

***Информация как объект
защиты. Методы защиты
информации. Правовые
аспекты.***

*

Екатеринбург, 2020



* Понятие защиты информации

Защита данных, защита информации [data protection] - совокупность мер, обеспечивающих защиту прав собственности владельцев информационной продукции, в первую очередь - программ, баз и банков данных от несанкционированного доступа, использования, разрушения или нанесения ущерба в какой-либо иной форме.



Защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Виды защиты информации



Информационная безопасность — это состояние защищённости информационной среды.

В вычислительной технике понятие безопасности подразумевает

- надёжность работы компьютера,
- сохранность ценных данных,
- защиту информации от внесения в нее изменений неуполномоченными лицами,
- сохранение тайны переписки в электронной связи.

Во всех цивилизованных странах на безопасности граждан стоят законы, но в вычислительной технике правоприменительная практика пока не развита, а законотворческий процесс не успевает за развитием технологий, и надёжность работы компьютерных систем во многом опирается на меры самозащиты.



* Правовые аспекты защиты информации.

- * На сегодня защита данных обеспечивается законодательными актами на международном и государственном уровне.
- * В России такими законодательными актами служат закон "Об информации, информатизации и защите информации" (базовый) и закон "О правовой охране программ для электронных вычислительных машин и баз данных", выпущенные соответственно в 1995 и 1992 гг.

* Правовые аспекты защиты информации.

В настоящее время некоторые статьи УК РФ также направлены на защиту информации. В частности глава 28. УК «Преступления в сфере компьютерной информации» состоит из трех статей:

- * Ст. 272. «Неправомерный доступ к компьютерной информации».
- * Эта статья, которая, как и последующие, состоит из 2 частей, содержит достаточно много признаков, обязательных для объекта, объективной и субъективной сторон состава преступления. Непосредственным объектом ее являются общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ, их системы или сети.

Правовые аспекты защиты информации.

Состав преступления сформулирован как материальный, причем если деяние в форме действия определено однозначно (неправомерный доступ к охраняемой законом компьютерной информации), то последствия; хотя и обязательны, могут быть весьма разнообразны:

- * 1) уничтожение информации,
- * 2) ее блокирование,
- * 3) модификация,
- * 4) копирование,
- * 5) нарушение работы ЭВМ,
- * 6) то же -- для системы ЭВМ

* Ст.273. «Создание, использование и распространение вредоносных программ для ЭВМ».

* Непосредственным объектом данного преступления являются общественные отношения по безопасному использованию ЭВМ, ее программного обеспечения и информационного содержания. Статья предусматривает наказания при совершении одного из действий:

- * 1) создание программ для ЭВМ, заведомо приводящих (приводящей) к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы аппаратной части;
- * 2) внесение в существующие программы изменений, обладающих аналогичными свойствами;
- * 3) использование двух названных видов программ;
- * 4) их распространение;
- * 5) использование машинных носителей с такими программами;
- * 6) распространение таких носителей.

* Ст.274. «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

* Целью данной статьи является предупреждение неисполнения пользователями своих профессиональных обязанностей, влияющих на сохранность хранимой и перерабатываемой информации. Непосредственный объект преступления, предусмотренного этой статьей, - отношения по соблюдению правил эксплуатации ЭВМ, системы или их сети, т. е. конкретно аппаратно-технического комплекса.

Под таковыми правилами понимаются, во-первых, **Общероссийские временные санитарные нормы** и правила для работников вычислительных центров, во-вторых, техническая документация на приобретаемые компьютеры, в-третьих, конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка

Законодательная база информационной безопасности в России.

- * В то же время с помощью блока специальных законов регулируется информационная безопасность государства, общества и личности. Среди этих законов:
- * · Закон «О средствах массовой информации» от 27.12.91 г. №2124-1;
- * · Закон «О Федеральных органах правительственной связи и информации» от 19.02.92 №4524-1;
- * · Закон «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.92 года №3523-1;
- * · Закон «О правовой охране топологий интегральных микросхем» от 23.09.92 г. №3526-1;
- * · Закон «О государственной тайне» от 21 июля 1993 г. №5485-1;
- * · Закон «Об обязательном экземпляре документов» от 29.12.94 г. №77-ФЗ;
- * · Закон «Об информации, информатизации и защите информации» от 20.02.95 года №24-ФЗ;
- * · Закон «О внешней разведке» от 10.01.96 г. №5-ФЗ;
- * · Закон «Об участии в международном информационном обмене» от 5.06.1996 г. №85-ФЗ;
- * · Закон «О Государственной автоматизированной системе Российской Федерации «Выборы» №20-ФЗ от 10 января 2003 г.

