# Компьютерные вирусы и их классификация. Средства защиты от вирусо
## Компьютерные вирусы и их классификация

**Компьютерный вирус** - это специально написанная небольшая по размерам программа, имеющая специфический алгоритм, направленный на тиражирование копии программы, или её модификацию и выполнению действий развлекательного, пугающего или разрушительного характера.

Тем или иным способом вирусная программа попадает в компьютер и заражает их. Программа, внутри которой находится вирус, называется **зараженной**. Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и заражает другие программы, а также выполняет какие-либо вредоносные действия. Например, портит файлы или таблицу размещения файлов на диске, занимает оперативную память и т.д. После того, как вирус выполнит свои действия, он передает управление той программе, в которой он находится, и она работает как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной. Поэтому далеко не сразу пользователь узнаёт о присутствии вируса в машине.

Многие разновидности вирусов устроены так, что при запуске зараженной программы вирус остается в памяти компьютера и время от времени заражает программы и выполняет нежелательные действия на компьютере. Пока на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметным.

К числу наиболее характерных **признаков заражения компьютера вирусами** относятся следующие:

- некоторые ранее исполнявшиеся программы перестают запускаться или внезапно останавливаются в процессе работы;
- увеличивается длина исполняемых файлов;
- быстро сокращается объём свободной дисковой памяти;
- на носителях появляются дополнительные сбойные кластеры, в которых вирусы прячут свои фрагменты или части повреждённых файлов;
- замедляется работа некоторых программ;
- в текстовых файлах появляются бессмысленные фрагменты;
- наблюдаются попытки записи на защищённую дискету;
- на экране появляются странные сообщения, которые раньше не наблюдались;
- появляются файлы со странными датами и временем создания (несуществующие дни несуществующих месяцев, годы из следующего

столетия, часы, минуты и секунды, не укладывающиеся в общепринятые интервалы и т. д.);

- операционная система перестаёт загружаться с винчестера;
- появляются сообщения об отсутствии винчестера;
- данные на носителях портятся.

Любая внешний носитель информации (флэш. диск и пр.), не защищённый от записи, находясь в заражённом компьютере, может быть заражен. Следовательно. побывав в зараженном компьютере они являются разносчиками вирусов. Существует ещё один канал распространения вирусов, связанный с компьютерными сетями, особенно всемирной сетью Internet. Часто источниками заражения являются программные продукты, приобретённые нелегальным путем.

Существует несколько **классификаций компьютерных вирусов**:

1. **По среде обитания** различают вирусы сетевые, файловые, загрузочные и файлово-загрузочные.

2. **По способу заражения** выделяют резидентные и нерезидентные вирусы.

3. **По степени воздействия** вирусы бывают неопасные, опасные и очень опасные;

4. **По особенностям алгоритмов** вирусы делят на паразитические, репликаторы, невидимки, мутанты, троянские, макро-вирусы.

**Загрузочные вирусы** заражают загрузочный сектор винчестера или дискеты и загружаются каждый раз при начальной загрузке операционной системы.

**Резидентные вирусы** загружается в память компьютера и постоянно там находится до выключения компьютера.

**Самомодифицирующиеся вирусы (мутанты)** изменяют свое тело таким образом, чтобы антивирусная программа не смогла его идентифицировать.

**Стелс-вирусы (невидимки)** перехватывает обращения к зараженным файлам и областям и выдают их в незараженном виде.

**Троянские вирусы** маскируют свои действия под видом выполнения обычных приложений.

Вирусом могут быть заражены следующие объекты:

**1. Исполняемые файлы**, т.е. файлы с расширениями имен .com и .exe, а также оверлейные файлы, загружаемые при выполнении других программ. Вирусы, заражающие файлы, называются **файловыми.** Вирус в зараженных исполняемых файлах начинает свою работу при запуске той программы, в которой он находится. Наиболее опасны те вирусы, которые

после своего запуска остаются в памяти резидентно - они могут заражать файлы и выполнять вредоносные действия до следующей перезагрузки компьютера. А если они заразят любую программу из автозапуска компьютера, то и при перезагрузке с жесткого диска вирус снова начнет свою работу.

