных Microsoft Access.

#### Сетевые вирусы

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла. Пример сетевых вирусов – так называемые IRC-черви.

IRC (Internet Relay Chat) — это специальный протокол, разработанный для коммуникации пользователей Интернет в реальном времени. Этот протокол предоставляет им возможность Итрернет-"разговора" при помощи специально разработанного программного обеспечения. Помимо посещения общих конференций пользователи IRC имеют возможность общаться один-на-один с любым другим пользователем. Кроме этого существует довольно большое количество IRC-команд, при помощи которых пользователь может получить информацию о других пользователях и каналах, изменять некоторые установки IRC-клиента и прочее. Существует также возможность передавать и принимать файлы - именно на этой возможности и базируются IRC-черви. Как оказалось, мощная и разветвленная система команд IRC-клиентов позволяет на основе их скриптов создавать компьютерные вирусы, передающие свой код на компьютеры пользователей сетей IRC, так называемые "IRC-черви". Принцип действия таких IRC-червей примерно одинаков. При помощи IRC-команд файл сценария работы (скрипт) автоматически посылается с зараженного компьютера каждому вновь присоединившемуся к каналу пользователю. Присланный файл-сценарий замещает стандартный и при следующем сеансе работы уже вновь зараженный клиент будет рассылать червя. Некоторые IRC-черви также содержат троянский компонент: по заданным ключевым словам производят разрушительные действия на пораженных компьютерах. Например, червь "pIRCH.Events" по определенной команде стирает все файлы на диске пользователя.

Существует большое количество сочетаний - например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс и полиморфик-технологии. Другой пример такого сочетания - сетевой макро-вирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

В дополнение к этой классификации следует сказать несколько слов о других вредоносных программах, которые иногда путают с вирусами. Эти программы не обладают способностью к самораспространению как вирусы, но способны нанести столь же разрушительный урон.

#### Троянские кони (логические бомбы или временные бомбы)

К троянским коням относятся программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от каких-либо условий или при каждом запуске уничтожающая информацию на дисках, "завешивающая" систему, и т.п. В качестве примера можно привести и такой случай – когда такая программа во время сеанса работы в Интернете пересылала своему автору идентификаторы и пароли с компьютеров, где она обитала. Большинство известных троянских коней являются программами, которые "подделываются" под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по BBS-станциям или электронным конференциям. По сравнению с вирусами "троянские кони" не получают широкого распространения по достаточно простым причинам - они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем.

### Методы обнаружения и удаления компьютерных вирусов.

Способы противодействия компьютерным вирусам можно разделить на несколько групп: профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения; методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса; способы обнаружения и удаления неизвестного вируса.

1. Профилактика заражения компьютера
2. Восстановление пораженных объектов
3. Антивирусные программы

#### Профилактика заражения компьютера

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение небольшого числа правил, которое позволяет значительно снизить вероятность заражения вирусом и потери каких-либо данных.

Для того чтобы определить основные правила компьютерной гигиены, необходимо выяснить основные пути проникновения вируса в компьютер и компьютерные сети.

Основным источником вирусов на сегодняшний день является глобальная сеть Internet. Наибольшее число заражений вирусом происходит при обмене письмами в форматах Word/Office97. Пользователь зараженного макро-вирусом редактора, сам того не подозревая, рассылает зараженные письма адресатам, которые в свою очередь отправляют новые зараженные письма и т.д. Выводы – следует избегать контактов с подозрительными источниками информации и пользоваться только законными (лицензионными) программными продуктами. К сожалению в нашей стране это не всегда возможно.

#### Восстановление пораженных объектов

В большинстве случаев заражения вирусом процедура восстановления зараженных файлов и дисков сводится к запуску подходящего антивируса, способного обезвредить систему. Если же вирус неизвестен ни одному антивирусу, то достаточно отослать зараженный файл фирмам-производителям антивирусов и через некоторое время (обычно — несколько дней или недель) получить лекарство-«апдейт» против вируса. Если же время не ждет, то обезвреживание вируса придется произвести самостоятельно. Для большинства пользователей необходимо иметь резервные копии своей информации.

#### Классификация антивирусных программ.

Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы. Однако сразу хотелось бы отметить, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, и заявления о существовании таких систем можно расценить как либо недобросовестную рекламу, либо непрофессионализм. Таких систем не существует, поскольку на любой алгоритм антивируса всегда можно предложить контр-алгоритм вируса, невидимого для этого антивируса (обратное, к счастью, тоже верно: на любой алгоритм вируса всегда можно создать антивирус).

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры (другие названия: фаг, полифаг, программа-доктор). Следом за ними по эффективности и популярности следуют CRC-сканеры (также: ревизор, checksumer, integrity checker). Часто оба приведенных метода объединяются в одну универсальную антивирусную программу, что значительно повышает ее мощность. Применяются также различного типа блокировщики и иммунизаторы.

#### Сканеры

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые «маски». Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски, или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода являетcя алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфик - вирусов. Сканеры также можно разделить на две категории — «универсальные» и «специализированные». Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макро-вирусов. Специализированные сканеры, рассчитанные только на макро-вирусы, часто оказываются наиболее удобным и надежным решением для защиты систем документооборота в средах MS Word и MS Excel.

Сканеры также делятся на «резидентные» (мониторы, сторожа), производящие сканирование «на-лету», и «нерезидентные», обеспечивающие проверку системы только по запросу. Как правило, «резидентные» сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как «нерезидентный» сканер способен опознать вирус только во время своего очередного запуска. С другой стороны резидентный сканер может несколько замедлить работу компьютера в том числе и из-за возможных ложных срабатываний.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам —относительно небольшую скорость поиска вирусов. Наиболее распространены в России следующие программы: AVP - Касперского, Dr.Weber – Данилова, Norton Antivirus

фирмы Semantic.