* Несанкциониро доступ. Техническая э



Несанкционированный доступ - действия, нарушающие установленный порядок доступа или правила разграничения, доступ к программам и данным, который получают абоненты, которые не прошли регистрацию и не имеют права на ознакомление или работу с этими ресурсами.

Для предотвращения несанкционированного доступа осуществляется контроль доступа.



Защита с использованием паролей

Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются *пароли*.

Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль.

Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам.

При этом может производиться регистрация всех попыток несанкционированного доступа.



Защита с использованием пароля используется при загрузке операционной системы

Вход по паролю может быть установлен в программе BIOS Setup, компьютер не начнет загрузку операционной системы, если не введен правильный пароль.

Преодолеть такую защиту нелегко.

От несанкционированного доступа могут быть защищены

- каждый диск,
- каждая папка,
- каждый файл локального компьютера.

Для них могут быть установлены определенные права доступа

- полный доступ,
- возможность внесения изменений,
- только чтение,
- запись и др.

Права могут быть различными для различных пользователей

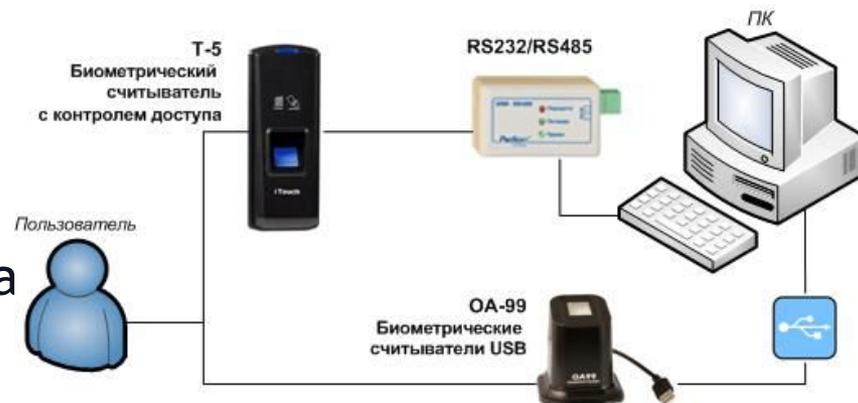
Биометрические системы защиты

В настоящее время для защиты от несанкционированного доступа к информации все более часто используются *биометрические системы идентификации*.

Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными.

К биометрическим системам защиты информации относятся системы идентификации:

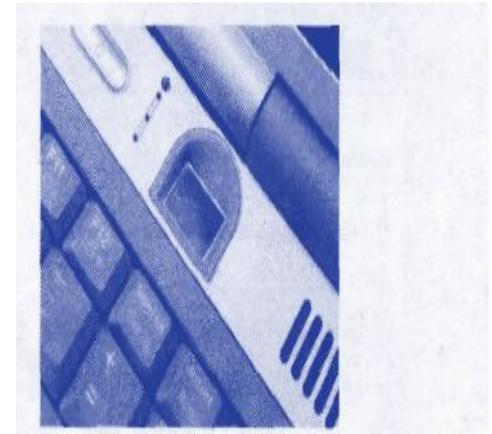
- по отпечаткам пальцев;
- по характеристикам речи;
- по радужной оболочке глаза
- по изображению лица;
- по геометрии ладони руки.



Идентификация по отпечаткам пальцев

Оптические сканеры считывания отпечатков пальцев устанавливаются на ноутбуки, мыши, клавиатуры, флэш-диски, а также применяются в виде отдельных внешних устройств и терминалов (например, в аэропортах и банках).

Если узор отпечатка пальца не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен.



