Информационная безопасность.

Защита информации.

Информационная безопасность - защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Цель мероприятий в области информационной безопасности – защитить интересы субъектов информационных отношений. Интересы эти многообразны, но все они концентрируются вокруг трех основных аспектов:

- **доступность**;
- **целостность**;
- **конфиденциальность**

- **Доступность** – это возможность за приемлемое время получить требуемую информационную услугу.
- **Целостностью** - актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.
- **Конфиденциальность** – это защита от несанкционированного доступа к информации

Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку, – **злоумышленником.**

Потенциальные злоумышленники называются **источниками угрозы**.

Классификация угроз

- **по аспекту информационной безопасности** (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
- **по компонентам информационных систем**, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- **по способу осуществления** (случайные/ преднамеренные действия природного/ техногенного характера);
- **по расположению источника угроз** (внутри/вне рассматриваемой ИС).

Угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются **непреднамеренные ошибки** штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

По некоторым данным, до 65% потерь – следствие непреднамеренных ошибок.

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе.

Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками – **максимальная автоматизация и строгий контроль.**

Другие угрозы доступности

- **отказ пользователей**;
- **внутренний отказ** информационной системы;
- **отказ поддерживающей инфраструктуры**.

Отказ пользователей

- Нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- Невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
- Невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации).

Внутренние отказы

- Отступление (случайное или умышленное) от установленных правил эксплуатации;
- Выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- Ошибки при (пере)конфигурировании системы;
- Отказы программного и аппаратного обеспечения;
- Разрушение данных;
- Разрушение или повреждение аппаратуры.

Отказ поддерживающей инфраструктуры

- Нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- Разрушение или повреждение помещений;
- Невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

«Обиженные" сотрудники

- Весьма опасны так называемые **"обиженные" сотрудники** – нынешние и бывшие. Как правило, они стремятся нанести вред организации-"обидчику", например:
  - испортить оборудование;
  - встроить логическую бомбу, которая со временем разрушит программы и/или данные;
  - удалить данные.
- Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Стихийные бедствия

стихийные бедствия и события, воспринимаемые как стихийные бедствия,– грозы, пожары, наводнения, землетрясения, ураганы.

По статистике, на долю огня, воды и тому подобных "злоумышленников" (среди которых самый опасный – перебой электропитания) приходится 13% потерь, нанесенных информационным системам.

Вредоносное программное обеспечение

- Вредоносная функция;
- Способ распространения;
- Внешнее представление.
- Т.н. "бомбы" предназначаются для:
  - внедрения другого вредоносного ПО;
  - получения контроля над атакуемой системой;
  - агрессивного потребления ресурсов;
  - изменения или разрушения программ и/или данных.

По механизму распространения различают:

- **вирусы** – код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
- **"черви"** – код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

Основные угрозы целостности

- Статическая целостность
  - ввести неверные данные;
  - изменить данные.
- Динамическая целостность
  - нарушение атомарности транзакций,
  - переупорядочение,
  - кража,
  - дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.).
- Соответствующие действия в сетевой среде называются активным прослушиванием.

Основные угрозы конфиденциальности

- Служебная информация (пароли)
- Предметная информация
  - Перехват данных - Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям
  - Маскарад-представление за другого
  - Злоупотребление полномочиями