#### CRC-сканеры

Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом. CRC-сканеры, использующие анти-стелс алгоритмы, являются довольно сильным оружием против вирусов: практически 100% вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у этого типа антивирусов есть врожденный недостаток, который заметно снижает их эффективность. Этот недостаток состоит в том, что CRC-сканеры не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время, уже после того, как вирус разошелся по компьютеру. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах. Более того, периодически появляются вирусы, которые используют эту «слабость» CRC-сканеров, заражают только вновь создаваемые файлы и остаются, таким образом, невидимыми для них. Наиболее используемые в России программы подобного рода- ADINF и AVP Inspector.

#### Блокировщики

Антивирусные блокировщики — это резидентные программы, перехватывающие «вирусо-опасные» ситуации и сообщающие об этом пользователю. К «вирусо-опасным» относятся вызовы на открытие для записи в выполняемые файлы, запись в boot-сектора дисков или MBR винчестера, попытки программ остаться резидентно и т.д., то есть вызовы, которые характерны для вирусов в моменты из размножения. Иногда некоторые функции блокировщиков реализованы в резидентных сканерах.

К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения, что, кстати, бывает очень полезно в случаях, когда давно известный вирус постоянно «выползает неизвестно откуда». К недостаткам относятся существование путей обхода защиты блокировщиков и большое количество ложных срабатываний, что, видимо, и послужило причиной для практически полного отказа пользователей от подобного рода антивирусных программ (например, неизвестно ни об одном блокировщике для Windows95/NT — нет спроса, нет и предложения).

Необходимо также отметить такое направление антивирусных средств, как антивирусные блокировщики, выполненные в виде аппаратных компонентов компьютера («железа»). Наиболее распространенной является встроенная в BIOS защита от записи в MBR винчестера. Однако, как и в случае с программными блокировщиками, такую защиту легко обойти прямой записью в порты контроллера диска, а запуск DOS-утилиты FDISK немедленно вызывает «ложное срабатывание» защиты.

Существует несколько более универсальных аппаратных блокировщиков, но к перечисленным выше недостаткам добавляются также проблемы совместимости со стандартными конфигурациями компьютеров и сложности при их установке и настройке. Все это делает аппаратные блокировщики крайне непопулярными на фоне остальных типов антивирусной защиты.

#### Иммунизаторы

Иммунизаторы - это программы записывающие в другие программы коды, сообщающие о заражении. Они обычно записывают эти коды в конец файлов (по принципу файлового вируса) и при запуске файла каждый раз проверяют его на изменение. Недостаток у них всего один, но он летален: абсолютная неспособность сообщить о заражении стелс-вирусом. Поэтому такие иммунизаторы, как и блокировщики, практически не используются в настоящее время. Кроме того многие программы, разработанные в последнее время, сами проверяют себя на целостность и могут принять внедренные в них коды за вирусы и отказаться работать.

#### Перспективы борьбы с вирусами.

Вирусы успешно внедрились в повседневную компьютерную жизнь и покидать ее в обозримом будущем не собираются. Так кто же пишет вирусы? Основную их массу создают студенты и школьники, которые только что изучили язык ассемблера, хотят попробовать свои силы, но не могут найти для них более достойного применения. Вторую группу составляют также молодые люди (чаще - студенты), которые еще не полностью овладели искусством программирования, но уже решили посвятить себя написанию и распространению вирусов. Единственная причина, толкающая подобных людей на написание вирусов, это комплекс неполноценности, который проявляет себя в компьютерном хулиганстве. Из-под пера подобных «умельцев» часто выходят либо многочисленные модификации «классических» вирусов, либо вирусы крайне примитивные и с большим числом ошибок. Став старше и опытнее, но так и не повзрослев, некоторые из подобных вирусописателей попадают в третью, наиболее опасную группу, которая создает и запускает в мир «профессиональные» вирусы. Однако другие профессионалы будут создавать и новые более совершенные антивирусные средства. Какой прогноз этого единоборства? Для того, чтобы ответить на этот вопрос следует определить, где и при каких условиях размножаются вирусы.

Основная питательная среда для массового распространения вируса в ЭВМ – это:

1. слабая защищенность операционной системы (ОС);
2. наличие разнообразной и довольно полной документации по OC и «железу». используемой авторами вирусов;
3. широкое распространение этой ОС и этого «железа».

Хотя следует отметить, что понятие операционной системы достаточно растяжимое. Например, для макро-вирусов операционной системой являются редакторы Word и Excel, поскольку именно редакторы, а не Windows предоставляют макро-вирусам (т.е. программам на бейсике) необходимые ресурсы и функции.

Чем больше в операционной системе присутствуют элементов защиты информации, тем труднее будет вирусу поразить объекты своего нападения, так как для этого потребуется (как минимум) взломать систему шифрования, паролей и привилегий. В результате работа, необходимая для написания вируса, окажется по силам только профессионалам высокого уровня. А у профессионалов, как представляется, уровень порядочности все-таки намного выше, чем в среде потребителей их продукции, и, следовательно, число созданных и запущенных в большую жизнь вирусов будет сокращаться. Пример этому – новая операционная система Windows 2000 с модифицированной файловой системой NTFS. (Уже ближайшее будущее даст оценку усилиям разработчиков создать операционную систему с высокой степенью защищенности).

## Криптографические методы защиты

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии - ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.

Криптографические методы защиты информации - это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования. Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи носителя). Данный метод защиты реализуется в виде программ или пакетов программ

Современная криптография включает в себя четыре крупных раздела:

.