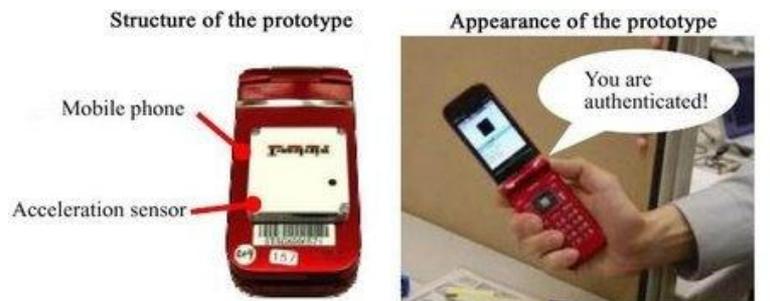
Оптический сканер отпечатка пальца, вмонтированный в ноутбук



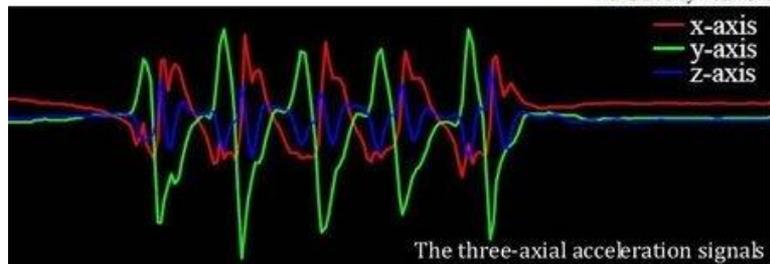
Идентификация по характеристикам речи

Идентификация человека по голосу — один из традиционных способов распознавания, интерес к этому методу связан и с прогнозами внедрения голосовых интерфейсов в операционные системы.

Голосовая идентификация бесконтактна и существуют системы ограничения доступа к информации на основании частотного анализа речи.



Translated by Tech-On!



Идентификация по радужной оболочке глаза



Радужная оболочка глаза является уникальной для каждого человека биометрической характеристикой.

Изображение глаза выделяется из изображения лица и на него накладывается специальная маска штрих-кодов. Результатом является матрица, индивидуальная для каждого человека.

Для идентификации по радужной оболочке глаза применяются специальные сканеры, подключенные к компьютеру.

Идентификация по изображению лица

Для идентификации личности часто используются технологии распознавания по лицу. Распознавание человека происходит на расстоянии.

Идентификационные признаки учитывают форму лица, его цвет, а также цвет волос. К важным признакам можно отнести также координаты точек лица в местах, соответствующих смене контраста (брови, глаза, нос, уши, рот и овал).

В настоящее время начинается выдача новых загранпаспортов, в микросхеме которых хранится цифровая фотография владельца.



Идентификация по ладони руки

В биометрике в целях идентификации используется простая геометрия руки — размеры и форма, а также некоторые информационные знаки на тыльной стороне руки (образы на сгибах между фалангами пальцев, узоры расположения кровеносных сосудов).

Сканеры идентификации по ладони руки установлены в некоторых аэропортах, банках и на атомных электростанциях .



Физическая защита данных на дисках

Для обеспечения большей скорости чтения, записи и надежности хранения данных на жестких дисках используются RAID-массивы (Redundant Arrays of Independent Disks - избыточный массив независимых дисков). Несколько жестких дисков подключаются к RAID - контроллеру, который рассматривает их как единый логический носитель информации.





Защита от вредоносных программ

Вредоносная программа (буквальный перевод англоязычного термина *Malware*, *malicious* — злонамеренный и *software* — программное обеспечение, жаргонное название — «малварь», «маловарь», «мыловарь» и даже «мыловарня») — злонамеренная программа, то есть программа, созданная со злым умыслом и/или злыми намерениями.



Типы вредоносных программ



- компьютерные вирусы



- сетевые черви



- программы показа рекламы (adware)



- программы-шпионы



- хакерские утилиты

Антивирусная программа

проверка
файлов

проверка
загрузочных
секторов
ДИСКОВ

проверка
оперативной
памяти

антивирусные программы

- ① Маска вируса - некоторая постоянная последовательность программного кода, специфичная для данного вируса.
- ① Для поиска новых вирусов - алгоритмы эвристического сканирования - анализ последовательности команд в проверяемом объекте.

