1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ.

1. Общие понятия

Целью защиты информации является обеспечении безопасности хранимой и обрабатываемой информации, а также используемых программных средств.

Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе.

Под ***безопасностью информации*** понимается состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних и внешних угроз.

Другими словами – это состояние устойчивости информации к случайным или преднамеренным воздействиям, исключающее недопустимые риски ее уничтожения, искажения и раскрытия, которые приводят к материальному ущербу владельца или пользователя информации.

Безусловно, особую опасность представляют нарушения «извне», т.е. внешние, которые всегда осуществляются умышленно. К этой категории относятся, например, действия хакеров, обративших свои знания и умения в средство добывания денег незаконными способами.

1.1. Модель системы защиты информации.

В процессе деятельности сотрудники принимают, обрабатывают и передают информацию, организуя информационный обмен. Именно эти процессы и вызывают необходимость защиты информации. Всю ли информацию надо одинаково защищать? Это зависит от того, какая информация, т.е. какие сведения она содержит, к какой категории ее можно отнести.

1.2. Классификация информации.

Применительно к уровню защиты информацию можно разделить на три категории:

1. Информация, составляющая государственную тайну;
2. Сведения, содержащие коммерческую тайну;
3. Персональные данные.

1. Информация, составляющая государственную тайну.

Владельцем этой категории информации является государство. Оно само выдвигает требования по ее защите и контролирует их исполнение Законом РФ «О государственной тайне» (от 21 июля 1993 года №5485-1). Нарушение этих требований влечет за собой применение санкций, предусмотренных Уголовным кодексом.

Преступлениям в сфере компьютерной информации посвящены три статьи Уголовного Кодекса России это:

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование

информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.
2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.
2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.

К государственной тайне относятся защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной и т.п. деятельности, распространение которых может нанести ущерб безопасности РФ. В связи с чрезвычайной важностью данного вида информации доступ к сведениям, составляющим государственную тайну, обеспечивается для работников только после проведения процедуры оформления соответствующего права. Речь идет о получении так называемого «допуска».

2. Сведения, содержащие коммерческую тайну.

Информацией этой категории владеют предприятия, и поэтому они вправе ею распоряжаться и самостоятельно определять степень защиты. Вопросы законодательной защиты коммерческой тайны рассматривались в законах, принятых в России.

22 января 1999 г. Государственной Думой был принят проект закона «О коммерческой тайне», в котором коммерческая тайна определена следующим образом: «Коммерческая тайна – научно-техническая, коммерческая, организационная или иная используемая в предпринимательской деятельности информация, которая: обладает реальной или потенциальной экономической ценностью в силу того, что она не является общеизвестной и не может быть легко получена законным образом другими лицами, которые могли бы получить экономическую выгоду от ее разглашения или использования, и является предметом адекватных обстоятельств правовых, организационных, технических и иных мер по охране информации (режим коммерческой тайны)». Законом устанавливаются три крикерия, которые определяют охраноспособность сведений, составляющих коммерческую тайну:

- информация должна иметь действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;
- к информации не должно быть свободного доступа на законных основаниях;

- требуется, чтобы обладатель информации принимал меры к охране ее конфиденциальности.

Для того, чтобы сведения, которые должны быть отнесены к категории коммерческой тайны, приобрели законную силу, их необходимо оформить в виде специального перечня, утвержденного руководителем предприятия. При этом возможно установление грифов «коммерческая тайна» или «конфиденциально».

Однако не все сведения могут быть отнесены к категории имеющих статус коммерческой тайны. Так, поскольку государство берет на себя функции контроля за осуществление деятельности коммерческих организаций, правовыми документами определен перечень сведений, которые не могут составлять коммерческую тайну предприятия:

- его учредительные документы;
- разрешительные документы на право осуществления коммерческой деятельности;
- сведения по установленным формам отчетности о финансово-хозяйственной деятельности предприятия;
- сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения;
- документы о платежеспособности;
- сведения о численности, составе работающих, их заработной плате и условиях труда.

3. Персональные данные. Информация затрагивает личную жизнь. Государство рассматривает ее защиту как одну из своих важных задач.