1. Симметричные криптосистемы. В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ. (Шифрование - преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом, дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный)
2. Криптосистемы с открытым ключом. В системах с открытым ключом используются два ключа - открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.( Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.)
3. Электронная подпись. Системой электронной подписи. называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.
4. Управление ключами. Это процесс системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Основные направления использования криптографических методов - передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

### Требования к криптосистемам.

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

1. зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
2. число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;
3. число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);
4. знание алгоритма шифрования не должно влиять на надежность защиты;
5. незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
6. структурные элементы алгоритма шифрования должны быть неизменными;
7. дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;
8. длина шифрованного текста должна быть равной длине исходного текста;
9. не должно быть простых и легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;
10. любой ключ из множества возможных должен обеспечивать надежную защиту информации;
11. алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

### Симметричные криптосистемы

Все многообразие существующих криптографических методов в симметричных криптосистемах можно свести к следующим 4 классам преобразований:

1. подстановка - символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее определенным правилом;
2. перестановка - символы шифруемого текста переставляются по некоторому правилу в пределах заданного блока передаваемого текста;
3. аналитическое преобразование - шифруемый текст преобразуется по некоторому аналитическому правилу, например гаммирование - заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа ;
4. комбинированное преобразование - представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста. Блочные шифры на практике встречаются чаще, чем “чистые” преобразования того или иного класса в силу их более высокой криптостойкости. Российский и американский стандарты шифрования основаны именно на этом классе .

### Системы с открытым ключом

Как бы ни были сложны и надежны криптографические системы - их слабое мест при практической реализации - проблема распределения ключей. Для того, чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС, ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому. Т.е. в общем случае для передачи ключа опять же требуется использование какой-то криптосистемы. Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены системы с открытым ключом. Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне. Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Дешифрование сообщения возможно только с использованием закрытого ключа, который известен только самому адресату. Криптографические системы с открытым ключом используют так называемые необратимые или односторонние функции, которые обладают следующим свойством: при заданном значении x относительно просто вычислить значение f(x), однако если y=f(x), то нет простого пути для вычисления значения x. Множество классов необратимых функций и порождает все разнообразие систем с открытым ключом. Однако не всякая необратимая функция годится для использования в реальных ИС. В самом определении необратимости присутствует неопределенность. Под необратимостью понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение используя современные вычислительные средства за обозримый интервал времени. Поэтому чтобы гарантировать надежную защиту информации, к системам с открытым ключом (СОК) предъявляются два важных и очевидных требования:

1. Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.
2. Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне. При этом желательна точная нижняя оценка сложности (количества операций) раскрытия шифра.

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах. Так, алгоритм RSA стал мировым стандартом де-факто для открытых систем. Вообще же все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

1. Разложение больших чисел на простые множители.
2. Вычисление логарифма в конечном поле.
3. Вычисление корней алгебраических уравнений.

Здесь же следует отметить, что алгоритмы криптосистемы с открытым ключом (СОК) можно использовать в следующих назначениях:.

1. Как самостоятельные средства защиты передаваемых и хранимых данных.
2. Как средства для распределения ключей.

Алгоритмы СОК более трудоемки, чем традиционные криптосистемы. Поэтому часто на практике рационально с помощью СОК распределять ключи, объем которых как информации незначителен. А потом с помощью обычных алгоритмов осуществлять обмен большими информационными потоками. Один из наиболее распространенных - система с открытым ключом - RSA. Криптосистема RSA, разработанная в 1977 году и получила название в честь ее создателей: Рона Ривеста, Ади Шамира и Леонарда Эйдельмана. Они воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Доказано (теорема Рабина), что раскрытие шифра RSA эквивалентно такому разложению. Поэтому для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время. Возможность гарантированно оценить защищенность алгоритма RSA стала одной из причин популярности этой СОК на фоне десятков других схем. Поэтому алгоритм RSA используется в банковских компьютерных сетях, особенно для работы с удаленными клиентами (обслуживание кредитных карточек).

### Электронная подпись.

В чем состоит проблема аутентификации данных? В конце обычного письма или документа исполнитель или ответственное лицо обычно ставит свою подпись. Подобное действие обычно преследует две цели. Во-первых, получатель имеет возможность убедиться в истинности письма, сличив подпись с имеющимся у него образцом. Во-вторых, личная подпись является юридическим гарантом авторства документа. Последний аспект особенно важен при заключении разного рода торговых сделок, составлении доверенностей, обязательств и т.д. Если подделать подпись человека на бумаге весьма непросто, а установить авторство подписи современными криминалистическими методами - техническая деталь, то с подписью электронной дело обстоит иначе. Подделать цепочку битов, просто ее скопировав, или незаметно внести нелегальные исправления в документ сможет любой пользователь. С широким распространением в современном мире электронных форм документов (в том числе и конфиденциальных) и средств их обработки особо актуальной стала проблема установления подлинности и авторства безбумажной документации. В разделе криптографических систем с открытым ключом было показано, что при всех преимуществах современных систем шифрования они не позволяют обеспечить аутентификацию данных. Поэтому средства аутентификации должны использоваться в комплексе и криптографическими алгоритмами.

### Управление ключами.

Кроме выбора подходящей для конкретной ИС криптографической системы, важная проблема - управление ключами. Как бы ни была сложна и надежна сама криптосистема, она основана на использовании ключей. Если для обеспечения конфиденциального обмена информацией между двумя пользователями процесс обмена ключами тривиален, то в ИС, где количество пользователей составляет десятки и сотни управление ключами - серьезная проблема. Под ключевой информацией понимается совокупность всех действующих в ИС ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то завладев ею, злоумышленник получает неограниченный доступ ко всей информации. Управление ключами - информационный процесс, включающий в себя три элемента:

1. генерацию ключей;
2. накопление ключей;
3. распределение ключей.

Рассмотрим, как они должны быть реализованы для того, чтобы обеспечить безопасность ключевой информации в ИС.