Заражение файла компьютерным вирусом

Компьютерный вирус

антивирусной программой

Антивирусная программа

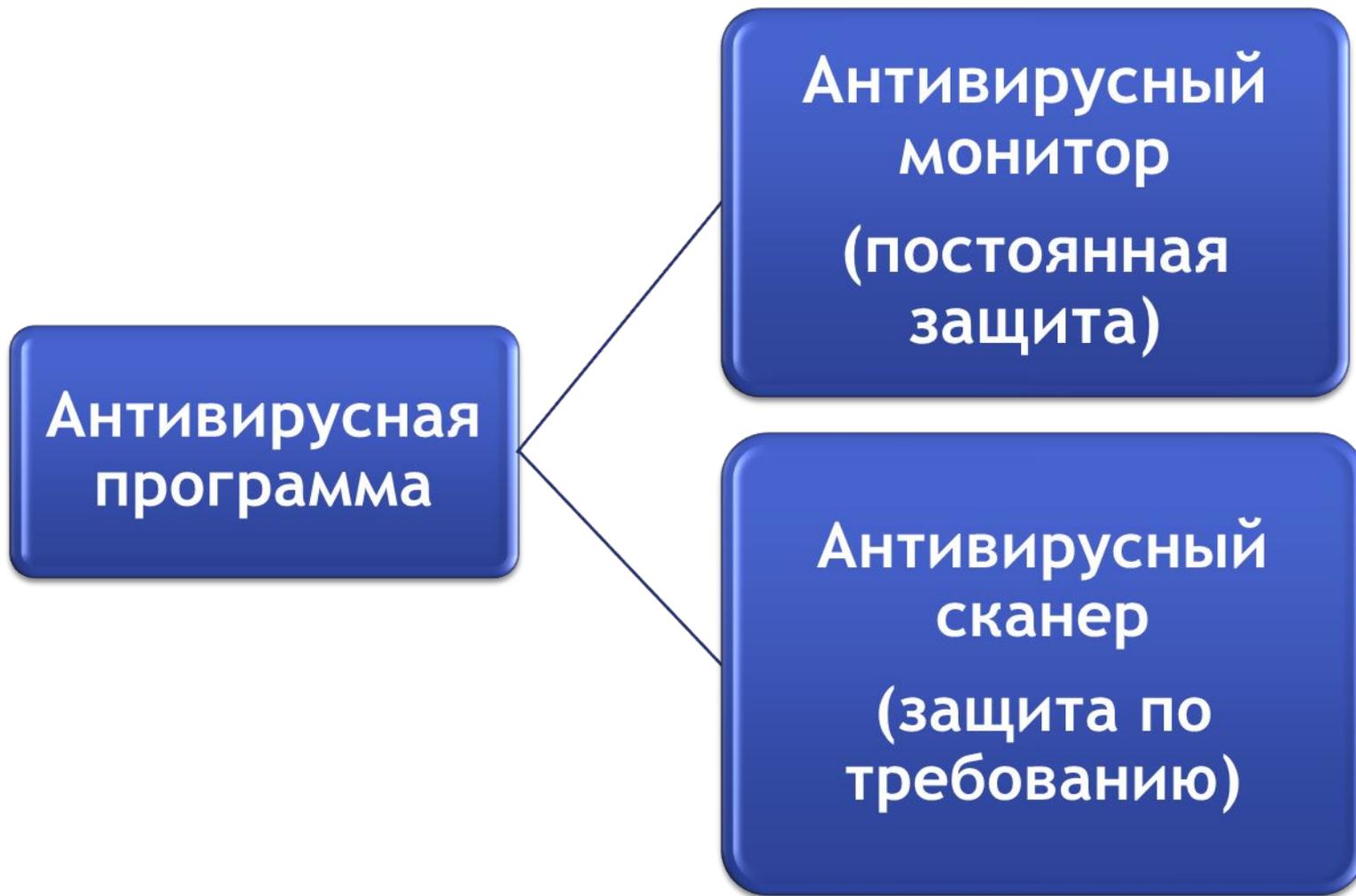
111000



Незараженный файл
10101010

Зараженный файл
1010101010111000

Вылеченный файл
10101010



* Защита информации.

Антивирусные программы



Современные антивирусные программы обеспечивают *комплексную защиту программ* и данных на компьютере от всех типов вредоносных программ и методов их проникновения на к

- Интернет,
- локальная сеть,
- электронная почта,
- съемные носители информации



Для защиты от вредоносных программ каждого типа в антивирусе предусмотрены отдельные компоненты.