**2. Загрузчик операционной системы и главная загрузочная запись жесткого диска**. Вирусы, поражающие эти области, называются **загрузочными**. Такой вирус начинает свою работу при начальной загрузке компьютера и становится резидентным, т.е. постоянно находится в памяти компьютера. Механизм распространения загрузочных вирусов - заражение загрузочных записей вставляемых в компьютер дискет. Часто такие вирусы состоят из двух частей, поскольку загрузочная запись имеет небольшие размеры и в них трудно разместить целиком программу вируса. Часть вируса располагается в другом участке диска, например, в конце корневого каталога диска или в кластере в области данных диска. Обычно такой кластер объявляется дефектным, чтобы исключить затирание вируса при записи данных на диск.

**3. Файлы документов, информационные файлы баз данных, таблицы табличных процессоров** и другие аналогичные файлы могут быть заражены **макро-вирусами**. Макро-вирусы используют возможность вставки в формат многих документов макрокоманд.

Если не принимать мер по защите от вирусов, то последствия заражения могут быть очень серьезными. Например, в начале 1989 г. вирусом, написанным американским студентом Моррисом, были заражены и выведены из строя тысячи компьютеров, в том числе принадлежащих министерству обороны США. Автор вируса был приговорен судом к трем месяцам тюрьмы и штрафу в 270 тыс. дол. Наказание могло быть и более строгим, но суд учел, что вирус не портил данные, а только размножался.

**Средства защиты от вирусов**

**Для защиты** от вирусов можно использовать:

- Общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы или комплексы программ для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих методов защиты:

- резервное копирование информации, т. е. создание копий файлов и системных областей дисков на дополнительном носителе;

- разграничение доступа, предотвращающее несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их одних недостаточно. Необходимо применять специализированные программы для защиты от вирусов. Эти программы можно разделить на несколько видов:

1. Программы-**детекторы** позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.
2. Программы-**доктора**, или **фаги**, восстанавливают зараженные программы убирая из них тело вируса, т.е. программа возвращается в то состояние, в котором она находилась до заражения вирусом.
3. Программы-**ревизоры** сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий об этом сообщается пользователю.
4. **Доктора-ревизоры** - это гибриды ревизоров и докторов, т.е. программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут автоматически вернуть их в исходное состояние.
5. **Программы-фильтры** располагаются резидентно в оперативной памяти компьютера, перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Поэтому наилучшей стратегией защиты от вирусов является **многоуровневая защита.**

**Средствами разведки** в защите от вирусов являются программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

**На первом уровне защиты** находятся резидентные программы для защиты от вируса. Эти программы могут первыми сообщить о вирусной атаке и предотвратить заражение программ и диска.

**Второй уровень защиты** составляют программы-ревизоры, программы-доктора и доктора-ревизоры. Ревизоры обнаруживают нападение

тогда, когда вирус сумел пройти сквозь первый уровень. Программы-доктора применяются для восстановления зараженных программ, если ее копий нет в архиве, но они не всегда лечат правильно. Доктора-ревизоры обнаруживают нападение вируса и лечат зараженные файлы, причем контролируют правильность лечения.

**Третий уровень защиты** - это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные.

В **резерве** находятся архивные копии информации и эталонные диски с программными продуктами. Они позволяют восстановить информацию при ее повреждении на жестком диске.

Среди наиболее распространненых российских антивирусных пакетов следует отметить **Kaspersky Antivirus**,**DrWeb**, **Adinf**. Перечисленные средства могут оказать серьёзную помощь в обнаружении вирусов и восстановлении повреждённых файлов, однако не менее важно и соблюдение сравнительно простых **правил антивирусной безопасности.**

1. Следует избегать пользоваться нелегальными источниками получения программ. Наименее же опасен законный способ покупки фирменных продуктов.
2. Осторожно следует относиться к программам, полученным из сети Internet, так как нередки случаи заражения вирусами программ, распространяемых по электронным каналам связи.
3. Всякий раз, когда дискета побывала в чужом компьютере, необходимо проверить дискету с помощью одного или двух антивирусных средств.
4. Необходимо прислушиваться к информации о вирусных заболеваниях на компьютерах в своем районе проживания или работы и о наиболее радикальных средствах борьбы с ними. Атакам нового вируса в первую очередь подвергаются компьютеры образовательных учреждений.
5. При передаче программ или данных на своей дискете её следует обязательно защитить от записи.