Обычно ***данные о людях*** наиболее важны для них самих, но, как бы это не описывали в шпионских фильмах, мало что значат для похитителей. Иногда личные данные могут использоваться для компрометации не только отдельных людей, но целых организаций, например, если выяснится скрываемая прежняя судимость за растрату директора коммерческого банка. Но тот, кто компрометирует, не имея твердой моральной основы для этого, в большинстве случаев теряет больше самого компрометируемого. Лишь малая кучка профессиональных негодяев из адвокатов и журналистов, которым уже нет дела до своего морального облика, наживается, занимаясь компрометацией. Тем не менее информация о людях ценна сама по себе***, основной убыток от ее разглашения - личное несчастье человека.***

1.3. Цели и задачи защиты информации

Информация необходима для принятия различных управленческих решений в процессе деятельности компаний, предприятий и организаций.

Частота возникновения атак на информационные системы (цели вторжения злоумышленников в информационное пространство предприятии):

1. Хищение коммерческой информации – 45%
2. Финансовое мошенничество – 13%
3. Несанкционированный доступ изнутри компании – 10%
4. Проникновение в систему извне- 9%
5. Нарушение целостности данных- 5%
6. Атаки с целью вызвать отказ в обслуживании – 4%
7. Вирусные атаки – 3%
8. Хищение компьютеров и носителей информации- 2 %

Причины убытков, вызванных недостаточностью уровня информационной безопасности:

1. Вирус – 70 %
2. Неработоспособность системы – 48%
3. Умышленные действия персонала – 30%
4. Стихийные бедствия – 22%
5. Действия людей, не работающих в компании – 15%
6. Неизвестные причины – 12%
7. Промышленный шпионаж – 5%

Основными *целями защиты информации* являются:

- предотвращение утечки, хищения, искажения и подделки;

- обеспечение безопасности личности, общества, государства;
- предотвращение несанкционированного ознакомления, уничтожения, искажения, копирования, блокирования информации в информационных системах;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;
- сохранение государственной тайны, конфиденциальности документированной информации;
- соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах обработки;
- сохранение возможности управления процессом обработки и пользования информацией.

Одни технологии по защите системы и обеспечению учета всех событий могут быть встроены в сам компьютер, другие – в программы.

Основными *задачами защиты информации* традиционно считаются обеспечение:
- доступности (возможность за приемлемое время получить требуемую информационную услугу);
- конфиденциальности (защищенность информации от несанкционированного ознакомления);
- целостности (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- юридической значимости (развитие нормативно-правовой базы безопасности информации в нашей стране, актуальна при необходимости обеспечения строгого учета платежных документов и любых информационных услуг).

Проблемы информационной безопасности решаются, как правило, посредством создания специализированных систем защиты информации, которые должны обеспечивать безопасность информационной системы от несанкционированного доступа к информации и ресурсам, несанкционированных и непреднамеренных вредоносных воздействий. Система защиты информации является инструментом администраторов информационной безопасности.

Система защиты информации должна выполнять следующие ***функции***:
1. Регистрация и учет пользователей, носителей информации, информационных массивов.
2. Обеспечение целостности системного и прикладного ПО и обрабатываемой информации.
3. Защита коммерческой тайны, в том числе с использованием сертифицированных средств криптозащиты;
4. Создание защищенного электронного документооборота с использованием сертифицированных средств криптопреобразования и электронной цифровой подписи.
5. Централизованное управление системой защиты информации, реализованное на рабочем месте администратора информационной безопасности.
6. Защищенный удаленный доступ мобильных пользователей на основе использования технологий виртуальных частных сетей (VPN).
7. Управление доступом.
8. Обеспечение эффективной антивирусной защиты.

Уровни защиты информационной системы

Организация защиты на *физическом уровне* должна уменьшить возможность несанкционированных действий посторонних лиц и персонала предприятия, а также снизить влияние техногенных источников.

Защита на *технологическом уровне* направлена на уменьшение возможных проявлений угроз безопасности информации, связанных с использованием некачественного программного продукта и технических средств обработки информации и некорректных действий разработчиков ПО. Система защиты на этом уровне должна быть автономной, но обеспечивать реализацию единой политики безопасности и строиться на основе использования совокупности защитных функций встроенных систем защиты ОС и систем управления БД и знаний.