Элементы политики безопасности

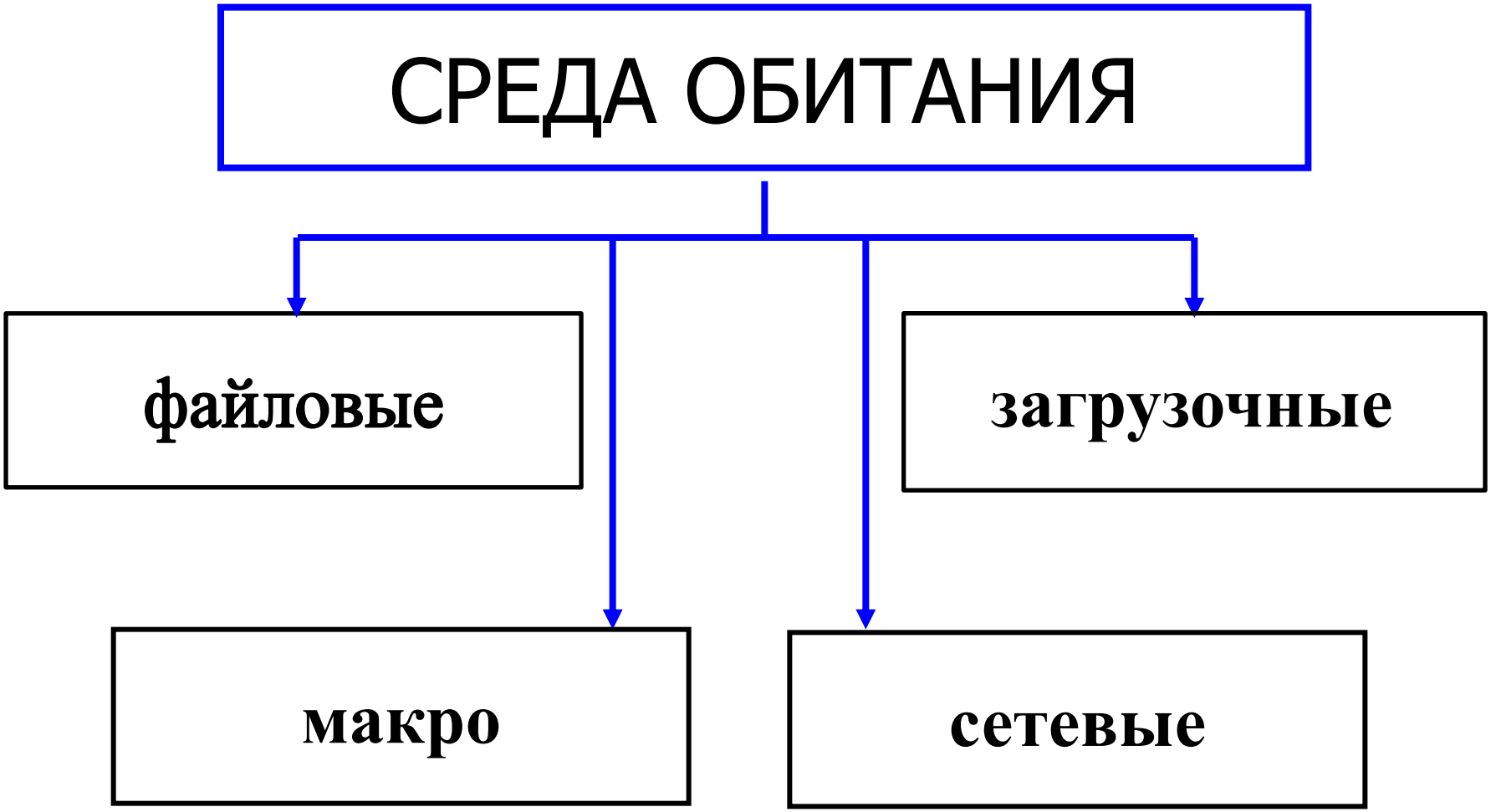
- произвольное управление доступом
  - метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. (может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту)
- безопасность повторного использования объектов
  - для областей оперативной памяти и дисковых блоков и магнитных носителей в целом

- метки безопасности
  - Метка субъекта описывает его благонадежность, метка объекта – степень конфиденциальности содержащейся в нем информации.
- принудительное управление доступом
  - Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. Смысл сформулированного правила понятен – читать можно только то, что положено.

- **идентификация и аутентификация**;
- **защита данных пользователя**;
- **защита функций безопасности** (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
- **управление безопасностью** (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
- **аудит безопасности** (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);