Антивирусный комплекс - набор программ, предназначенных для решения практических проблем по обеспечению двух режимов антивирусной проверки, а также содержащий средства для обновления антивирусных баз и управления

# Разработка политики информационной безопасности

**Признаки компьютерных преступлений:**

- неавторизованное использование компьютерного времени;
- неавторизованные попытки доступа к файлам данных;
- кражи частей компьютеров;
- кражи программ;
- физическое разрушение оборудования;
- уничтожение данных или программ;
- неавторизованное владение дискетами, лентами или распечатками.

Это только самые очевидные признаки, на которые следует обратить внимание при выявлении компьютерных преступлений. Иногда эти признаки говорят о том, что преступление уже совершено, или что не выполняются меры защиты. Они также могут свидетельствовать о наличии уязвимых мест и указать, где находится брешь в защите. В то время как признаки могут помочь выявить преступление или злоупотребление, меры защиты могут помочь предотвратить его.

**Защита информации** – это деятельность по предотвращению утраты и утечки защищаемой информации.

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.

Информационная безопасность дает гарантию того, что достигаются следующие цели:

- конфиденциальность критической информации;
- целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода);
- доступность информации, когда она нужна;
- учет всех процессов, связанных с информацией.

Под ***критическими данными*** понимаются данные, которые требуют защиты из-за вероятности нанесения ущерба и его величины в том случае, если произойдет случайное или умышленное раскрытие, изменение, или разрушение данных. К критическим также относят данные, которые при неправильном использовании или раскрытии могут отрицательно воздействовать на способности организации решать свои задачи;

персональные данные и другие данные, защита которых требуется указами Президента РФ, законами РФ и другими подзаконными документами.

Любая система безопасности, в принципе, может быть вскрыта. Эффективной считают такую защиту, стоимость взлома которой соизмерима с ценностью добываемой при этом информации.

Применительно к средствам защиты от несанкционированного доступа определены семь классов защищенности (1 - 7) средств вычислительной техники и девять классов (1А, 1Б, 1В, 1Г, 1Д, 2А, 2Б, 3А, 3Б) автоматизированных систем. Для средств вычислительной техники самым низким является класс 7, а для автоматизированных систем - 3Б.

**Политика безопасности** определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:

1. **Невозможность миновать защитные средства.** Все информационные потоки в защищаемую сеть и из нее должны проходить через средства защиты. Не должно быть тайных модемных входов или тестовых линий, идущих в обход защиты.

2. **Усиление самого слабого звена.** Надежность любой защиты определяется самым слабым звеном, так как злоумышленники взламывать именно его. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

3. **Невозможность перехода в небезопасное состояние.** Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ.

4. **Минимизация привилегий.** Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

5. **Разделение обязанностей.** Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс.

6. **Эшелонированность обороны.** Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж. Эшелонированная оборона способна по крайней мере задержать

злоумышленника и существенно затруднить незаметное выполнение вредоносных действий.

**7. Разнообразие защитных средств.** Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными, по возможности, несовместимыми между собой навыками.

**8. Простота и управляемость информационной системы.** Принцип простоты и управляемости гласит, что только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование.

**9. Обеспечение всеобщей поддержки мер безопасности.** Принцип всеобщей поддержки мер безопасности носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или враждебным, то режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное теоретическое и практическое обучение.

## Технические, организационные и программные средства обеспечения сохранности и защиты от несанкционированного доступа

Существует **четыре уровня защиты компьютерных и информационных ресурсов:**

**Предотвращение** предполагает, что только авторизованный персонал имеет доступ к защищаемой информации и технологии.

**Обнаружение** предполагает раннее раскрытие преступлений и злоупотреблений, даже если механизмы защиты были обойдены.

**Ограничение** уменьшает размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению.

**Восстановление** обеспечивает эффективное воссоздание информации при наличии документированных и проверенных планов по восстановлению.

**Меры защиты** - это меры, вводимые руководством, для обеспечения безопасности информации. К мерам защиты относят разработку административных руководящих документов, установку аппаратных устройств или дополнительных программ, основной целью которых является предотвращение преступлений и злоупотреблений.

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно разделить на **четыре уровня**:

- **законодательный:** законы, нормативные акты, стандарты и т. п.;

- **административный:** действия общего характера, предпринимаемые руководством организации;

- **процедурный:** конкретные меры безопасности, имеющие дело с людьми;

- **программно-технический:** конкретные технические меры.

