Практическая работа № 4
По теме: современные способы и средства зашиты информации

Выполнила студентка:
группы ИФ2И Китаева Дарья

Общее понятие информационной безопасности

- ГОСТ "*Защита информации*. Основные термины и определения" вводит понятие **информационной безопасности** как состояние защищенности информации, при котором обеспечены ее *конфиденциальность*, доступность и *целостность*.
- **Угрозы информационной безопасности** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. **Атакой** называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, **- злоумышленником**. Потенциальные злоумышленники называются *источниками угрозы*.
- *Угроза* является следствием наличия **уязвимых мест или уязвимостей** в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

- Обеспечение информационной безопасности является сложной задачей, для решения которой требуется *комплексный подход*. Выделяют следующие уровни защиты информации:
- законодательный – законы, нормативные акты и прочие документы РФ и международного сообщества;
- административный – комплекс мер, предпринимаемых локально руководством организации;
- процедурный уровень – меры безопасности, реализуемые людьми;
- *программно-технический уровень* – непосредственно средства защиты информации.
- Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия *предметной области* и определяет меру наказания для потенциальных злоумышленников.

Цели информационной безопасности

- Основные цели достижения высокого уровня информационной безопасности – это обеспечение конфиденциальности, целостности, доступности, подлинности и неотказуемости информации.
- Конфиденциальность информации — такое состояние информации, при котором доступ к ней только у объектов с наличием прав на неё.
- Целостность информации — блокировка несанкционированных изменений информации.
- Доступность информации — избежание сокрытия информации от пользователей с правами доступа.
- Подлинность информации — предполагает соответствие этой информации её явному описанию и содержанию.

Угроза безопасности компьютерной системы

- Безопасность информации в компьютерной системе (КС) - это такое состояние всех компонент КС, при котором обеспечивается защита информации от *возможных угроз.*
- Угрозы информационным системам можно объединить в следующие группы:
- угроза раскрытия информации;
- угроза нарушения целостности — умышленное несанкционированное или неумышленное изменение (удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую;
- угроза отказа в обслуживании блокировка доступа к некоторому ресурсу вычислительной системы.
- По природе возникновения угрозы можно разделить на: естественные; искусственные.
- Естественные угрозы — это угрозы, связанные с воздействиями на ИС объективных физических процессов или природных явлений. Ис кусственные угрозы — это угрозы информационной системе, связанные с деятельностью человека.

- **Угрозы безопасности информации в компьютерных системах (КС)**
- Случайные (до 80%) - Стихийные бедствия, аварии; Сбои, отказы технических средств; Ошибки при разработке КС; Алгоритмические и программные ошибки; Ошибки пользователей и обслуживающего персонала. [до 65%]
- Преднамеренные – Шпионаж, диверсии; Несанкционированный доступ к информации (НСД); Электромагнитные излучения, наводки (ПЭМИН); Несанкционированная модификация структур; Вредительские программы. [до 69%]

Виды информационных угроз

Виды информационных угроз

Политика безопасности

- Под **политикой безопасности** организации понимают совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Политика безопасности является тем средством, с помощью которой реализуется деятельность в компьютерной информационной системе организации.

Технические средства защиты информации

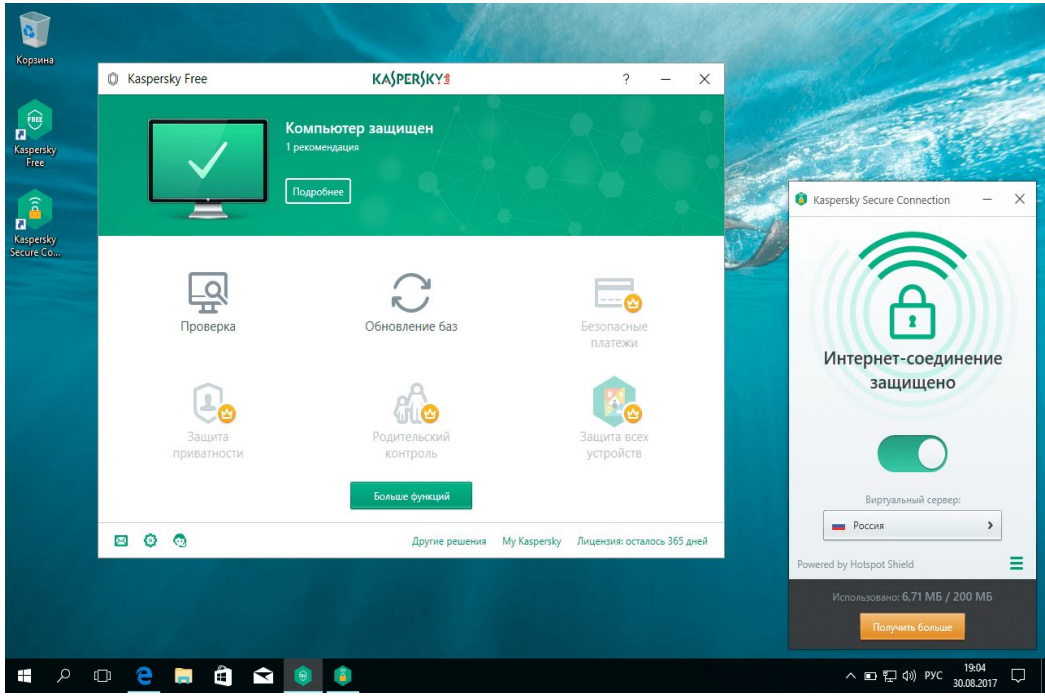
- **Инженерно-техническая защита (ИТЗ)** — это совокупность специальных органов, технических средств и мероприятий по их использованию в целях защиты конфиденциальной информации. По функциональному назначению средства инженерно-технической защиты делятся на следующие группы:
- **1) Физические средства**, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий;
- **2) Аппаратные средства защиты информации** — это различные технические устройства, системы и сооружения (**техническая защита информации**), предназначенные для защиты информации от разглашения, утечки и несанкционированного доступа.
- **3) Программные средства**. Программная защита информации — это система специальных программ, реализующих функции защиты информации.
- **4) Криптографические средства —** это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Аппаратные средства защиты информации