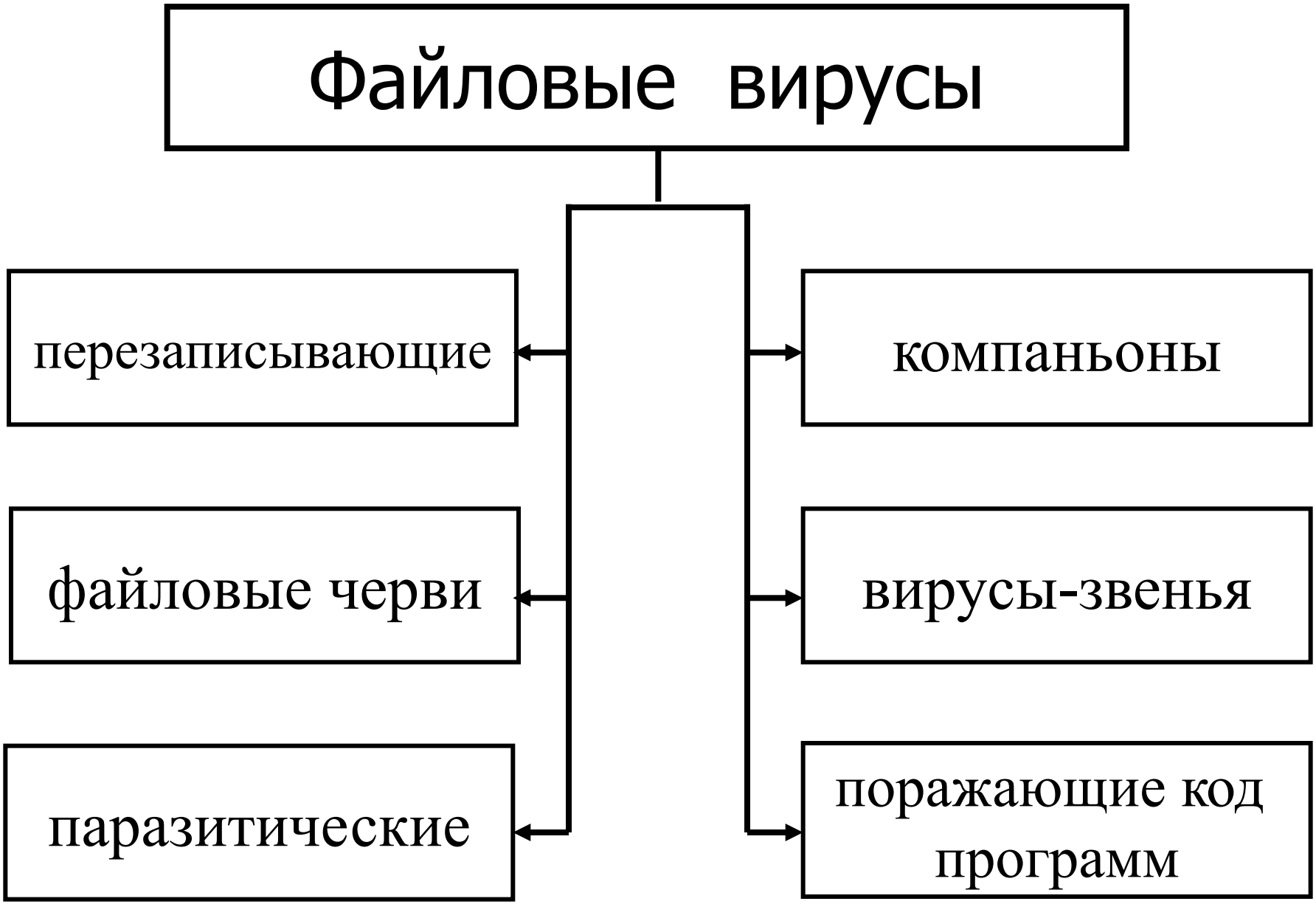
- **доступ к объекту оценки**;
- **приватность** (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
- **использование ресурсов** (требования к доступности информации);
- **криптографическая поддержка** (управление ключами);
- **связь** (аутентификация сторон, участвующих в обмене данными);
- **доверенный маршрут/канал** (для связи с сервисами безопасности).

Компьютерные вирусы и их виды


СРЕДА ОБИТАНИЯ
файловые
загрузочные
макро
сетевые

ФАЙЛОВЫЕ ВИРУСЫ

Внедряются в программы и активизируются при их запуске. После запуска заражённой программой могут заражать другие файлы до момента выключения компьютера или перезагрузки операционной системы.


