Основы защиты информации.
Компьютерные преступления и борьба с ними

План лекции:

1. Информационная безопасность и виды компьютерных преступлений.
2. Профилактика компьютерных преступлений.
3. Компьютерные вирусы, их классификация.
4. В антивирусные программы.

Защита информации – это применение различных средств и методов, использование мер и осуществление мероприятий для того чтобы обеспечивать систему надежности передаваемой, хранимой и обрабатываемой информации.

Юридически информационная безопасность должна обеспечивать:

- целостность данных;
- конфиденциальность информации;
- доступность информации для всех зарегистрированных пользователей.

Процессы по нарушению надежности информации подразделяют на

- **случайные**, которые возникают в результате непреднамеренных, ошибочных действий людей, технических сбоев;
- **злоумышленные** (преднамеренные), которые появляются в результате целенаправленных действий людей.

Все компьютерные преступления условно можно разделить на

- преступления, нарушающие работу компьютера;
- преступления, использующие ПК как необходимые технические средства.

Среди компьютерных преступлений можно выделить основные:

- **Неправомерный доступ к информации, хранящейся на компьютере, хищение компьютерной информации**. Осуществляется изменением программного и аппаратного обеспечения, хищением носителей, установкой аппаратуры перехвата информации при ее передаче, нарушением систем защиты информации. Включает нарушение авторских прав - нелицензионное ПО, книги и т.п.
- **Подделка компьютерной информации**. Например, разработчик ПО имитирует получение каких-то параметров, выгодных себе или третьему лицу, т.е вместо разработки математической модели имитирует выходные данные.

- **Создание, использование и распространение вредоносных программ для ЭВМ** (вирусы, в т.ч. «троянские кони»).

Профилактика компьютерных преступлений

К мерам профилактики компьютерных преступлений и борьбы с ними относят:

1. **юридические и морально-этические**, которые включают в себя действующие в стране законы, нормативные акты, нормы поведения, соблюдение которых способствует защите информации.
2. **организационные** – регламентация доступа к информационным и вычислительным ресурсам, процессам обработки информации. В частности:
   - допуск к информации проверенных лиц;
   - разделение доступа должностных лиц с соответствии с их функциональными обязанностями;
   - хранение носителей информации в сейфах, недоступных для посторонних лиц;
   - учет применения и уничтожения документов;
3. **технические** – применяются для создания некоторой физически замкнутой среды вокруг объекта и элементов защиты. В частности,
   - установка систем защиты от сбоя электропитания;
   - ограничение электромагнитного излучения через экранирование;
   - оборудование системой кодовых замков; установка сигнализации.
4. **технологические –** мероприятия, встраиваемые в процессы преобразования данных. К ним относятся:
   - создание архивных копий носителей;
   - сохранение обрабатываемых файлов во внешней памяти компьютера;
5. **программные** реализуют защитные функции:
   - разграничение и контроль доступа к ресурсам;
   - регистрация и изучение протекающих процессов;
   - предотвращение возможных разрушительных воздействий на ресурсы;
   - криптографическая защита информации.

Компьютерные вирусы, их классификация и борьба с ними

Компьютерный вирус – самовоспроизводящаяся программа, наносящая ущерб аппаратно-программному обеспечению компьютера.

В компьютерной вирусологии часто используется термин

Сигнатура – двоичный уникальный код, характеризующий компьютерную программу (в т.ч. вирусную).

Компьютерные вирусы классифицируются по следующим признакам:

- Место расположения программного ядра вирусной программы
- Способ заражения
- Деструктивные результаты
- Способ проявления

По виду среды обитания выделяют:

- ***Загрузочные (бутовые) вирусы*** переносятся из системы в систему через загрузочный сектор и заражает только boot-секторы дискет и жестких дисков.
- ***Файловые вирусы*** распространяются в файлах. Инфицируют .com и .exe файлы. При запуске зараженной программы происходит самокопирование вируса.
- ***Файлово-загрузочные*** вирусы заражают загрузочные секторы дисков и файлы прикладных программ.
- ***Сетевые вирусы*** распространяются по локальной или глобальной сети. Компьютерные «черви» размножаются с высокой скоростью на всех участках сети, что приводит к понижению пропускной способности сети, замедлению работы на участках с наиболее напряженным потокообменом данных.
- Системные вирусы внедряются в системные модули и драйверы переферийных устройств, таблицы размещения файлов и таблицы разделов.

По пути заражения среды обитания выделяют:

- ***Резидентные вирусы*** инсталлируют свою копию в оперативную память, после чего резидентная копия заражает другие файлы.
- ***Нерезидентные вирусы*** не заражают ОП компьютера и проявляют активность ограниченное время.

По деструктивным результатам (по степени воздействия на ресурсы компьютерных систем и сетей) выделяют:

- ***Безвредные вирусы*** не оказывают патологического влияния на работу компьютера.
- ***Неопасные вирусы*** не разрушают файлы, но уменьшают свободную дисковую память, выводят на экран графические эффекты.
- ***Опасные вирусы*** вызывают значительные нарушения в работе компьютера.

- ***Разрушительные вирусы*** могут привести к потере информации, полному или частичному нарушению работы прикладных программ.

