

ЛЕКЦИЯ. Основы компьютерной безопасности.

План.

1. Компьютерные преступления: общая характеристика и классификация.
2. Способы защиты информации.
3. Компьютерные вирусы: их действие и последствия.
4. Основные виды вирусов.
5. Профилактика и борьба с компьютерными вирусами.

1. Компьютерные преступления: общая характеристика и классификация.

Компьютерными преступлениями называются действия, объектом или орудием совершения которых являются электронные вычислительные машины.

Они связаны с внесением изменений в информацию на различных этапах ее обработки, с незаконным овладением программным обеспечением, или искажением его, с незаконным овладением информацией с целью ее использования для хищения денег, укрытия от налогообложения, для промышленного или коммерческого шпионажа, с нанесением ущерба в виде уничтожения программ и данные конкурентов.

Основой для совершения таких преступлений является то, что в автоматизированных вычислительных системах имеется ряд незащищенных мест, которые могут быть использованы для совершения правонарушений. К их числу относятся:

периферийные устройства, системные и прикладные программы, бумажные и безбумажные носители данных (карточки с данными, дискеты), микросхемы, каналы связи.

Термин «компьютерные преступления» появился в американской, а затем в зарубежной литературе с середины 60-х годов. По оценке американского юриста А. Бекля ежегодно компьютерные воры похищают у населения более 100 млн. долларов. И это только надводная часть айсберга, поскольку раскрываемость таких преступлений составляет 1%. В Англии ущерб от компьютерного мошенничества оценивается в 750 млн. фунтов стерлингов.

Для предотвращения компьютерных преступлений необходима правовая база. Ее основанием является законодательное признание программного обеспечения ЭВМ и данных в качестве товара. Это позволяет определить состав преступления.

В нашей стране с 01.01.97 установлена уголовную ответственность за всякое несанкционированное получение из ЭВМ данных или программ. В соответствии с Уголовным Кодексом наказания за преступления такого рода носят материальный характер, а также связаны с лишением свободы.

Компьютерные преступления классифицируются следующим образом:

КОМПЬЮТЕРНОЕ МОШЕННИЧЕСТВО - преступное искажение программ, а так же запись и использование искаженных данных. Цель компьютерного мошенничества - незаконное получение имущественных выгод для себя или для других лиц. Этот вид преступлений достаточно широко развит за рубежом.

КРАЖИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ - незаконное приобретение или использование программ записанных в памяти ЭВМ. Эти преступления

затрагивают интересы авторских прав, а так же государства. Они чрезвычайно распространены в нашей стране.

КОМПЬЮТЕРНЫЙ САБОТАЖ - нарушение функционирования информационной системы при манипуляциях с программным обеспечением и аппаратурой. Этот вид преступлений включает уничтожение или фальсификацию информации повреждение или разрушение средств информационной техники. Особую разновидность этого вида преступлений представляют действия по созданию и распространению компьютерных вирусов. ***Компьютерные вирусы*** - это разновидность несанкционированного доступа, приводящей к уничтожению или модификации данных и программного обеспечения.

Подлинный ущерб от компьютерного вируса неизвестен, поскольку пострадавшие предпочитают скрывать сведения об этом, чтобы не получить статус неблагонадежных и не проиграть в конкурентной борьбе. Однако ежегодно становится известно об ущербе от этих преступлений, измеряемом десятками миллионов долларов. Сопоставимые по объему средства затрачиваются на борьбу с этими преступлениями.

КОМПЬЮТЕРНЫЙ ШПИОНАЖ - незаконное овладение информацией, находящейся в компьютере.

КОМПЬЮТЕРНОЕ ЗЛОУПОТРЕБЛЕНИЕ - правонарушение, включающее неправомерное использование, уничтожение, изменение обрабатываемых информационных ресурсов. Примером злоупотребления могут служить несанкционированное использование ресурсов компьютеров для программистской деятельности, игр и др.

2. Способы защиты информации.

Для предупреждения компьютерных преступлений и разрабатываются различные способы защиты от несанкционированного доступа к данным и программным средствам. Из них основными являются:

1. технические,
2. программные,
3. криптографические
4. правовые.

Под **ТЕХНИЧЕСКИМИ** способами защиты данных и программного обеспечения понимаются

экранирование помещений, в которых находятся ЭВМ,
установка генераторов шумов.

Однако только техническим способом защитить информацию от несанкционированного доступа практически невозможно.

При **ПРОГРАММНОЙ** защите данных и программного обеспечения разрабатываются специальные программы, которые не позволяют постороннему пользователю не знакомому с видом защиты получать информацию из системы. Примером такого рода защиты может служить система паролей.

Под **КРИПТОГРАФИЧЕСКИМ** способом защиты данных подразумевается предварительная их зашифровка до ввода в ЭВМ.

ПРАВОВАЯ защита информации - комплекс административно-правовых **норм**, устанавливающих ответственность за несанкционированное использование данных и программных средств.

На практике используются комбинированные способы защиты информации от несанкционированного доступа. Вопрос о выборе способов защиты информации решается разработчиками автоматизированных систем совместно с конкретными заказчиками.

3. Компьютерные вирусы: их действие и последствия.

Компьютерным вирусом называется специально написанная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе на компьютере.

Причины появления и распространения компьютерных вирусов, с одной стороны, скрываются в психологии человеческой личности и ее теневых сторон (завести, мести и т.п.), с другой стороны, обусловлены отсутствием аппаратных средств защиты и противодействия со стороны операционной системы персонального компьютера.

Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет.