На *локальном уровне* организуется разделение информационных ресурсов ИС на сегменты по степени конфиденциальности, территориальному и функциональному принципу, а также выделение в обособленный сегмент средств работы с конфиденциальной информацией.

На *сетевом уровне* должен быть организован защищенный информационный обмен между автоматизированными рабочими местами, в том числе удаленными и мобильными. Основой организации защиты может служить применение программно-аппаратных средств повышенной аутентификации и защиты от несанкционированного доступа к информации. Дополнительно могут использоваться средства построения виртуальных сетей (VPN-технологии) и криптографической защиты информации при передаче по открытым каналам.

На *пользовательском уровне* должен быть обеспечен допуск только авторизованных пользователей к работе в информационной системе, создана защитная оболочка вокруг ее элементов, а также организована индивидуальная среда деятельности каждого пользователя.

2. Угрозы информационной безопасности

Построение надежной защиты компьютерной системы невозможно без предварительного анализа возможных угроз безопасности системы. Этот анализ включает в себя:

- выявление характера хранящейся в системе информации, выделение наиболее опасных угроз (несанкционированное чтение, несанкционированное изменение и т.д.);
- определение затрат времени и средств на вскрытие системы, допустимых для злоумышленников;
- оценку ценности информации, хранящейся в системе;
- построение модели злоумышленника (определение того, от кого нужно защищаться – от постороннего лица, пользователя системы, администратора);
- оценку допустимых затрат времени, средств, ресурсов системы на организацию защиты.

Угрозами информационной безопасности называются потенциальные источники нежелательных событий, которые могут нанести ущерб ресурсам информационной системы.

Как правило, угрозы информационной безопасности различаются по способу их реализации. Исходя из этого, можно выделить следующие основные классы угроз безопасности, направленных против информационных ресурсов:

- Угрозы, реализуемые воздействием на программное обеспечение.
- Угрозы, связанные с выходом из строя технических средств системы.
- Угрозы, обусловленные человеческим фактором.

2.1. Классификация угроз

Угрозы с использованием программных средств.

Наиболее многочисленный класс угроз конфиденциальности, целостности и доступности информационных ресурсов связан с получением внутренними и внешними нарушителями логического доступа к информации с использованием возможностей, предоставляемых общесистемным и прикладным ПО.

Большинство рассматриваемых в этом классе угроз реализуется путем локальных или удаленных атак на информационные ресурсы системы внутренними и внешними нарушителями. Результатом успешного осуществления этих угроз становится несанкционированный доступ к информации системы, управляющей информации, хранящейся на рабочем месте администратора системы и т.д.

В этом классе выделяются следующие основные угрозы:

- использование чужого идентификатора посторонними, сотрудниками организации;
- несанкционированный доступ к приложению;
- внедрение вредоносного ПО;
- сбои системного и прикладного ПО;
- и тд.

Угрозы техническим средствам.

Угрозы доступности и целостности информации, хранимой, обрабатываемой и передаваемой по каналам связи, связаны с физическими повреждениями и отказами технических средств системы и вспомогательных коммуникаций. Последствия реализации данного класса угроз могут привести к полному или частичному разрушению информации, отказу в обслуживании пользователей и их запросов к системе, невозможности вывода или передачи сформированной информации. В этом классе выделяют следующие основные угрозы:

- неисправности сетевого сервера, накопительного устройства, печатающих устройств, электропитания и т.п.;
- пожар, затопление, природные катаклизмы.

Угрозы, обусловленные человеческим фактором.

Угрозы возникают вследствие умышленных или неумышленных действий персонала или посторонних лиц, приводящих к выходу из строя либо нештатной работе программных или технических средств ИС.

В этом классе выделяются следующие основные угрозы:

- ошибки операторов (при конфигурировании системы);
- ошибки пользователей;
- ошибки при профилактических работах с ПО и оборудованием.

2.2. Пути реализации угроз информационной безопасности.

Хотя угрозы могут и не осуществиться, тем не менее весьма полезно знать, что может способствовать их реализации. Среди возможных путей реализации угроз информационной безопасности рассматривают организационно-правовые, информационные, программные, физические способы.