#### Генерация ключей.

В самом начале разговора о криптографических методах было сказано, что не стоит использовать неслучайные ключи с целью легкости их запоминания. В серьезных ИС используются специальные аппаратные и программные методы генерации случайных ключей. Как правило используют датчики ПСЧ. Однако степень случайности их генерации должна быть достаточно высоким. Идеальным генераторами являются устройства на основе “натуральных” случайных процессов. Например случайным математическим объектом являются десятичные знаки иррациональных чисел, которые вычисляются с помощью стандартных математических методов.

#### Накопление ключей.

Под накоплением ключей понимается организация их хранения, учета и удаления. Поскольку ключ является самым привлекательным для злоумышленника объектом, открывающим ему путь к конфиденциальной информации, то вопросам накопления ключей следует уделять особое внимание. Секретные ключи никогда не должны записываться в явном виде на носителе, который может быть считан или скопирован. В достаточно сложной ИС один пользователь может работать с большим объемом ключевой информации, и иногда даже возникает необходимость организации мини-баз данных по ключевой информации. Такие базы данных отвечают за принятие, хранение, учет и удаление используемых ключей. Итак, каждая информация об используемых ключах должна храниться в зашифрованном виде. Ключи, зашифровывающие ключевую информацию называются мастер-ключами. Желательно, чтобы мастер-ключи каждый пользователь знал наизусть, и не хранил их вообще на каких-либо материальных носителях. Очень важным условием безопасности информации является периодическое обновление ключевой информации в ИС. При этом переназначаться должны как обычные ключи, так и мастер-ключи. В особо ответственных ИС обновление ключевой информации желательно делать ежедневно. Вопрос обновления ключевой информации связан и с третьим элементом управления ключами - распределением ключей.

#### Распределение ключей.

Распределение ключей - самый ответственный процесс в управлении ключами. К нему предъявляются два требования:

1. Оперативность и точность распределения
2. Скрытность распределяемых ключей.

В последнее время заметен сдвиг в сторону использования криптосистем с открытым ключом, в которых проблема распределения ключей отпадает. Тем не менее распределение ключевой информации в ИС требует новых эффективных решений. Распределение ключей между пользователями реализуются двумя разными подходами:

1. Путем создания одного ли нескольких центров распределения ключей. Недостаток такого подхода состоит в том, что в центре распределения известно, кому и какие ключи назначены и это позволяет читать все сообщения, циркулирующие в ИС. Возможные злоупотребления существенно влияют на защиту.

2. Прямой обмен ключами между пользователями информационной системы. В этом случае проблема состоит в том, чтобы надежно удостоверить подлинность субъектов. Для обмена ключами можно использовать криптосистемы с открытым ключом, используя тот же алгоритм RSA.

В качестве обобщения сказанного о распределении ключей следует сказать следующее. Задача управления ключами сводится к поиску такого протокола распределения ключей, который обеспечивал бы:

1. возможность отказа от центра распределения ключей;
2. взаимное подтверждение подлинности участников сеанса;
3. подтверждение достоверности сеанса механизмом запроса-ответа, использование для этого программных или аппаратных средств;
4. использование при обмене ключами минимального числа сообщений.

### Реализация криптографических методов.

Проблема реализации методов защиты информации имеет два аспекта:

1. разработку средств, реализующих криптографические алгоритмы,
2. методику использования этих средств.

Каждый из рассмотренных криптографических методов могут быть реализованы либо программным, либо аппаратным способом. Возможность программной реализации обуславливается тем, что все методы криптографического преобразования формальны и могут быть представлены в виде конечной алгоритмической процедуры. При аппаратной реализации все процедуры шифрования и дешифрования выполняются специальными электронными схемами. Наибольшее распространение получили модули, реализующие комбинированные методы. Большинство зарубежных серийных средств шифрования основано на американском стандарте DES. Отечественные же разработки, такие как, например, устройство КРИПТОН, использует отечественный стандарт шифрования. Основным достоинством программных методов реализации защиты является их гибкость, т.е. возможность быстрого изменения алгоритмов шифрования. Основным же недостатком программной реализации является существенно меньшее быстродействие по сравнению с аппаратными средствами (примерно в 10 раз). В последнее время стали появляться комбинированные средства шифрования, так называемые программно-аппаратные средства. В этом случае в компьютере используется своеобразный “криптографический сопроцессор” - вычислительное устройство, ориентированное на выполнение криптографических операций (сложение по модулю, сдвиг и т.д.). Меняя программное обеспечения для такого устройства, можно выбирать тот или иной метод шифрования. Такой метод объединяет в себе достоинства программных и аппаратных методов.

Таким образом, выбор типа реализации криптозащиты для конкретной ИС в существенной мере зависит от ее особенностей и должен опираться на всесторонний анализ требований, предъявляемых к системе защиты информации.

## Идентификация и аутентификация

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности. Идентификация и аутентификация - это первая линия обороны, "проходная" информационного пространства организации.

Идентификация позволяет субъекту - пользователю или процессу, действующему от имени определенного пользователя, назвать себя, сообщив свое имя. Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого себя выдает. В качестве синонима слова "аутентификация" иногда используют сочетание "проверка подлинности". Субъект может подтвердить свою подлинность, если предъявит по крайней мере одну из следующих сущностей:

1. нечто, что он знает: пароль, личный идентификационный номер, криптографический ключ и т.п.,
2. нечто, чем он владеет: личную карточку или иное устройство аналогичного назначения,
3. нечто, что является частью его самого: голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики,
4. нечто, ассоциированное с ним, например координаты

Главное достоинство парольной аутентификации - простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее по совокупности характеристик их следует признать самым слабым средством проверки подлинности. Надежность паролей основывается на способности помнить их и хранить в тайне. Ввод пароля можно подсмотреть. Пароль можно угадать методом грубой силы, используя, быть может, словарь. Если файл паролей зашифрован, но доступен на чтение, его можно перекачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор.