Файловые вирусы
перезаписывающие
файловые черви
паразитические
компаньоны
вирусы-звенья
поражающие код программ

По способу заражения файловые вирусы разделяются на:

1. ***Перезаписывающие вирусы.*** Записывают свое тело вместо кода программы, не изменяя название исполняемого файла, вследствие чего программа перестает запускаться.
2. ***Вирусы-компаньоны.*** Создают свою копию на месте заражаемой программы, но не уничтожают оригинальный файл, а переименовывают его или перемещают. При запуске программы вначале выполняется код вируса, а затем управление передается оригинальной программе.
3. ***Файловые черви*** создают собственные копии с привлекательными для пользователя названиями в надежде, что он их запустит.
4. ***Вирусы-звенья*** не изменяют код программы, а заставляют ОС выполнить свой код, изменяя адрес местоположения на диске зараженной программы, на собственный адрес.

По способу заражения файловые вирусы разделяются на:

5. ***Паразитические вирусы*** изменяют содержимое файла, добавляя в него свой код. При этом зараженная программа сохраняет полную или частичную работоспособность. Код может внедряться в начало, середину или конец программы.

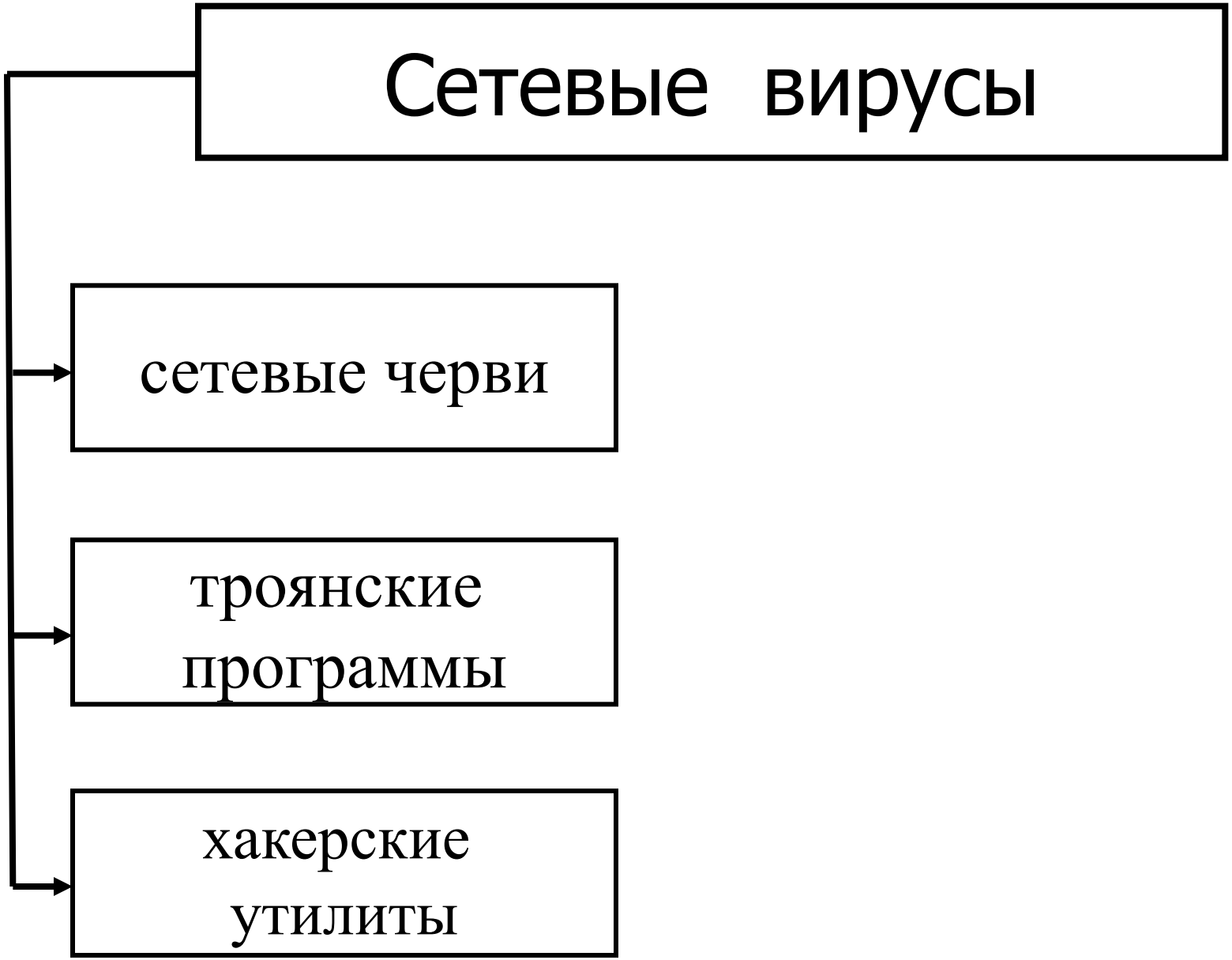
6. ***Вирусы, поражающие исходный код программы.*** Вирусы данного типа поражают исходный код программы или ее компоненты (.OBJ, .LIB, .DCU). После компиляции программы оказываются встроенными в неё.