По особенностям построения вирусов, их функционированию выделяют:

- ***Макровирусы*** используют возможности макроязыков, которые встроены в Word, Excel, что приводит к блокировке команд открытия, сохранения и т.д. (WM.Cap).
- ***Вирусы-невидимки*** (стелс-вирусы) очень опасны, т.к. заразив ПК, остаются незамеченными системами контроля. Перехватывают обращения ОС к пораженным файлам и секторам дисков и подставляют вместо себя незараженные объекты. Применяют оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы.
- ***Полиморфные вирусы*** (вирусы-мутанты) затрудняют обнаружение зараженных файлов тем, что самовоспроизводясь, создают копии, отличные от оригинала (One Half 3544).
- ***Логическая бомба*** встраивается в большой программный комплекс. Безвредна до наступления определенного события, после которого реализуется ее логический механизм.

Основные **симптомы заражения**:

- Замедление работы компьютера
- Невозможность или замедление загрузки ОС или прикладных программ (при этом часто выдается сообщение о недостаточности памяти)
- Зависание программ либо неадекватные реакции
- Необычные сообщения
- Увеличение числа файлов или размера файлов на диске
- Нарушения файловой структуры, невозможность загрузки файлов
- Появление «сбойных» секторов на диске, даже если не проводилось проверки диска
- Утеря информации на диске или ее кодирование

Профилактика:

1) Копирование важной информации.

Наряду с обычным копированием данных полезно создание образа жесткого диска на внешних носителях (например, на гибких дисках). В случае выхода из строя данных в системных областях жесткого диска сохраненный "образ диска" может позволить восстановить большую часть данных. Это же средство может защитить от утраты данных при аппаратных сбоях и при неаккуратном форматировании жесткого диска.

2) Периодическая проверка на наличие вируса и проверка в фоновом режиме.

Существуют три рубежа защиты от компьютерных вирусов:

- предотвращение поступления вирусов;
- предотвращение вирусной атаки, если вирус все-таки поступил на компьютер;
- предотвращение разрушительных последствий, если атака все-таки произошла.

В антивирусные программы включается база данных сигнатур вирусов, которую следует регулярно обновлять. Желательная периодичность обновления - один раз в одну - две недели; допустимая – один раз в один - три месяца. Антивирусная программа анализирует компьютерную систему, отыскивая соответствие с сигнатурами в базе данных.

По способу работы можно выделить

- Программы-фильтры – сторожа, постоянно находятся в ОП. Являются резидентными, перехватывают все запросы к ОС на выполнение подозрительных действий. Не лечат файлы и диски. Уменьшают объем ОП. (AVP, Norton AntiVirus for Windows)
- Программы-ревизоры. Устанавливаются до заражения. Запоминают исходное состояние программ, каталогов и системных областей дисков. Постоянно сравнивают текущее состояние с исходным (Adinf).
- Программа-доктор способна «лечить» зараженные программы или диски, уничтожает зараженные программы тела вируса. Фаги – программы, с помощью которых отыскиваются вирусы определенного вида. Полифаги предназначены для обнаружения и уничтожения большого числа разнообразных вирусов (MS AntiVirus, Doctor Web).
- Программы-детекторы обнаруживают файлы, зараженные одним или несколькими известными вирусами.
- Программы-вакцины модифицируют программы и диски так, что вирус считает их зараженными и не внедряется в них.

Защита информации в Интернете

При работе в Интернете следует иметь в виду, что

- насколько ресурсы Всемирной сети открыты каждому клиенту, настолько же и ресурсы его компьютерной системы могут быть открыты всем, кто обладает необходимыми средствами.
- все действия фиксируются и протоколируются специальными программными средствами и информация как о законных, так и о незаконных действиях обязательно где-то накапливается.

Информация свободно циркулирует, она доступна всем участникам информационного процесса. Это касается всех служб Интернета, открытых для массового использования.

Системам шифрования столько же лет, сколько письменному обмену информацией. Обычный подход состоит в том, что к документу применяется некий метод шифрования (ключ), после чего документ становится недоступен для чтения обычными средствами. Его можно прочитать только тот, кто знает ключ. Аналогично шифруется и ответного сообщения.

Если для шифрования и чтения пользуются одним и тем же ключом, то такой криптографический процесс является симметричным. Основной недостаток симметричного процесса заключается в том, что, прежде чем начать обмен информацией, надо выполнить передачу ключа, а для этого опять-таки нужна защищенная связь.

Поэтому в настоящее время в Интернете используют несимметричные криптографические системы, основанные на использовании не одного, а двух ключей. Происходит это следующим образом. Компания для работы с клиентами создает два ключа: один - открытый (public - публичный) ключ, а другой - закрытый (private - личный) ключ. На самом деле это как бы две "половинки" одного целого ключа, связанные друг с другом.

Ключи устроены так, что сообщение, зашифрованное одной половинкой, можно расшифровать только другой половинкой (не той, которой оно было закодировано). Создав пару ключей, торговая компания широко распространяет публичный ключ (открытую половинку) и надежно сохраняет закрытый ключ (свою половинку).