Пароли уязвимы по отношению к электронному перехвату - это наиболее принципиальный недостаток, который нельзя компенсировать улучшением администрирования или обучением пользователей. Практически единственный выход - использование криптографии для шифрования паролей перед передачей по линиям связи.

Тем не менее, следующие меры позволяют значительно повысить надежность парольной защиты:

1. наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
2. управление сроком действия паролей, их периодическая смена;
3. ограничение доступа к файлу паролей;
4. ограничение числа неудачных попыток входа в систему, что затруднит применение метода грубой силы;
5. обучение и воспитание пользователей;
6. использование программных генераторов паролей, которые, основываясь на несложных правилах, могут порождать только благозвучные и, следовательно, запоминающиеся пароли.

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации, основанные, например, на применении токенов.

Токен - это предмет или устройство, владение которым подтверждает подлинность пользователя. Различают токены с памятью (пассивные, которые только хранят, но не обрабатывают информацию) и интеллектуальные токены (активные).

Самой распространенной разновидностью токенов с памятью являются карточки с магнитной полосой. Для использования подобных токенов необходимо устройство чтения, снабженное также клавиатурой и процессором. Обычно пользователь набирает на этой клавиатуре свой личный идентификационный номер, после чего процессор проверяет его совпадение с тем, что записано на карточке, а также подлинность самой карточки. Таким образом, здесь фактически применяется комбинация двух способов защиты, что существенно затрудняет действия злоумышленника.

Необходима обработка аутентификационной информации самим устройством чтения, без передачи в компьютер - это исключает возможность электронного перехвата.

Иногда (обычно для физического контроля доступа) карточки применяют сами по себе, без запроса личного идентификационного номера.

Как известно, одним из самых мощных средств в руках злоумышленника является изменение программы аутентификации, при котором пароли не только проверяются, но и запоминаются для последующего несанкционированного использования.

Интеллектуальные токены характеризуются наличием собственной вычислительной мощности. Они подразделяются на интеллектуальные карты, стандартизованные ISO и прочие токены. Карты нуждаются в интерфейсном устройстве, прочие токены обычно обладают ручным интерфейсом (дисплеем и клавиатурой) и по внешнему виду напоминают калькуляторы. Чтобы токен начал работать, пользователь должен ввести свой личный идентификационный номер.

По принципу действия интеллектуальные токены можно разделить на следующие категории.

1. Статический обмен паролями: пользователь обычным образом доказывает токену свою подлинность, затем токен проверяется компьютерной системой.
2. Динамическая генерация паролей: токен генерирует пароли, периодически изменяя их. Компьютерная система должна иметь синхронизированный генератор паролей. Информация от токена поступает по электронному интерфейсу или набирается пользователем на клавиатуре терминала.
3. Запросно-ответные системы: компьютер выдает случайное число, которое преобразуется криптографическим механизмом, встроенным в токен, после чего результат возвращается в компьютер для проверки. Здесь также возможно использование электронного или ручного интерфейса. В последнем случае пользователь читает запрос с экрана терминала, набирает его на клавиатуре токена (возможно, в это время вводится и личный номер), а на дисплее токена видит ответ и переносит его на клавиатуру терминала.

## Управление доступом

Средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты - пользователи и процессы могут выполнять над объектами - информацией и другими компьютерными ресурсами. Речь идет о логическом управлении доступом, который реализуется программными средствами. Логическое управление доступом - это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность путем запрещения обслуживания неавторизованных пользователей. Задача логического управления доступом состоит в том, чтобы для каждой пары (субъект, объект) определить множество допустимых операций, зависящее от некоторых дополнительных условий, и контролировать выполнение установленного порядка. Простой пример реализации таких прав доступа – какой-то пользователь (субъект) вошедший в информационную систему получил право доступа на чтение информации с какого-то диска(объект), право доступа на модификацию данных в каком-то каталоге(объект) и отсутствие всяких прав доступа к остальным ресурсам информационной системы.

Контроль прав доступа производится разными компонентами программной среды - ядром операционной системы, дополнительными средствами безопасности, системой управления базами данных, посредническим программным обеспечением (таким как монитор транзакций) и т.д.

## Протоколирование и аудит

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе. Например - кто и когда пытался входить в систему, чем завершилась эта попытка, кто и какими информациоными ресурсами пользовался, какие и кем модифицировались информационные ресурсы и много других..

Аудит - это анализ накопленной информации, проводимый оперативно, почти в реальном времени, или периодически.

Реализация протоколирования и аудита преследует следующие главные цели:

1. обеспечение подотчетности пользователей и администраторов;
2. обеспечение возможности реконструкции последовательности событий;
3. обнаружение попыток нарушений информационной безопасности;
4. предоставление информации для выявления и анализа проблем.

# Безопасность баз данных

Основной формой организации информационных массивов в ИС являются базы данных. Базу данных можно определить как совокупность взаимосвязанных хранящихся вместе данных при наличии такой минимальной избыточности, которая допускает их использование оптимальным образом для одного или нескольких приложений. В отличие от файловой системы организации и использования информации , БД существует независимо от конкретной программы и предназначена для совместного использования многими пользователями. Такая централизация и независимость данных в технологии БД потребовали создания соответствующих СУБД - сложных комплексов программ, которые обеспечивают выполнение операций корректного размещения данных, надежного их хранения, поиска, модификации и удаления.

Основные требования по безопасности данных, предъявляемые к БД и СУБД, во многом совпадают с требованиями, предъявляемыми к безопасности данных в компьютерных системах – контроль доступа, криптозащита, проверка целостности, протоколирование и т.д..

Под управлением целостностью в БД понимается защита данных в БД от неверных (в отличие от несанкционированных) изменений и разрушений . Поддержание целостности БД состоит в том, чтобы обеспечить в каждый момент времени корректность (правильность) как самих значений всех элементов данных, так и взаимосвязей между элементами данных в БД . С поддержанием целостности связаны следующие основные требования .