К *организационно-правовым* способам реализации угроз относят:

- невыполнение требований законодательства в сфере информационных отношений и защиты информации;
- задержки в принятии необходимых нормативно-правовых положений и административных решений в сфере информационных отношений и защиты информации;
- нарушение режима хранения и порядка транспортировки информации и ее носителей;
- несоблюдение регламента архивирования обрабатываемой информации;
- использование на вычислительных системах несертифицированных в установленном порядке программных продуктов;
- нарушение режима доступа лиц к охранной информации;
- и т.д.

Информационные способы реализации угроз объединяют:

- хищение информации из библиотек, архивов, банков и баз данных;
- противозаконный сбор и использование информации;
- несанкционированный доступ к информационных ресурсам;
- манипулирование информацией (фальсификация, модификация, подделка, сокрытие, несанкционированное искажение и уничтожение информации);
- и т.д.

Программные способы реализации угроз включают:

- внедрение программ-вирусов;
- поставку «зараженных» компонентов ИС.

Физические способы реализации угроз:

- хищение, уничтожение или разрушение средств хранения, обработки и передачи информации, ма-

шинных или других носителей информации;
- хищение программных или аппаратных ключей;
- физическое и информационно-психологическое воздействие на персонал, работающий с защищаемой информацией.

3. Комплекс мероприятий по защите информации

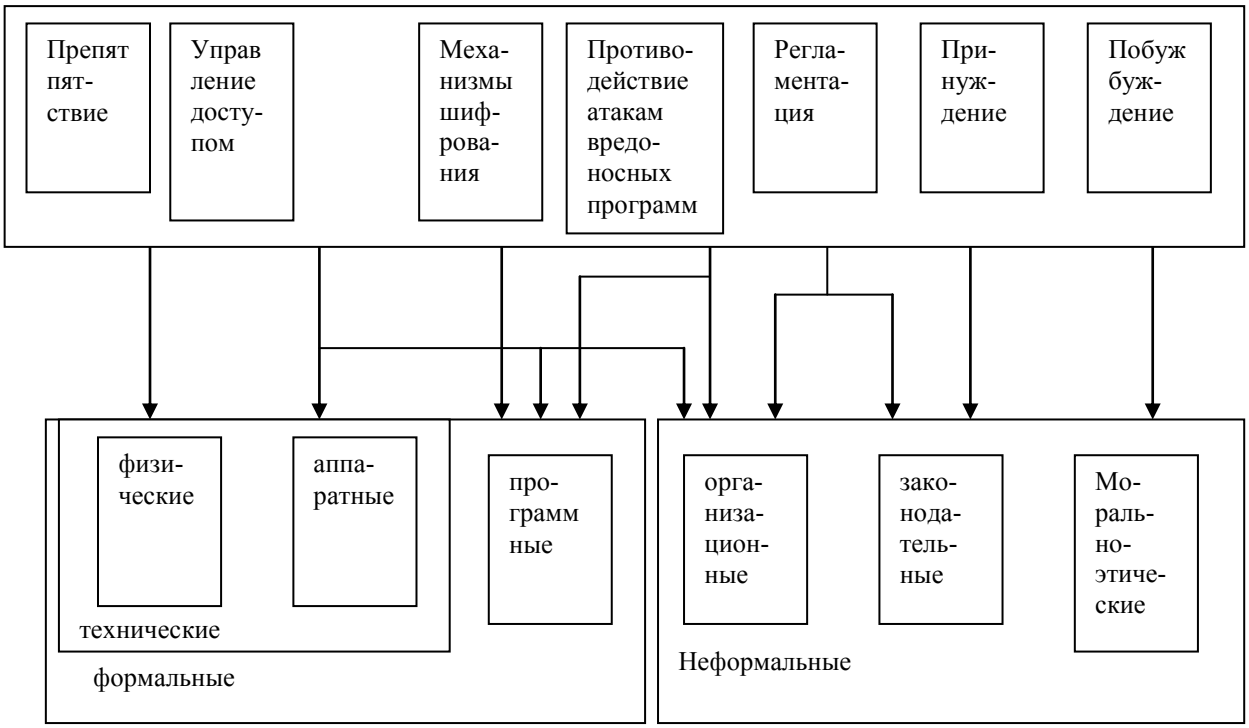
По мнению специалистов, проблема безопасности представляет собой как управленческую, так и техническую задачу и может оказывать значительное влияние на прогресс или регресс в использовании компьютерных технологий.