В настоящее время наиболее подробным законодательным документом России в области информационной безопасности является Уголовный кодекс. В разделе "Преступления против общественной безопасности" имеется глава "Преступления в сфере компьютерной информации". Она содержит три статьи - "Неправомерный доступ к компьютерной информации", "Создание, использование и распространение вредоносных программ для ЭВМ" и "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети". Уголовный кодекс стоит на страже всех аспектов информационной безопасности - доступности, целостности, конфиденциальности, предусматривая наказания за "уничтожение, блокирование, модификацию и копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети".

Рассмотрим некоторые меры защиты информационной безопасности компьютерных систем.

**1. Аутентификация пользователей**. Данная мера требует, чтобы пользователи выполняли процедуры входа в компьютер, используя это как средство для идентификации в начале работы. Для аутентификации личности каждого пользователя нужно использовать уникальные пароли, не являющиеся комбинациями личных данных пользователей, для пользователя. Необходимо внедрить меры защиты при администрировании паролей, и ознакомить пользователей с наиболее общими ошибками, позволяющими совершиться компьютерному преступлению. Если в компьютере имеется встроенный стандартный пароль, его нужно обязательно изменить.

Еще более надёжное решение состоит в организации контроля доступа в помещения или к конкретному компьютеру сети с помощью идентификационных пластиковых карточек с встроенной микросхемой - так называемых микропроцессорных карточек (smart - card). Их надёжность обусловлена в первую очередь невозможностью копирования или подделки кустарным способом. Установка специального считывающего устройства таких карточек возможна не только на входе в помещения, где расположены компьютеры, но и непосредственно на рабочих станциях и серверах сети.

Существуют также различные устройства для идентификации личности по биометрической информации - по радужной оболочке глаза, отпечаткам пальцев, размерам кисти руки и т.д.

**2. Защита пароля.**

Следующие правила полезны для защиты пароля:

- нельзя делится своим паролем ни с кем;
- пароль должен быть трудно угадываемым;
- для создания пароля нужно использовать строчные и прописные буквы, а еще лучше позволить компьютеру самому сгенерировать пароль;
- не рекомендуется использовать пароль, который является адресом, псевдонимом, именем родственника, телефонным номером или чем-либо очевидным;
- предпочтительно использовать длинные пароли, так как они более безопасны, лучше всего, чтобы пароль состоял из 6 и более символов;
- пароль не должен отображаться на экране компьютера при его вводе;
- пароли должны отсутствовать в распечатках;
- нельзя записывать пароли на столе, стене или терминале, его нужно держать в памяти;
- пароль нужно периодически менять и делать это не по графику;
- на должности администратора паролей должен быть самый надежный человек;
- не рекомендуется использовать один и тот же пароль для всех сотрудников в группе;
- когда сотрудник увольняется, необходимо сменить пароль;
- сотрудники должны расписываться за получение паролей.

**3. Процедуры авторизации.**

В организации, имеющей дело с критическими данными, должны быть разработаны и внедрены процедуры авторизации, которые определяют, кто из пользователей должен иметь доступ к той или иной информации и приложениям.

В организации должен быть установлен такой порядок, при котором для использования компьютерных ресурсов, получения разрешения доступа к информации и приложениям, и получения пароля требуется разрешение тех или иных начальников.

Если информация обрабатывается на большом вычислительном центре, то необходимо контролировать физический доступ к вычислительной технике. Могут оказаться уместными такие методы, как журналы, замки и пропуска, а также охрана. Ответственный за информационную безопасность

должен знать, кто имеет право доступа в помещения с компьютерным оборудованием и выгонять оттуда посторонних лиц.

**4. Предосторожности при работе.**

Рекомендуется:

- отключать неиспользуемые терминалы;
- закрывать комнаты, где находятся терминалы;
- разворачивать экраны компьютеров так, чтобы они не были видны со стороны двери, окон и прочих мест, которые не контролируются;
- установить специальное оборудование, ограничивающее число неудачных попыток доступа, или делающее обратный звонок для проверки личности пользователей, использующих телефоны для доступа к компьютеру
- использовать программы отключения терминала после определенного периода неиспользования;
- выключать систему в нерабочие часы;
- использовать системы, позволяющие после входа пользователя в систему сообщать ему время его последнего сеанса и число неудачных попыток установления сеанса после этого. Это позволит сделать пользователя составной частью системы проверки журналов.