1 . Обеспечение достоверности .

В каждый элемент данных информация заносится точно в соответствии с описанием этого элемента .Должны быть предусмотрены механизмы обеспечения устойчивости элементов данных и их логических взаимосвязей к ошибкам или неквалифицированным действиям пользователей .

2 . Управление параллелизмом .

Нарушение целостности БД может возникнуть при одновременном выполнении операций над данными, каждая из которых в отдельности не нарушает целостности БД . Поэтому должны быть предусмотрены механизмы управления данными, обеспечивающие поддержание целостности БД при одновременном выполнении нескольких операций .

3 .Восстановление .

Хранимые в БД данные должны быть устойчивы по отношению к неблагоприятным физическим воздействиям (аппаратные ошибки, сбои питания и т .п .) и ошибкам в программном обеспечении . Поэтому должны быть предусмотрены механизмы восстановления за предельно короткое время того состояния БД, которое было перед появлением неисправности .

Вопросы управления доступом и поддержания целостности БД тесно соприкасаются между собой, и во многих случаях для их решения используются одни и те же механизмы. Различие между этими аспектами обеспечения безопасности данных в БД состоит в том, что управление доступом связано с предотвращением преднамеренного разрушения БД, а управление целостностью - с предотвращением непреднамеренного внесения ошибки

.

## Управление доступом в базах данных

Большинство систем БД представляют собой средство единого централизованного хранения данных. Это значительно сокращает избыточность данных, упрощает доступ к данным и позволяет более эффективно защищать данные . Однако, в технологии БД возникает ряд проблем, связанных, например, с тем, что различные пользователи должны иметь доступ к одним данным и не иметь доступа к другим . Поэтому, не используя специальные средства и методы, обеспечить надежное разделение доступа в БД практически невозможно .

Большинство современных СУБД имеют встроенные средства, позволяющие администратору системы определять права пользователей по доступу к различным частям БД, вплоть до конкретного элемента . При этом имеется возможность не только предоставить доступ тому или иному пользователю, но и указать разрешенный тип доступа: что именно может делать конкретный пользователь с конкретными данными (читать, модифицировать, удалять и т . п .), вплоть до реорганизации всей БД Таблицы (списки) управления доступом широко используются в компьютерных системах, например, в ОС для управления доступом к файлам .Особенность использования этого средства для защиты БД состоит в том, что в качестве объектов защиты выступают не только отдельные файлы (области в сетевых БД, отношения в реляционных БД), но и другие структурные элементы БД: элемент, поле, запись, набор данных .

## Управление целостностью данных

Нарушение целостности данных может быть вызвано рядом причин:

1. сбои оборудования, физические воздействия или стихийные бедствия;
2. ошибки санкционированных пользователей или умышленные действия несанкционированных пользователей;
3. программные ошибки СУБД или ОС;
4. ошибки в прикладных программах;
5. совместное выполнение конфликтных запросов пользователей и др .

Нарушение целостности данных возможно и в хорошо отлаженных системах . Поэтому важно не только не допустить нарушения целостности, но и своевременно обнаружить факт нарушения целостности и оперативно восстановить целостность после нарушения .

## Управление параллелизмом

Поддержание целостности на основе приведенных выше ограничений целостности представляет собой достаточно сложную проблему в системе БД даже с одним пользователем . В системах, ориентированных на многопользовательский режим работы, возникает целый ряд новых проблем, связанных с параллельным выполнением конфликтующих запросов пользователей . Прежде , чем рассмотреть механизмы защиты БД от ошибок, возникающих в случае конфликта пользовательских запросов, раскроем ряд понятий, связанных с управлением параллелизмом .

Важнейшим средством механизма защиты целостности БД выступает объединение совокупности операций, в результате которых БД из одного целостного состояния переходит в другое целостное состояние, в один логический элемент работы, называемый транзакцией. Суть механизма транзакций состоит в том, что до завершения транзакции все манипуляции с данными проводятся вне БД, а занесение реальных изменений в БД производится лишь после нормального завершения транзакции .

С точки зрения безопасности данных такой механизм отображения изменений в БД очень существенен . Если транзакция была прервана, то специальные встроенные средства СУБД осуществляют так называемый откат - возврат БД в состояние, предшествующее началу выполнения транзакции (на самом деле откат обычно заключается просто в невыполнении изменений, обусловленных ходом транзакции, в физической БД) . Если выполнение одной транзакции не нарушает целостности БД, то в результате одновременного выполнения нескольких транзакций целостность БД может быть нарушена . Чтобы избежать подобного рода ошибок, СУБД должна поддерживать механизмы, обеспечивающие захват транзакциями модифицируемых элементов данных до момента завершения модификации так называемые блокировки . При этом гарантируется, что никто не получит доступа к модифицируемому элементу данных, пока транзакция не освободит его . Применение механизма блокировок приводит к новым проблемам управления параллелизмом, в частности, к возникновению ситуаций клинча двух транзакций. Причем, если некоторая транзакция пытается блокировать объект, который уже блокирован другой транзакцией, то ей придется ждать, пока не будет снята блокировка объекта транзакцией, установившей эту блокировку . Иными словами, блокировку объекта может выполнять только одна транзакция .

## Восстановление данных

Как уже отмечалось, возникновение сбоев в аппаратном или программном обеспечении может вызвать необходимость восстановления и быстрого возвращения в состояние, по возможности близкое к тому, которое было перед возникновением сбоя ( ошибки) . К числу причин, вызывающих необходимость восстановления, зачастую относится и возникновение тупиковой ситуации .

Можно выделить три основных уровня восстановления .

1. Оперативное восстановление, которое характеризуется возможностью восстановления на уровне отдельных транзакций при ненормальном окончании ситуации манипулирования данными (например, при ошибке в программе) .
2. Промежуточное восстановление .Если возникают аномалии в работе системы (системно-программные ошибки, сбои программного обеспечения, не связанные с разрушением БД), то требуется восстановить состояние всех выполняемых на момент возникновения сбоя транзакций .
3. Длительное восстановление .