Защита осуществляется различными способами. Это может быть и физическая охрана, осуществляемая охранными предприятиями, и технологическая защита с использованием специализированных средств и комплексов. Защита конфиденциальной информации от несанкционированного доступа выполняется с использованием средств шифрования и без их применения.

При построении системы информационной безопасности обязателен всесторонний подход, обеспечивающий предупреждение реализаций возможных угроз информационной безопасности. Это предполагает решение следующих задач:

1. В структуре подразделения, обеспечивающего безопасность предприятия в целом, должно быть специализированное инженерно - техническое подразделение по информационной безопасности.
2. Подразделение по информационной безопасности, изучив структуры, характеристики и точки уязвимости информационных систем и сетей связи, должно определить предварительную *политику информационной безопасности*. *Политика безопасности* – представляет собой набор законов, правил и практического опыта, на основе которых строятся управление, защита и распределение конфиденциальной информации.

Методы и средства обеспечения безопасности информации в ИС схематически можно представить:



Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.)

Управление доступом – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации. Включает в себя следующие функции защиты: идентификацию пользователей; опознание объекта или субъекта по предъявляемому ему идентификатору; проверку полномочий; разрешение и создание условий работы в пределах установленного регламента; регистрацию обращений к защищаемым ресурсам; реагирование при попытках несанкционированных действий.

Механизмы шифрования – криптографическое закрытие информации. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Противодействие атакам вредоносных программ предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ.

Регламентация – создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени.

Принуждение – метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение – метод защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Вся совокупность технических средств подразделяется на аппаратные и физические.

Аппаратные средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала, материальных средств и финансов, информации от противоправных действий (средства – замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.).

Программные средства – это специальные программы и программные комплексы, предназначенные для защиты информации в ИС. Из средств ПО можно выделить программные средства, реализующие механизмы шифрования (криптографии).

Организационные средства осуществляют регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты включают всевозможные нормы поведения, которые традиционно сложились ранее, складываются по мере распространения ИС и ИТ в стране и в мире или специально разрабатываются. Эти нормы могут быть неписанными.

4. Компьютерные вирусы, их классификация. Антивирусные программные средства

4.1. Вирусы. Определение. Классификация

Компьютерный вирус - специальная программа (некоторая совокупность выполняемого кода/инструкций), способная самопроизвольно присоединяться к другим программам; создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты/ресурсы компьютерных систем, сетей и т.д. без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.

При запуске зараженных программ выполняются различные нежелательные действия:

- порчу файлов и каталогов;
- искажение результатов вычислений;
- засорение или стирание памяти;
- создание помех в работе компьютера.

Наличие вирусов проявляется в разных ситуациях:

- Некоторые программы перестают работать или начинают работать некорректно.
- На экран выводятся посторонние сообщения, сигналы и другие эффекты.
- Работа компьютера существенно замедляется.
- Структура некоторых файлов оказывается испорченной.

Имеются несколько признаков классификации существующих вирусов:

- по среде обитания;
- по особенности алгоритма;
- по способу заражения;
- по деструктивным (разрушающим) возможностям.

1. По ***среде обитания*** различают файловые, загрузочные, макро- и сетевые вирусы.
   1.1. ***Файловые вирусы*** — наиболее распространенный тип вирусов. Эти вирусы внедряются в выполняемые файлы, создают файлы-спутники (companion-вирусы) или используют особенности организации файловой системы (link-вирусы).
   1.2. ***Загрузочные вирусы*** записывают себя в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий системный загрузчик винчестера (Master Boot Record). Начинают работу при загрузке компьютера и обычно становятся резидентными.
   1.3. ***Макровирусы з***аражают файлы широко используемых пакетов обработки данных. Эти вирусы представляют собой программы, написанные на встроенных в эти пакеты языках программирования. Наибольшее распространение получили макровирусы для приложений Microsoft Office.
   1.4. ***Сетевые вирусы*** используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. Полноценные компьютерные вирусы при этом обладают возможностью запустить на удаленном компьютере свой код на выполнение.