- Использование аппаратных средств защиты информации позволяет решать следующие задачи:
- проведение специальных исследований технических средств на наличие возможных каналов утечки информации;
- выявление каналов утечки информации на разных объектах и в помещениях;
- локализация каналов утечки информации;
- поиск и обнаружение средств промышленного шпионажа;
- противодействие НСД (несанкционированному доступу) к источникам конфиденциальной информации и другим действиям.

Программные средства защиты информации

- Выделяют следующие направления использования программ для обеспечения безопасности конфиденциальной информации
- защита информации от несанкционированного доступа;
- защита информации от копирования;
- защита информации от вирусов;
- программная защита каналов связи.



Виды антивирусных программ

- На сегодняшний день перечень доступных антивирусных программ весьма обширен. Они различаются как по цене (от весьма дорогих до абсолютно бесплатных), так и по своим функциональным возможностям.

- **Типовой перечень функций, которые способны выполнять антивирусные программы:**
- - сканирование памяти и содержимого дисков по расписанию;
- - сканирование памяти компьютера, а также записываемых и читаемых файлов в реальном режиме времени с помощью резидентного модуля;
- - выборочное сканирование файлов с измененными атрибутами;
- - распознавание поведения, характерного для компьютерных вирусов;
- - блокировка и/или удаление выявленных вирусов;
- - восстановление зараженных информационных объектов;
- - принудительная проверка подключенных к корпоративной сети компьютеров;
- - удаленное обновление антивирусного программного обеспечения и баз данных с информацией о вирусах, в том числе автоматическое обновление баз данных по вирусам через Интернет;
- - фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;
- - выявление потенциально опасных Java-апплетов и модулей ActiveX;
- - ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты.

- **К наиболее мощным и популярным на сегодняшний день в России антивирусным пакетам относятся:**
- - Doctor Web (в документации часто именуется более кратко - Dr Web) программа российской компании;
- - Антивирус Касперского (в документации именуется более кратко – AVP) разработка еще одной российской фирмы
- - Norton AntiVirus корпорации Simantec;
- - McAfee VirusScan компании Network Associates;
- - Panda AntiVirus.
- - Nod32 AntiVirus.

Недостатки антивирусных программ

- Ø Ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов.
- Ø Антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск. Особенно это может быть заметно на слабых компьютерах. Замедление в фоновом режиме работы может достигать 380 %.
- Ø Антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания).
- Ø Антивирусные программы загружают обновления из Интернета, тем самым расходуя трафик.
- Ø Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением.

Понятие компьютерного вируса

- ***Компьютерный вирус*** – это небольшая по размерам программа, ориентированная на существование и размножение в файле за счет его несанкционированного изменения, т.е. ***заражения***, а также выполнения нежелательных действий на компьютере.

- Основными источниками заражения являются электронная почта, Интернет, локальная сеть, съемные диски (дискеты и CD-ROM). Не следует запускать на исполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами, устанавливать общий доступ к папкам и файлам компьютера, работающего в сети.

Классификация компьютерных вирусов

- ***Существует несколько подходов к классификации компьютерных вирусов по их характерным особенностям:***
- — по среде обитания вируса;
- — по способу заражения;
- — по деструктивным возможностям;
- — по особенностям алгоритма работ.