МАКРОВИРУСЫ

Заражают файлы документов, например текстовых. После загрузки заражённого документа в текстовый редактор макровирус постоянно присутствует в оперативной памяти компьютера и может заражать другие документы. Угроза заражения прекращается только после закрытия текстового редактора.

СЕТЕВЫЕ ВИРУСЫ

Могут передавать по компьютерным сетям свой программный код и запускать его на компьютерах, подключённых к этой сети. Заражение сетевым вирусом может произойти при работе с электронной почтой или при «путешествиях» по Всемирной паутине.


Сетевые вирусы
сетевые черви
троянские программы
хакерские утилиты

Сетевые вирусы

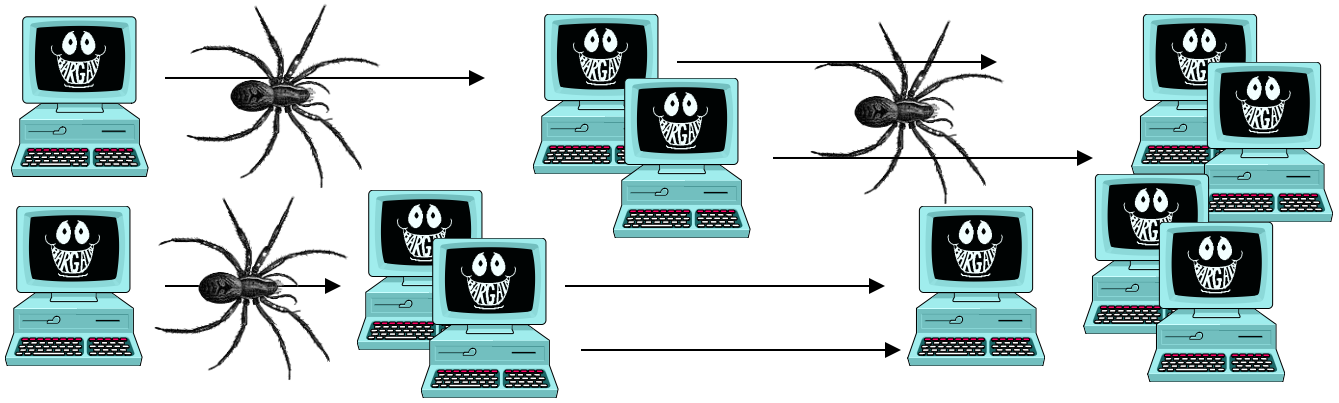
Сетевые черви – программы, распространяющие свои копии по локальным или глобальным сетям с целью:

- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие

Сетевые вирусы

Троянские программы. Эти программы осуществляют различные несанкционированные пользователем действия:

- сбор информации и ее передача злоумышленникам;
- разрушение информации или злонамереная модификация;
- нарушение работоспособности компьютера;
- использование ресурсов компьютера в неблаговидных целях.