Принцип работы антивирусных программ основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вредоносных программ.

Антивирусные программы

Для поиска известных вредоносных программ используются сигнатуры.

Сигнатура – это некоторая постоянная последовательность программного кода, специфичная для конкретной вредоносной программы. Если антивирусная программа обнаружит такую последовательность в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению или удалению.

Для поиска новых вирусов используются алгоритмы эвристического сканирования, т. е. анализа последовательности команд в проверяемом объекте. Если «подозрительная» последовательность команд обнаруживается, то антивирусная программа выдает сообщение о возможном заражении объекта.



Большинство антивирусных программ сочетает в *себе функции постоянной защиты* (антивирусный монитор) и *функции защиты по требованию пользователя* (антивирусный сканер).

Антивирусный монитор запускается автоматически при старте операционной системы и работает в качестве фонового системного процесса, проверяя на вредоносность совершаемые другими программами действия. Основная задача антивирусного монитора состоит в обеспечении максимальной защиты от вредоносных программ при минимальном замедлении работы компьютера.

Антивирусный сканер запускается по заранее выбранному расписанию или в произвольный момент пользователем. Антивирусный сканер производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера.

Действия при защита информации. наличии признаков заражения

компьютера

Прежде чем предпринимать какие либо действия, необходимо сохранить результаты работы на внешнем носителе (дискете, CD- или DVD-диске, флэш-карте и пр.).

Далее необходимо:

- * отключить компьютер от локальной сети и Интернета, если он к ним был подключен;
- * если симптом заражения состоит в том, что невозможно загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробовать загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows;
- * запустить антивирусную программу.



Компьютерные вирусы и защита от них

Компьютерные вирусы являются вредоносными программами, которые могут «размножаться» (самокопироваться) и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

Название «*вирус*» по отношению к компьютерным программам пришло из биологии именно по признаку способности к саморазмножению.

По «среде обитания» вирусы можно разделить на загрузочные, файловые и макровирусы.



Загрузочные вирусы

Загрузочные вирусы заражают загрузочный сектор гибкого или жесткого диска.

Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы, получающей управление при загрузке системы, и отдают управление не оригинальному коду загрузчика, а коду вируса. При инфицировании диска вирус в большинстве случаев переносит оригинальный загрузочный сектор в какой-либо другой сектор диска.

Профилактическая защита от загрузочных вирусов состоит в отказе от загрузки операционной системы с гибких дисков и установке в BIOS вашего компьютера защиты загрузочного сектора от изменений.



Файловые вирусы

Файловые вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске. После запуска зараженного файла вирус находится в оперативной памяти компьютера и является активным (т. е. может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.

Практически все **загрузочные и файловые вирусы резидентны** (стирают данные на дисках, изменяют названия и другие атрибуты файлов и т. д.).

Лечение от резидентных вирусов затруднено, так как даже после удаления зараженных файлов с дисков, вирус остается в оперативной памяти и возможно повторное заражение файлов.

Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на исполнение файлы, полученные из сомнительных источников и предварительно не проверенные антивирусными программами.

Макровирусы

Существуют макровирусы для интегрированного офисного приложения Microsoft Office. Макровирусы фактически являются макрокомандами (макросами), на встроенном языке программирования Visual Basic for Applications, которые помещаются в документ.

Макровирусы содержат стандартные макросы, вызываются вместо них и заражают каждый открываемый или сохраняемый документ.

Макровирусы являются ограниченно резидентными.

Профилактическая защита от макровирусов состоит в предотвращении запуска вируса. При открытии документа в приложениях Microsoft Office сообщается о присутствии в них макросов (потенциальных вирусов) и предлагается запретить их загрузку. Выбор запрета на загрузку макросов надежно защитит ваш компьютер от заражения макровирусами, однако отключит и полезные макросы, содержащиеся в документе.

Сетевые черви и * защита информации. защита от НИХ

Сетевые черви являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Активизация сетевого червя может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

Для своего распространения сетевые черви используют разнообразные сервисы глобальных и локальных компьютерных сетей: Всемирную паутину, электронную почту и т. д.