По среде обитания вирусы подразделяются на

- ***Файловые вирусы*** — вирусы поражающие исполняемые файлы, написанные в различных форматах. Соответственно в зависимости от формата, в котором написана программа это будут EXE или COM вирусы.
- ***Загрузочные вирусы*** — вирусы поражающие загрузочные сектора (Boot сектора) дисков или сектор содержащий системный загрузчик(Master Boot Record) винчестера.
- ***Сетевые вирусы*** — вирусы, распространяющиеся в различных компьютерных сетях и системах.
- ***Макро вирусы*** — вирусы поражающие файлы Microsoft Office
- ***Flash вирусы*** — вирусы поражающие микросхемы FLASH памяти BIOS.

По способу заражения вирусы делятся на:

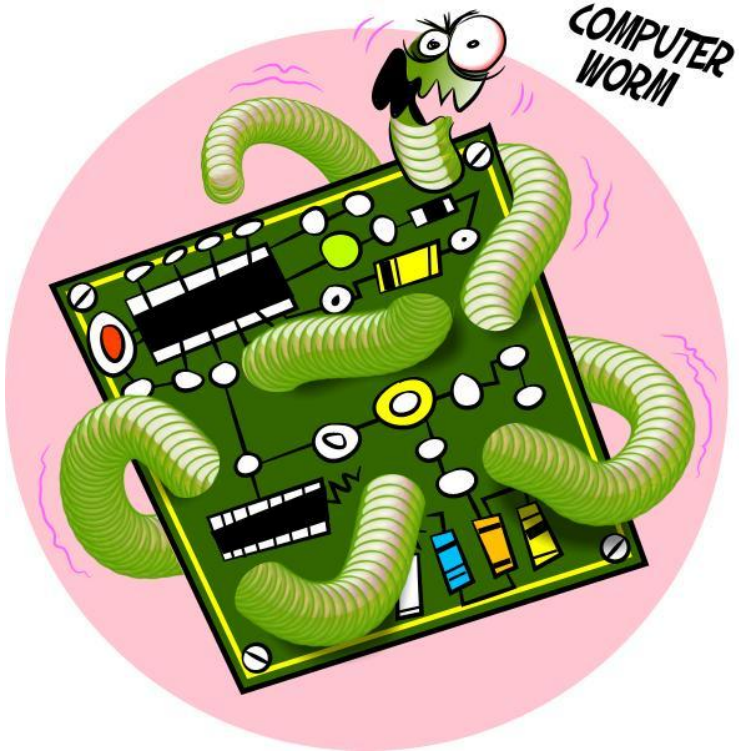
- ***Резидентные вирусы*** — вирусы, которые при инфицировании компьютера оставляют свою резидентную часть в памяти. Они могут перехватывать прерывания операционной системы, а также обращения к инфицированным файлам со стороны программ и операционной системы. Эти вирусы могут оставаться активными вплоть до выключения или перезагрузки компьютера.
- ***Нерезидентные вирусы*** — вирусы, не оставляющие своих резидентных частей в оперативной памяти компьютера. Некоторые вирусы оставляют в памяти некоторые свои фрагменты не способные к дальнейшему размножению такие вирусы считаются не резидентными.

По деструктивным возможностям вирусы подразделяются на:

- ***Безвредные вирусы*** — это вирусы ни как не влияющие на работу компьютера за исключение, быть может, уменьшения свободного места на диске и объема оперативной памяти.
- ***Неопасные вирусы*** — вирусы, которые проявляют себя в выводе различных графических, звуковых эффектов и прочих безвредных действий.
- ***Опасные вирусы*** — это вирусы, которые могут привести к различным сбоям в работе компьютеров, а также их систем и сетей.
- ***Очень опасные вирусы*** — это вирусы, приводящие к потере, уничтожению информации, потере работоспособности программ и системы в целом.

По особенностям алгоритма работы вирусы можно подразделить на:

- ***Вирусы спутники(compаnion)*** — эти вирусы поражают EXE-файлы путем создания COM-файла двойника, и поэтому при запуске программы запустится, сначала COM-файл с вирусом, после выполнения своей работы вирус запустит EXE-файл. При таком способе заражения «инфицированная» программа не изменяется.
- ***Вирусы «черви» (Worms)*** — вирусы, которые распространяются в компьютерных сетях. Они проникают в память компьютера из компьютерной сети, вычисляют адреса других компьютеров и пересылают на эти адреса свои копии. Иногда они оставляют временные файлы на компьютере но некоторые могут и не затрагивать ресурсы компьютера за исключением оперативной памяти и разумеется процессора.



СПАСИБО ЗА ВНИМАНИЕ