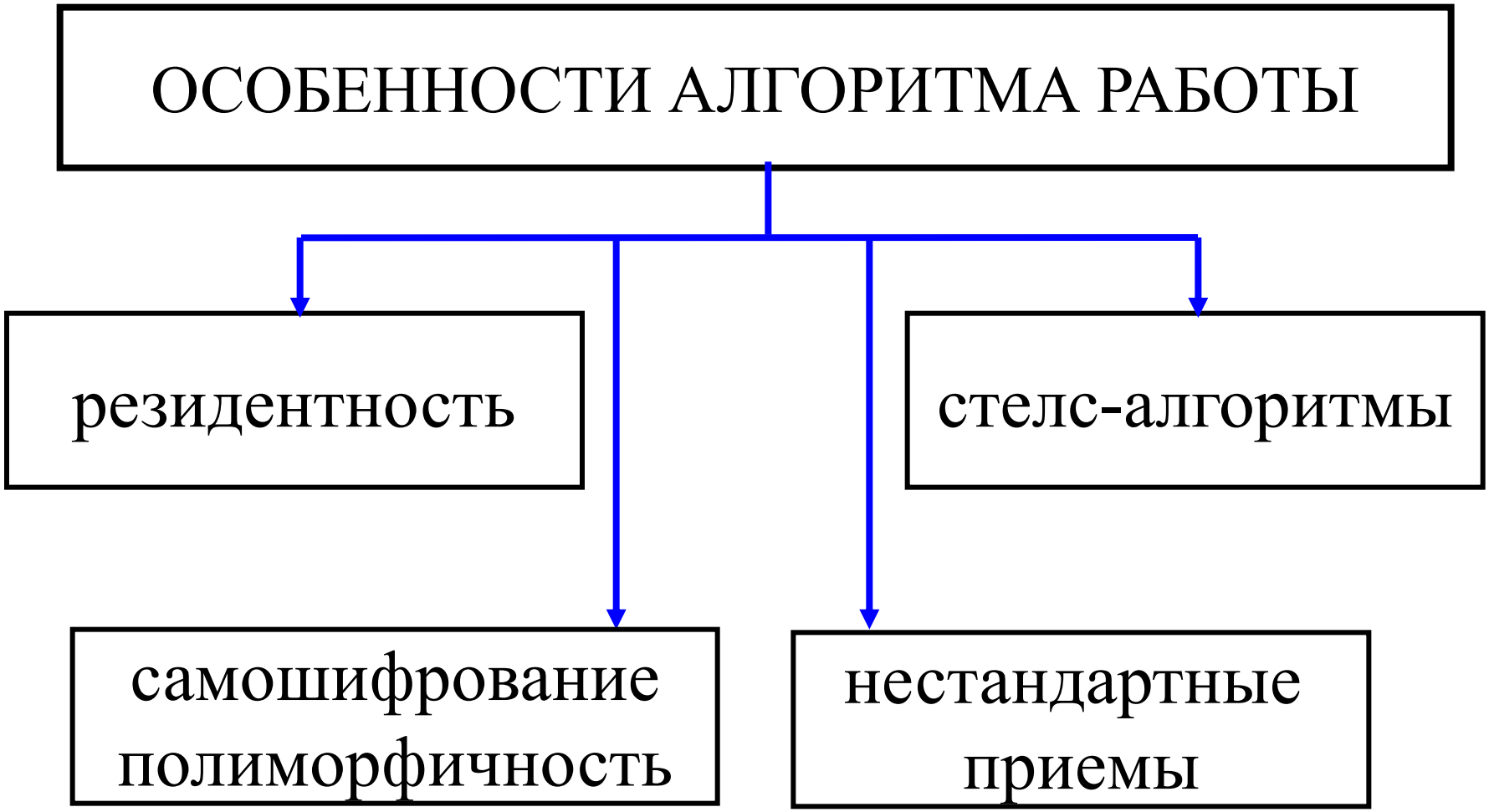


Сетевые вирусы

Хакерские утилиты и прочие вредоносные программы.

К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ;
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удаленным компьютерам.