На практике существуют разнообразные сочетания вирусов — например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные секторы дисков, или сетевые макровирусы, которые заражают редактируемые документы и рассылают свои копии по электронной почте.

Как правило, каждый вирус заражает файлы одной или нескольких ОС. Многие загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

2. По ***особенностям алгоритма*** выделяют:

При создании вирусов часто используются нестандартные приемы. Их применение должно максимально затруднить обнаружение и удаление вируса.

   2.1. ***компаньон-вирусы*** (companion) - это вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для EXE-файлов файлы-спутники, имеющие то же самое имя, но с расширением .COM, например, для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM-файл и никак не изменяет EXE-файл. При запуске такого файла DOS первым обнаружит и выполнит COM-файл, т.е. вирус, который затем запустит и EXE-файл.
   2.2. ***вирусы-“черви” (worm)*** - вирусы, которые распространяются в компьютерной сети и, так же как и компаньон-вирусы, не изменяют файлы или сектора на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти). К счастью, в вычислительных сетях IBM-компьютеров такие вирусы пока не завелись.
   2.3. ***“паразитические”*** - все вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. В эту группу относятся все вирусы, которые не являются “червями” или “компаньон”.
   2.4. “***стелс”-вирусы*** (вирусы-невидимки, stealth), Стелс-алгоритмы представляют собой весьма совершенные программы, которые позволяют вирусам полностью или частично скрыть свое присутствие. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат эти объекты, либо подставляют вместо себя незараженные участки информации. Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие “обманывать” резидентные антивирусные мониторы.
   2.5. ***Полиморфные вирусы*** (самошифрующиеся или вирусы-призраки, polymorphic) — это трудно

выявляемые вирусы, не имеющие постоянного участка кода. В общем случае два образца одного и того же вируса не имеют совпадений. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

3. По ***способу заражения*** и ***распространения*** различают.
   3.1. *Резидентные вирусы* при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть способны оставлять свои копии в ОЗУ, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них (например, обращение к файлам или дискам). Эти вирусы активны в памяти не только в момент работы зараженной программы, но и после. Резидентные копии таких вирусов жизнеспособны до перезагрузки ОС, даже если на диске уничтожены все зараженные файлы. Если резидентный вирус является также загрузочным и активизируется при загрузке ОС, то даже форматирование диска при наличии в памяти этого вируса его не удаляет.
   К разновидности резидентных вирусов следует отнести также макровирусы, поскольку они постоянно присутствуют в памяти компьютера во время работы зараженного редактора.
   3.2. *Нерезидентные вирусы* не заражают память компьютера и являются активными ограниченное время.
   3.3. *Троянские программы* получили свое название по аналогии с троянским конем. Назначение этих программ — имитация каких-либо полезных программ, новых версий популярных утилит или дополнений к ним. При их записи пользователем на свой компьютер троянские программы активизируются и выполняют нежелательные действия.
   3.4. Разновидностью троянских программ являются *утилиты скрытого администрирования*. По своей функциональности и интерфейсу они во многом напоминают системы администрирования компьютеров в сети, разрабатываемые и распространяемые различными фирмами — производителями программных продуктов. При инсталляции эти утилиты самостоятельно устанавливают на компьютере систему скрытого удаленного управления. В результате возникает возможность скрытого управления этим компьютером. Реализуя заложенные алгоритмы, утилиты без ведома пользователя принимают, запускают или отсылают файлы, уничтожают информацию, перезагружают компьютер и т. д. Возможно использование этих утилит для обнаружения и передачи паролей и ной конфиденциальной информации, запуска вирусов, уничтожения данных.
   3.5. К ***Intended-вирусам*** относятся программы, которые не способны размножаться из-за существующих в них ошибок. К этому классу также можно отнести вирусы, которые размножаются только один раз. Заразив какой-либо файл, они теряют способность к дальнейшему размножению через него.