При разрушении БД в результате дефекта на диске восстановление осуществляется с помощью копии БД. Затем воспроизводят результаты выполненных с момента снятия копии транзакций и возвращают систему в состояние на момент разрушения .

### Транзакция и восстановление

Прекращение выполнения транзакции вследствие появления сбоя нарушает целостность БД . Если результаты такого выполнения транзакции потеряны, то имеется возможность их воспроизведения на момент возникновения сбоя . Таким образом, понятие транзакции играет важную роль при восстановлении . Для восстановления целостности БД транзакции должны удовлетворять следующим требованиям:

1. необходимо, чтобы транзакция или выполнялась полностью, или не выполнялась совсем;
2. необходимо, чтобы транзакция допускала возможность возврата в первоначальное состояние, причем, для обеспечения независимого возврата транзакции в начальное состояние монопольную блокировку необходимо осуществлять до момента завершения изменения всех объектов;
3. необходимо иметь возможность воспроизведения процесса выполнения транзакции, причем, для обеспечения этого требования, совместную блокировку необходимо осуществлять до момента завершения просмотра данных всеми транзакциями .

В процессе выполнения любой транзакции наступает момент ее завершения . При этом все вычисления, сделанные транзакцией в ее рабочей области, должны быть закончены, копия результатов ее выполнения должна быть записана в системный журнал . Подобные действия называют операцией фиксации . При появлении сбоя целесообразнее осуществлять возврат не в начало транзакции, а в некоторое промежуточное положение. Точку, куда происходит такой возврат, называют точкой фиксации (контрольной точкой) . Пользователь может установить в процессе выполнения транзакции произвольное количество таких точек . Если в ходе выполнения транзакции достигается точка фиксации, то СУБД автоматически осуществляет указанную выше операцию .

### Откат и раскрутка транзакции

Основным средством, используемым при восстановлении, является системный журнал, в котором регистрируются все изменения, вносимые в БД каждой транзакцией . Возврат транзакции в начальное состояние состоит в аннулировании всех изменений, которые осуществлены в процессе выполнения транзакции . Такую операцию называют откатом . Для воспроизведения результатов выполнения транзакции можно, используя системный журнал, восстановить значения проведенных изменений в порядке их возникновения, либо выполнить транзакцию повторно . Воспроизведение результатов выполнения транзакции с использованием системного журнала называется раскруткой . Раскрутка является достаточно сложной, но необходимой операцией механизмов восстановления современных БД .

# Защита информации при работе в сетях

В настоящее время вопросам безопасности данных в распределенных компьютерных системах уделяется очень большое внимание. Разработано множество средств для обеспечения информационной безопасности, предназначенных для использования на различных компьютерах с разными ОС. В качестве одного из направлений можно выделить межсетевые экраны (firewalls), призванные контролировать доступ к информации со стороны пользователей внешних сетей.

## межсетевые экраны и требования к ним.

Проблема межсетевого экранирования формулируется следующим образом. Пусть имеется две информационные системы или два множества информационных систем. Экран (firewall) - это средство разграничения доступа клиентов из одного множества систем к информации, хранящейся на серверах в другом множестве.

Экран выполняет свои функции, контролируя все информационные потоки между этими двумя множествами информационных систем, работая как некоторая “информационная мембрана”. В этом смысле экран можно представлять себе как набор фильтров, анализирующих проходящую через них информацию и, на основе заложенных в них алгоритмов, принимающих решение: пропустить ли эту информацию или отказать в ее пересылке. Кроме того, такая система может выполнять регистрацию событий, связанных с процессами разграничения доступа. в частности, фиксировать все “незаконные” попытки доступа к информации и, дополнительно, сигнализировать о ситуациях, требующих немедленной реакции, то есть поднимать тревогу.

Рассмотрим требования к реальной системе, осуществляющей межсетевое экранирование. В большинстве случаев экранирующая система должна:

1. Обеспечивать безопасность внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи;
2. Обладать мощными и гибкими средствами управления для полного и, насколько возможно, простого воплощения в жизнь политики безопасности организации. Кроме того, экранирующая система должна обеспечивать простую реконфигурацию системы при изменении структуры сети;
3. Работать незаметно для пользователей локальной сети и не затруднять выполнение ими легальных действий;
4. Работать достаточно эффективно и успевать обрабатывать весь входящий и исходящий трафик в "пиковых" режимах. Это необходимо для того, чтобы firewall нельзя было, образно говоря, "забросать" большим количеством вызовов, которые привели бы к нарушению работы;
5. Обладать свойствами самозащиты от любых несанкционированных воздействий, поскольку межсетевой экран является ключом к конфиденциальной информации в организации;
6. Если у организации имеется несколько внешних подключений, в том числе и в удаленных филиалах, система управления экранами должна иметь возможность централизованно обеспечивать для них проведение единой политики безопасности;
7. Иметь средства авторизации доступа пользователей через внешние подключения. Типичной является ситуация, когда часть персонала организации должна выезжать, например, в командировки, и в процессе работы им требуется доступ, по крайней мере, к некоторым ресурсам внутренней компьютерной сети организации. Система должна надежно распознавать таких пользователей и предоставлять им необходимый виды доступа.