ОСОБЕННОСТИ АЛГОРИТМА РАБОТЫ
резидентность
стелс-алгоритмы
самошифрование
полиморфичность
нестандартные
приемы

Особенности алгоритма работы

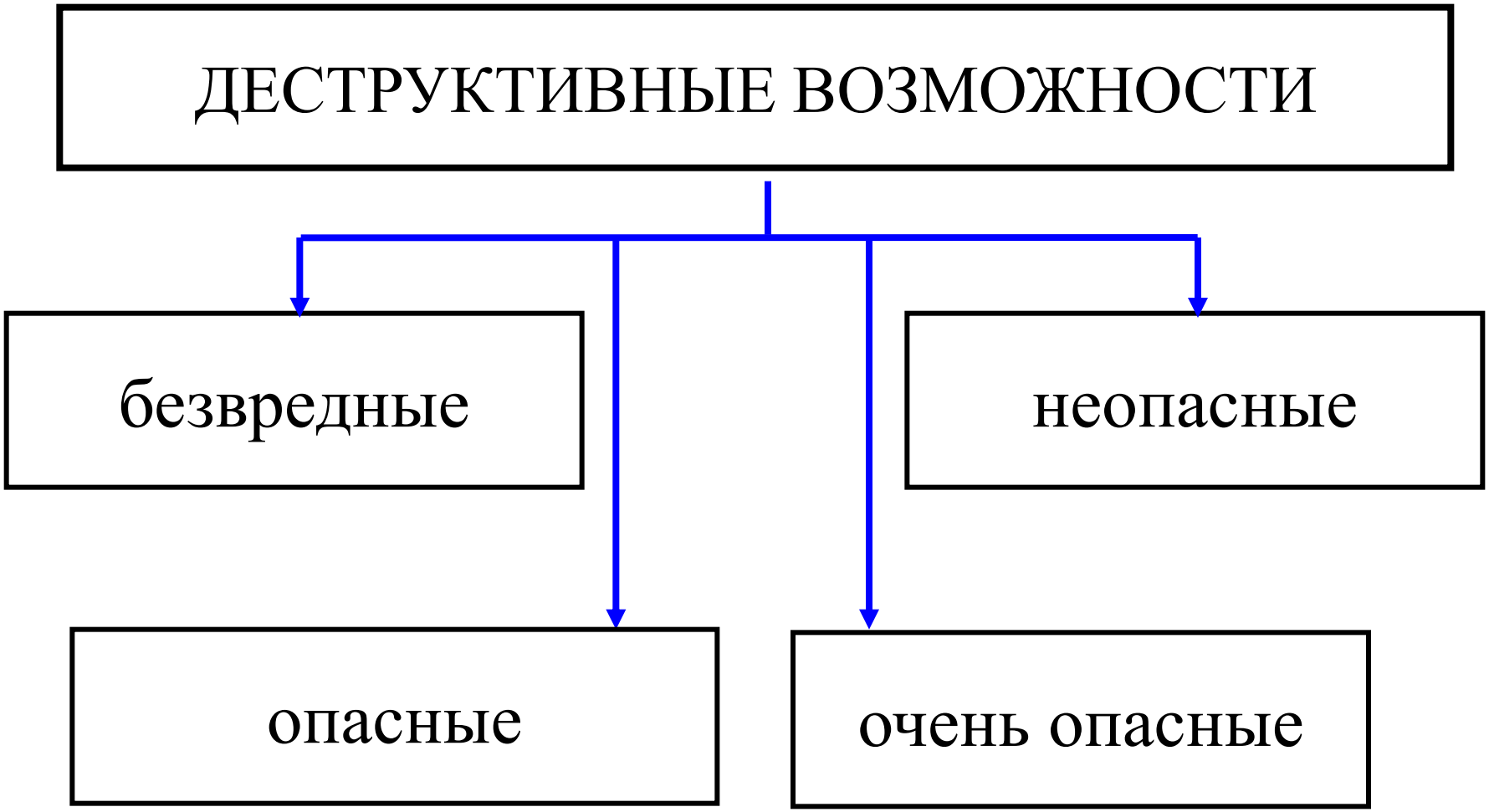
Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. Резидентными можно считать макро-вирусы, поскольку они постоянно присутствуют в памяти компьютера на все время работы зараженного редактора.

Использование ***стел-алгоритмов*** позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации.

Особенности алгоритма работы

Самошифрование **и** ***полиморфичность*** используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфик-вирусы - это достаточно труднообнаружимые 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.