4. По ***деструктивным (разрушительным) возможностям*** вирусы разделяются на:
   4.1. ***безвредные***, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
   4.2. ***Неопасные***, влияние которых ограничивается уменьшением свободной памяти на диске, замедлением работы компьютера, графическими, звуковыми э и др. эффектами;
   4.3. ***опасные***, которые потенциально могут привести к нарушениям в структуре файлов и сбоям в работе компьютера;
   4.4. ***очень опасные***, в алгоритм которых специально заложены процедуры уничтожения данных и возможность обеспечивать быстрый износ движущихся частей механизмов путем ввода в резонанс и разрушения головок чтения/записи некоторых НЖМД.

4.2. Антивирусные программы

Для борьбы с вирусами существуют программы, которые можно разбить на основные группы:
- мониторы,
- детекторы,
- доктора,
- ревизоры
- и вакцины.

Программы-мониторы (программы-фильтры) располагаются резидентно в ОП компьютера, перехватывают и сообщают пользователю об обращениях ОС, которые используются вирусами для размножения и нанесения ущерба. Пользователь имеет возможность разрешить или запретить выполнение этих обращений. К преимуществу таких программ относится возможность обнаружения неизвестных вирусов. Использование программ-фильтров позволяет обнаруживать вирусы на ранней стадии заражения компьютера. Недостатками программ являются невозможность отслеживания вирусов, обращающихся непосредственно к BIOS, а также загрузочных вирусов, активизирующихся до запуска антивируса при загрузке DOS, и частая выдача запросов на выполнение операций.

Программы-детекторы проверяют, имеется ли в файлах и на дисках специфическая для данного вируса комбинация байтов. При ее обнаружении выводится соответствующее сообщение. Недостаток — возможность защиты только от известных вирусов.

Программы-доктора восстанавливают зараженные программы путем удаления из них тела вируса. Обычно эти программы рассчитаны на конкретные типы вирусов и основаны на сравнении последовательности кодов, содержащихся в теле вируса, с кодами проверяемых программ. Программы-доктора необходимо периодически обновлять с целью получения новых версий, обнаруживающих новые виды вирусов.

Программы-ревизоры анализируют изменения состояния файлов и системных областей диска. Проверяют состояние загрузочного сектора и таблицы FAT; длину, атрибуты и время создания файлов; контрольную сумму кодов. Пользователю сообщается о выявлении несоответствий.

Программы-вакцины модифицируют программы и риски так, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает программы или диски уже зараженными. Существующие антивирусные программы в основном относятся к классу гибридных (детекторы-доктора, доктора-ревизоры и пр.).

В России наибольшее распространение получили антивирусные программы Лаборатории Касперского (Anti-IViral Toolkit Pro) и ДиалогНаука (Adinf,Dr.Web). Антивирусный пакет AntiViral Toolkit Pro (AVP) включает AVP Сканер, резидентный сторож AVP Монитор, программу администрирования установленных компонентов. Центр управления и ряд других. AVP Сканер помимо традиционной проверки выполняемых файлов и файлов документов обрабатывает базы данных электронной почты. Использование сканера позволяет выявить вирусы в упакованных и архивированных файлах (не защищенных паролями). Обнаруживает к удаляет макровирусы, полиморфные, стеле, троянские, а также ранее неизвестные вирусы. Это достигается, например, за счет использования эвристических анализаторов. Такие анализаторы моделируют работу процессора и выполняют анализ действий диагностируемого файла. В зависимости от этих действий и принимается решение о наличии вируса.

Монитор контролирует типовые пути проникновения вируса, например операции обращения к файлам и секторам.

AVP Центр управления — сервисная оболочка, предназначенная для установки времени запуска сканера, автоматического обновления компонент пакета и др.

При заражении или при подозрении на заражение компьютера вирусом необходимо:

- оценить ситуацию и не предпринимать действий, приводящих к .потере информации;
- перезагрузить ОС компьютера. При этом использовать специальную, заранее созданную и защищенную от записи системную дискету. В результате будет предотвращена активизация загрузочных и резидентных вирусов с жесткого диска компьютера;
- запустить имеющиеся антивирусные программы, пока не будут обнаружены и удалены все вирусы. В случае невозможности удалить вирус и при наличии в файле ценной информации произвести архивирование файла и подождать выхода новой версии антивируса. После окончания перезагрузить компьютер.