При конфигурировании межсетевых экранов основные конструктивные решения заранее задаются политикой безопасности, принятой в организации. В описываемом случае необходимо рассмотреть два аспекта политики безопасности: политику доступа к сетевым сервисам и политику межсетевого экрана При формировании политики доступа к сетевым сервисам должны быть сформулированы правила доступа пользователей к различным сервисам, используемым в организации. Этот аспект, таким образом состоит из двух компонент. База правил для пользователей описывает когда, какой пользователь (группа пользователей) каким сервисом и на каком компьютере может воспользоваться. Отдельно определяются условия работы пользователей вне локальной сети организации равно как и условия их аутентификации. База правил для сервисов описывает набор сервисов, проходящих через сетевой экран, а также допустимые адреса клиентов серверов для каждого сервиса (группы сервисов). В политике, регламентирующей работу межсетевого экрана, решения могут быть приняты как в пользу безопасности в ущерб легкости использования, так и наоборот. Есть два основных:

1. Все, что не разрешено, то запрещено.
2. Все, что не запрещено, то разрешено.

В первом случае межсетевой экран должен быть сконфигурирован таким образом, чтобы блокировать все, а его работа должна быть упорядочена на основе тщательного анализа опасности и риска. Это напрямую отражается на пользователях и они, вообще говоря, могут рассматривать экран просто как помеху. Такая ситуация заставляет накладывать повышенные требования на производительность экранирующих систем и повышает актуальность такого свойства, как "прозрачность" работы межсетевого экрана с точки зрения пользователей. Первый подход является более безопасным, поскольку предполагается, что администратор не знает, какие сервисы или порты безопасны, и какие "дыры" могут существовать в ядре или приложении разработчика программного обеспечения. Ввиду того, что многие производители программного обеспечения не спешат публиковать обнаруженные недостатки, существенные для информационной безопасности (что характерно для производителей так называемого "закрытого" программного обеспечения, крупнейшим из которых является Microsoft), этот подход является, несомненно, более консервативным. В сущности, он является признанием факта, что незнание может причинить вред. Во втором случае, системный администратор работает в режиме реагирования, предсказывая, какие действия, отрицательно воздействующие на безопасность, могут совершить пользователи либо нарушители, и готовит защиту против таких действий. Это существенно восстанавливает администратора firewall против пользователей в бесконечных "гонках вооружений", которые могут оказаться весьма изматывающими. Пользователь может нарушить безопасность информационной системы, если не будет уверен в необходимости мер, направленных на обеспечение безопасности

Но в любом случае хорошо сконфигуированный межсетевой экран в состоянии остановить большинство известных компьютерных атак.

## Использование электронной почты

Электронная почта или email – самый популярный вид использования Интернета. С помощью электронной почты в Интернете вы можете послать письмо миллионам людей по всей планете. Существуют шлюзы частных почтовых систем в интернетовский email, что занчительно расширяет ее возможности.

### Защита от фальшивых адресов

Адресу отправителя в электронной почте Интернета нельзя доверять, так как отправитель может указать фальшивый обратный адрес, или заголовок может быть модифицирован в ходе передачи письма, или отправитель может сам соединиться с SMTP-портом на машине, от имени которой он хочет отправить письмо, и ввести текст письма.

От этого можно защититься с помощью использования шифрования для присоединения к письмам электронных подписей. Одним популярным методом является использование шифрования с открытыми ключами. Однонаправленная хэш-функция письма шифруется, используя секретный ключ отправителя. Получатель использует открытый ключ отправителя для расшифровки хэш-функции и сравнивает его с хэш-функцией, рассчитанной по полученному сообщению. Это гарантирует, что сообщение на самом деле на писано отправителем, и не было изменено в пути

### Защита от перехвата

Заголовки и содержимое электронных писем передаются в чистом виде. В результате содержимое сообщения может быть прочитано или изменено в процессе передачи его по Интернету. Заголовок может быть модифицирован, чтобы скрыть или изменить отправителя, или для того чтобы перенаправить сообщение. От него можно защититься с помощью шифрования содержимого сообщения или канала, по которому он передается. Если канал связи зашифрован, то системные администраторы на обоих его концах все-таки могут читать или изменять сообщения. Было предложено много различных схем шифрования электронной почты, но ни одна из них не стала массовой. Одним из самых популярных приложений является PGP. В прошлом использование PGP было проблематичным, так как в ней использовалось шифрование, подпадавшее под запрет на экспорт из США. Коммерческая версия PGP включает в себя плагины для нескольких популярных почтовых программ, что делает ее особенно удобной для включения в письмо электронной подписи и шифрования письма клиентом. Последние версии PGP используют лицензированную версию алгоритма шифрования с открытыми ключами RSA.

# Заключение.

Нужно четко представлять себе, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в информационных системах. 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. В России на рынке защитных средств, присутствуют такие продукты как Кобра, Dallas Lock, Secret Net, Аккорд, Криптон и ряд других. 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 неконкурентноспособной, 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.

Поэтому 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..

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ.

1. П. Зегжда, «Теория и практика. Обеспечение информационной безопасности». - Москва, 1996.
2. “Энциклопедия компьютерных вирусов Евгения Касперского” – электронная версия от 16.10.1999 г.
3. Л.Хофман, «Современные методы защиты информации», - Москва, 1995.
4. Бюллетень лаборатории информационных технологий NIST за май 1999 г. Э. Леннон " Компьютерные атаки: что это такое и как защититься от них"
5. Левин В.К. Защита информации в информационно-вычислительных системах и сетях // Программирование. - 1994. - N5.
6. Гайкович В., Першин А. Безопасность электронных банковских систем. - М.: "Единая Европа", 1994.
7. Громов В.И. Васильев Г.А "Энциклопедия компьютерной безопасности" (электронный сборник 1999 год)
8. Д. Ведеев Защита данных в компьютерных сетях / Открытые системы Москва, 1995, №3,
9. Косарев В.П. и др. Под ред. Косарева В.П. и Еремина Л.В. Компьютерные системы и сети: Учеб. Пособие - М.: Финансы и статистика ,1999г.
10. Баричев С. “Введение в криптографию” - электронный сборник
11. Вьюкова Н.И., Галатенко В.А. “Информационная безопасность систем управления базами данных” 1996 – статья в электронном журнале.