Различные ***нестандартные приемы*** часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре ОС, защитить от обнаружения свою резидентную копию, затруднить лечение от вируса и т.д.


ДЕСТРУКТИВНЫЕ ВОЗМОЖНОСТИ
безвредные
неопасные
опасные
очень опасные

По деструктивным особенностям вирусы можно разделить на:

- ***безвредные,*** т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- ***неопасные***, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
- ***опасные вирусы***, которые могут привести к серьезным сбоям в работе компьютера;
- ***очень опасные***, в алгоритмах работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов - вводить в резонанс и разрушать головки некоторых типов винчестеров.

Пути проникновения вирусов

- ☑ Глобальная сеть Internet
- ☑ Электронная почта
- ☑ Локальная сеть
- ☑ Компьютеры «Общего назначения»
- ☑ Пиратское программное обеспечение
- ☑ Ремонтные службы
- ☑ Съемные накопители

Пути проникновения вирусов

Глобальная сеть Интернет

Основным источником вирусов на сегодняшний день является глобальная сеть Internet. Возможно заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта, а ничего не подозревающие пользователи зайдя на такой сайт рискуют заразить свой компьютер.

Пути проникновения вирусов

Электронная почта

Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов.

Пути проникновения вирусов

Локальные сети

Третий путь «быстрого заражения» - локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере

На следующий день пользователи при входе в сеть запускают зараженные файлы с сервера, и вирус, таким образом, получает доступ на компьютеры пользователей.

Пути проникновения вирусов

Персональные компьютеры «общего пользования»

Опасность представляют также компьютеры, установленные в учебных заведениях. Если один из студентов принес на своих носителях вирус и заразил какой-либо учебный компьютер, то очередную «заразу» получат и носители всех остальных студентов, работающих на этом компьютере.

То же относится и к домашним компьютерам, если на них работает более одного человека.

Пиратское программное обеспечение

Нелегальные копии программного обеспечения, как это было всегда, являются одной из основных «зон риска».Часто пиратские копии на дисках содержат файлы, зараженные самыми разнообразными типами вирусов.

Пути проникновения вирусов

Ремонтные службы

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре. Ремонтники — тоже люди, и некоторым из них свойственно наплевательское отношение к элементарным правилам компьютерной безопасности.

Съемные накопители

В настоящее время большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны.

Антивирусная программа – это специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Классификация антивирусных программ:

Программы-детекторы позволяют обнаружить файлы, зараженные каким-либо известным вирусом. Данные программы проводят только проверку компьютера на наличие вирусов. Лечить данные программы не могут.

Программы-доктора позволяют не только обнаружить файлы, зараженные известным вирусом, но и произвести их лечение. При лечении зараженных файлов программа-доктор удаляет тело вируса из файла, т.е. восстанавливает файл в том состоянии, в котором он находился до заражения вирусом.

Программы-ревизоры работают следующим образом. При своем первом запуске они запоминают сведения о состоянии программ и системных областей диска компьютера, в которые входят загрузочные секторы, таблицы размещения файлов, корневой каталог. Предполагается, что в этот момент программы и системные области дисков не заражены. Затем при последующих проверках компьютера программы-ревизоры сравнивают состояние файлов и системных областей диска с исходным. Если произошли изменения, характерные для действий вируса, то они сообщают об этом пользователю.

Программы-фильтры, постоянно находясь в памяти компьютера, следят за действиями, которые выполняются на компьютере. При появлении действий, указывающих на наличие вирусов, они сообщают об этом пользователю. К этим действиям можно отнести изменение файлов с расширением COM и EXE, снятие с файлов атрибута "только для чтения", прямая запись на диск, форматирование диска, установка "резидентной" (постоянно находящейся в оперативной памяти) программы.

Программы-вакцины – это программы, предотвращающие заражение файлов. Сущность действия данных программ заключается в том, что они изменяют файлы специальным образом. Причем это не отражается на работе, но вирус воспринимает эти файлы как зараженные и не внедряется в них. В настоящее время данный вид программ практически не используется.

Рейтинг антивирусных программ по версии сайта www.compbegin.ru