**5. Физическая безопасность.**

В защищаемых компьютерных системах необходимо принимать меры по предотвращению, обнаружению и минимизации ущерба от пожара, наводнения, загрязнения окружающей среды, высоких температур и скачков напряжения.

Пожарная сигнализация и системы пожаротушения должны регулярно проверяться. ПЭВМ можно защитить с помощью кожухов, чтобы они не были повреждены системой пожаротушения. Горючие материалы не должны храниться в этих помещениях с компьютерами.

Температура в помещении может контролироваться кондиционерами и вентиляторами, а также хорошей вентиляцией в помещении. Проблемы с чрезмерно высокой температурой могут возникнуть в стойках периферийного оборудования или из-за закрытия вентиляционного отверстия в терминалах или ПЭВМ, поэтому необходима их регулярная проверка.

Желательно применение воздушных фильтров, что поможет очистить воздух от веществ, которые могут нанести вред компьютерам и дискам. Следует запретить курить, принимать пищу и пить возле ПЭВМ.

Компьютеры должны размещаться как можно дальше источников большого количества воды, например трубопроводов.

**6. Защита носителей информации (исходных документов, лент, картриджей, дисков, распечаток).**

Для защиты носителей информации рекомендуется:

- вести, контролировать и проверять реестры носителей информации;
- обучать пользователей правильным методам очищения и уничтожения носителей информации;
- делать метки на носителях информации, отражающие уровень критичности содержащейся в них информации;
- уничтожать носители информации в соответствии с планом организации;
- доводить все руководящие документы до сотрудников;
- хранить диски в конвертах, коробках, металлических сейфах;
- не касаться поверхностей дисков, несущих информацию
- осторожно вставлять диски в компьютер и держать их подальше от источников магнитного поля и солнечного света;
- убирать диски и ленты, с которыми в настоящий момент не ведется работа;
- хранить диски разложенными по полкам в определенном порядке;
- не давать носители информации с критической информацией неавторизованным людям;
- выбрасывать или отдавать поврежденные диски с критической информацией только после их размагничивания или аналогичной процедуры;
- уничтожать критическую информацию на дисках с помощью их размагничивания или физического разрушения в соответствии с порядком в организации;
- уничтожать распечатки и красящие ленты от принтеров с критической информацией в соответствии с порядком организации;
- обеспечить безопасность распечаток паролей и другой информации, позволяющей получить доступ к компьютеру.

**7. Выбор надежного оборудования.**

Производительность и отказоустойчивость информационной системы во многом зависит от работоспособности серверов. При необходимости обеспечения круглосуточной бесперебойной работы информационной системы используются специальные отказоустойчивые компьютеры, т. е. такие, выход из строя отдельного компонента которых не приводит к отказу машины.

На надежности информационных систем отрицательно сказываются и наличие устройств, собранных из комплектующих низкого качества, и использование нелицензионного ПО. Чрезмерная экономия средств на

обучение персонала, закупку лицензионного ПО и качественного оборудования приводит к уменьшению времени безотказной работы и значительным затратам на последующее восстановление системы.

**8. Источники бесперебойного питания.**

Компьютерная система энергоемка, и потому первое условие ее функционирования - бесперебойная подача электроэнергии. Необходимой частью информационной системы должны стать источники бесперебойного питания для серверов, а по возможности, и для всех локальных рабочих станций. Рекомендуется также дублировать электропитание, используя для этого различные городские подстанции. Для кардинального решения проблемы можно установить резервные силовые линии от собственного генератора организации.

**9. Разработка адекватных планов обеспечения непрерывной работы и восстановления.**

Целью планов обеспечения непрерывной работы и восстановления являются гарантии того, что пользователи смогут продолжать выполнять свои самые главные обязанности в случае невозможности работы по информационной технологии. Обслуживающий персонал должен знать, как им действовать по этим планам.

Планы обеспечения непрерывной работы и восстановления (ОНРВ) должны быть написаны, проверены и регулярно доводиться до сотрудников. Процедуры плана должны быть адекватны уровню безопасности и критичности информации. План ОНРВ может применяться в условиях неразберихи и паники, поэтому нужно регулярно проводить тренировки сотрудников.