Основным признаком, по которому типы червей различаются между собой, является способ распространения червя — как он передает свою копию на удаленные компьютеры. Однако многие сетевые черви используют более одного способа распространения своих копий по компьютерам

Web-черви

Отдельную категорию составляют *черви, использующие для своего распространения web-серверы*. Заражение происходит в два этапа. Сначала червь проникает в компьютер-сервер и модифицирует web-страницы сервера. Затем червь «ждет» посетителей, которые запрашивают информацию с зараженного сервера (например, открывают в браузере зараженную web-страницу), и таким образом проникает на другие компьютеры сети.

Разновидностью Web-червей являются *скрипты* — активные элементы (программы) на языках JavaScript или VBScript.

Профилактическая защита от web-червей состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.

Еще более эффективны Web-антивирусные программы, которые включают межсетевой экран и модуль проверки скриптов на языках JavaScript или VBScript



Межсетевой экран

Межсетевой экран (брандмауэр) — это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет ее, либо пропускает в компьютер, в зависимости от параметров брандмауэра.

Межсетевой экран обеспечивает проверку всех web-страниц, поступающих на компьютер пользователя. Каждая web-страница перехватывается и анализируется межсетевым экраном на присутствие вредоносного кода.

Распознавание вредоносных программ происходит на основании баз, используемых в работе межсетевого экрана, и с помощью эвристического алгоритма. *Базы* содержат описание всех известных на настоящий момент вредоносных программ и способов их обезвреживания. *Эвристический алгоритм* позволяет обнаруживать новые вирусы, еще не описанные в базах.

Почтовые черви

Почтовые черви для своего распространения используют электронную почту.

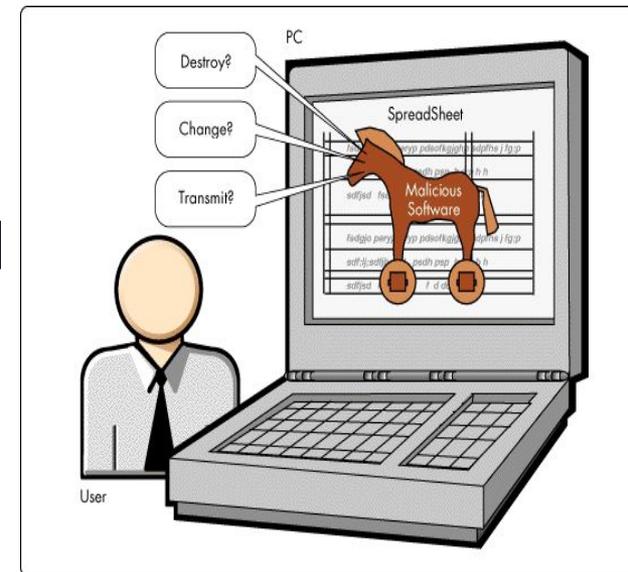
Червь либо отсылает свою копию в виде вложения в электронное письмо, либо отсылает ссылку на свой файл, расположенный на каком-либо сетевом ресурсе. В первом случае код червя активизируется при открытии (запуске) зараженного вложения, во втором — при открытии ссылки на зараженный файл. В обоих случаях эффект одинаков — активизируется код червя.

Червь после заражения компьютера начинает рассылать себя по всем адресам электронной почты, которые имеются в адресной книге пользователя.

Профилактическая защита от почтовых червей состоит в том, что

- не рекомендуется открывать вложенные в почтовые сообщения файлы, полученные из сомнительных источников.
- рекомендуется своевременно скачивать из Интернета и устанавливать обновления системы безопасности операционной системы и приложений.

Троянские программы и защита от них



Троянская программа, троянец (от англ. trojan) — вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удаленному пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

Троянские утилиты удаленного администрирования

Троянские программы этого класса являются утилитами удаленного администрирования компьютеров в сети. Утилиты скрытого управления позволяют принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д.

При запуске троянец устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянской программы в системе. В результате «пользователь» этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Являются одним из самых опасных видов вредоносного программного обеспечения.

Троянские программы - шпионы

осуществляют электронный шпионаж за пользователем зараженного компьютера: вводимая с клавиатуры информация, снимки экрана, список активных приложений и действия пользователя с ними сохраняются в каком-либо файле на диске и периодически отправляются злоумышленнику.

Троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайн-платежей и банковских систем.

Рекламные программы

Рекламные программы (англ. *Adware: Advertisement* – реклама и *Software* – программное обеспечение) встраивают рекламу в основную полезную программу и могут выполнять функцию троянских программ. Рекламные программы могут скрытно собирать различную информацию о пользователе компьютера и затем отправлять ее злоумышленнику.

Защита от троянских программ. Троянские программы часто изменяют записи системного реестра операционной системы, который содержит все сведения о компьютере и установленном программном обеспечении. Для их удаления необходимо восстановление системного реестра, поэтому компонент, восстанавливающий системный реестр, входит в современные операционные системы.

Хакерские утилиты и защита от них Сетевые атаки

Сетевые атаки на удаленные серверы реализуются с помощью специальных программ, которые посылают на них многочисленные запросы. Это приводит к отказу в обслуживании (зависанию сервера), если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов.

Некоторые хакерские утилиты реализуют фатальные сетевые атаки. Такие утилиты используют уязвимости в операционных системах и приложениях и отправляют специально оформленные запросы на атакуемые компьютеры в сети. В результате сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении, и система прекращает работу.

Утилиты взлома удалённых компьютеров

Утилиты взлома удаленных компьютеров предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими (используя методы троянских программ типа утилит удаленного администрирования) или для внедрения во взломанную систему других вредоносных программ.

Утилиты взлома удаленных компьютеров обычно используют уязвимости в операционных системах или приложениях, установленных на атакуемом компьютере.

Профилактическая защита от таких хакерских утилит состоит в своевременной загрузке из Интернета обновлений системы безопасности операционной системы и приложений.

Руткиты

Руткит (от англ. root kit – «набор для получения прав root») – программа или набор программ для скрытого взятия под контроль взломанной системы.

Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Руткиты модифицируют операционную систему на компьютере и заменяют основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Защита от хакерских атак, сетевых червей и троянских программ.

Защита компьютерных сетей или отдельных компьютеров от несанкционированного доступа может осуществляться с помощью межсетевого экрана.

Межсетевой экран позволяет:

- блокировать хакерские DoS-атаки, не пропуская на защищаемый компьютер сетевые пакеты с определенных серверов (определенных IP-адресов или доменных имен);
- не допускать проникновение на защищаемый компьютер сетевых червей (почтовых, Web и др.);
- препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.

Классификация вирусов по особенностям алгоритма

Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Можно отметить вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

Известны *вирусы-невидимки*, называемые *стелс-вирусами*, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.

Наиболее трудно обнаружить *вирусы-мутанты*, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

Имеются и так называемые *квазивирусные* или «троянские» программы, которые хотя и не способны к самораспространению,

Виды и методы защиты информации

Вид защиты	Метод защиты
От сбоев оборудования	<ul style="list-style-type: none">• Архивирование файлов (со сжатием или без);• резервирование файлов
От случайной потери или искажения информации, хранящейся в компьютере	<ul style="list-style-type: none">• Запрос на подтверждение выполнения команд, изменяющих файлы;• установка специальных атрибутов документов и программ;• возможность отмены неверного действия или восстановления ошибочно удалённого файла;• разграничение доступа пользователей к ресурсам файловой системы

Виды и методы защиты информации

Вид защиты	Метод защиты
От преднамеренного искажения, вандализма (компьютерных вирусов)	<ul style="list-style-type: none">• Общие методы защиты информации;• профилактические меры;• использование антивирусных программ
От несанкционированного (нелегального) доступа к информации (её использования, изменения, распространения)	<ul style="list-style-type: none">• Шифрование;• паролирование;• «электронные замки»;• совокупность административных и правоохранительных мер

*Контрольные вопросы.

1. Дайте понятие защиты информации.
2. Назовите основные виды защиты информации.
3. Перечислите статьи УК РФ, направленные на правовую защиту информации.
4. Что такое несанкционированный доступ?
5. Перечислите меры по предотвращению несанкционированного доступа к информации.
6. Перечислите основные виды вредоносных программ.
7. Какие методы борьбы с вредоносными программами вы знаете?
8. Назовите классификацию вирусов по особенностям алгоритма.
9. Что такое межсетевой экран?
10. Какие методы защиты информации от сбоев