**10. Резервное копирование.**

Одним из ключевых моментов, обеспечивающих восстановление системы при аварии, является резервное копирование рабочих программ и данных. В локальных сетях, где установлены несколько серверов, чаще всего система резервного копирования устанавливается непосредственно в свободные слоты серверов. В крупных корпоративных сетях предпочтение отдается выделенному специализированному архивационному серверу, который автоматически архивирует информацию с жестких дисков серверов и рабочих станций в определенное время, установленное администратором сети, выдавая отчет о проведенном резервном копировании.

Для архивной информации, представляющей особую ценность, рекомендуется предусматривать охранное помещение. Дубликаты наиболее ценных данных, лучше хранить в другом здании или даже в другом городе.

Последняя мера делает данные неуязвимыми в случае пожара или другого стихийного бедствия.

**11. Дублирование, мультиплексирование и резервирование офисов.**

Помимо резервного копирования, которое производится при возникновении внештатной ситуации либо по заранее составленному расписанию, для большей сохранности данных на жестких дисках применяют специальные технологии - зеркалирование дисков и создание RAID-массивов, которые представляют собой объединение нескольких жестких дисков. При записи информация поровну распределяется между ними, так что при выходе из строя одного из дисков находящиеся на нем данные могут быть восстановлены по содержимому остальных.

Технология кластеризации предполагает, что несколько компьютеров функционируют как единое целое. Кластеризуют, как правило, серверы. Один из серверов кластера может функционировать в режиме горячего резерва в полной готовности начать выполнять функции основной машины в случае ее выхода из строя. Продолжением технологии кластеризации является распределенная кластеризация, при которой через глобальную сеть объединяются несколько кластерных серверов, разнесенных на большое расстояние.

Распределенные кластеры близки к понятию резервных офисов, ориентированных на обеспечение жизнедеятельности предприятия при уничтожении его центрального помещения. Резервные офисы делят на холодные, в которых проведена коммуникационная разводка, но отсутствует какое-либо оборудование и горячие, которыми могут быть дублирующий вычислительный центр, получающий всю информацию из центрального офиса, филиал, офис на колесах и т.д.

**12. Резервирование каналов связи.**

При отсутствии связи с внешним миром и своими подразделениями, офис оказывается парализованным, потому большое значение имеет резервирование внешних и внутренних каналов связи. При резервировании рекомендуется сочетать разные виды связи - кабельные линии и радиоканалы, воздушную и подземную прокладку коммуникаций и т.д.

По мере того, как компании все больше и больше обращаются к Internet, их бизнес оказывается в серьезной зависимости от функционирования Internet-провайдера. У поставщиков доступа к Сети иногда случаются достаточно серьезные аварии, поэтому важно хранить все важные приложения во внутренней сети компании и иметь договора с несколькими местными провайдерами. Следует также заранее продумать

способ оповещения стратегических клиентов об изменении электронного адреса и требовать от провайдера проведения мероприятий, обеспечивающих оперативное восстановление его услуг после аварий.

**12. Защита данных от перехвата.**

Для любой из трех основных технологий передачи информации существует технология перехвата: для кабельных линий - подключение к кабелю, для спутниковой связи – использование антенны приема сигнала со спутника, для радиоволн - радиоперехват. Российские службы безопасности разделяют коммуникации на три класса. Первый охватывает локальные сети, расположенные в зоне безопасности, т. е. территории с ограниченным доступом и заэкранированным электронным оборудованием и коммуникационными линиями, и не имеющие выходов в каналы связи за ее пределами. Ко второму классу относятся каналы связи вне зоны безопасности, защищенные организационно-техническими мерами, а к третьему - незащищенные каналы связи общего пользования. Применение коммуникаций уже второго класса значительно снижает вероятность перехвата данных.

Для защиты информации во внешнем канале связи используются следующие устройства: скремблеры для защиты речевой информации, шифраторы для широковещательной связи и криптографические средства, обеспечивающие шифрование цифровых данных.

Важнейшими характеристиками алгоритмов шифрования являются криптостойкость, длина ключа и скорость шифрования. В настоящее время наиболее часто применяются три основных стандарта шифрования:

- DES;
- ГОСТ 28147-89 - отечественный метод, отличающийся высокой криптостойкостью;
- RSA - система, в которой шифрование и расшифровка осуществляется с помощью разных ключей.