Действия, выполняемые КВ, и их последствия заключаются в следующем:

1. КВ портят файлы (тексты программ и документов; информационные базы данных; таблицы табличных процессоров и др. подобные файлы).
2. КВ "засоряют" оперативную память (искусственно уменьшают емкость памяти, ухудшая технико-эксплуатационные характеристики ПК);
3. КВ порождают различные звуковые и видеоэффекты (музыка, мешающая работе, падающие буквы, помеха на экране);
4. КВ замедляют выполнение некоторых операций (в первую очередь ввод-вывод);
5. КВ препятствуют выполнению некоторых программ;
6. по влиянием КВ "некорректно выполняют некоторые запросы программ к ОС;
7. КВ незаметно модифицируют файлы данных (например, менять местами две последовательные цифры в базах данных);
8. КВ уничтожают информацию на дисках путем форматирования или затирания участков диска;
9. КВ разрушают файловую систему (таблицу размещения файлов, каталоги, загрузочный сектор диска) файловые и загрузочные вирусы;
10. в результате работы компьютерных вирусов физически разрушаются некоторые устройства ЭВМ. (например, есть вирусы, которые постоянно производят запись на определенную дорожку жесткого диска и тем самым приводят к стиранию на ней магнитного покрытия. Другие вирусы портят диски путем некорректных операций ввода-вывода, либо портят монитор сведением всех лучей в одну точку).

Чтобы предотвратить свое обнаружение КВ используют приемы маскировки. Широко распространены:

1. *невидимые вирусы* - перехватывают сообщения DOS к зараженным областям и выдают их в исходном виде.
2. *самомодифицирующиеся вирусы* - хранят свой текст в закодированном виде. Это существенно затрудняет их поиск.

По данным научной периодики, в настоящее время в мире известны свыше 40 000 KB. Их число ежедневно увеличивается.

KB не только портят, но и *заражают* файлы. **Программа**, внутри которой находится вирус, называется **зараженной**. KB заражает следующие виды программ:

1. *исполнимые файлы* т.е. с расширением .COM и .EXE. Вирус в зараженных исполняемых файлах начинает свою работу при запуске той программы в которой он находится. Наиболее опасно заражение командного процессора COMMAND.COM, т.к. этот вирус будет работать при выполнении любой команды и любая выполняемая программа будет заражена;
2. *загрузчик операционной системы и главная загрузочная запись жесткого диска*;
3. *драйверы устройств*;
4. *объектные файлы и библиотеки* т.е. файлы с расширением .OBJ и .LIB;
5. *системные файлы*;

4. Основные виды вирусов. САМОСТОЯТЕЛЬНО.

В настоящее время известно более 45000 программных вирусов, их можно классифицировать по следующим признакам:

- среде обитания (сетевые, файловые, загрузочные, файлово-загрузочные),
- способу заражения среды обитания (резидентные, нерезидентные);
- " воздействию (неопасные, опасные, очень опасные);
- особенностям алгоритма (паразитические, репликаторы, невидимки, мутанты, троянские, вирусы-спутники).

Сетевые вирусы распространяются по различным компьютерным сетям.

Файловые вирусы внедряются главным образом в исполняемые модули, имеющие расширение COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они не могут получить управления и теряют способность к размножению.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (MASTER BOOT RECORD).

Файлово-загрузочные заражают как файлы, так и загрузочные сектора дисков.

Резидентные вирусы при заражении компьютера оставляют в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т.п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

Неопасные - не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, проявляются в каких-либо графических или звуковых эффектах.

Опасные вирусы, которые могут привести к различным нарушениям в работе компьютера.

Очень опасные - воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

Паразитические - они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.

Вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

Вирусы невидимки (стелс-вирусы) - трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки дисков.

Вирусы-мутанты - наиболее трудно обнаружить, содержат алгоритмы шифровки - расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

Троянские или квазивирусные программы - это те, которые, хотя и неспособны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Вирусы-спутники - 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 ХСОРУ.EXE создается файл ХСОРУ.COM. Вирус записывается в .COM файл и не как не изменяет EXE файл. При запуске такого файла DOS первым обнаружит и вытащит COM файл, т.е. вирус который затем запустит EXE файл.

5.Профилактика и борьба с компьютерными вирусами.

Для того, **чтобы компьютер заразился вирусом** необходимо, чтобы:

1. на нем была выполнена хотя бы одна программа, содержащая вирус.
2. компьютер загружался с дискеты, содержащей зараженный загрузочный сектор.
3. на компьютере была установлена зараженная ОС или зараженный драйвер устройства.

Чтобы грамотно осуществлять профилактику и борьбу с **компьютерными** вирусами, надо знать как они работают.

При запуске "зараженной" программы вирус до перезагрузки остается в оперативной памяти компьютера и время от времени заражают другие программы и выполняют вредоносные действия на компьютер. Действия вируса выполняются достаточно быстро и без видных каких-либо сообщений, поэтому пользователю трудно заметить, что в компьютере происходит необычного. Если на компьютере заражено относительно мало программ, то наличие вируса практически не заметно.

Кроме того, зараженные программы с одного компьютера переносятся на другие с помощью дискет или локальных сетей.

Для обнаружения и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаружить и уничтожить вирусы. Такие программы называются **антивирусными**.

Различают следующие виды антивирусных программ:

- программы-детекторы;
- программы-доктора или фаги;
- программы-ревизоры;
- программы-фильтры;
- программы-вакцины или иммунизаторы.

Программы-детекторы - осуществляют поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса) в оперативной памяти и в файлах, при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора или фаги, а также вакцины программы не только находят зараженные вирусами файлы, но и лечат их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только потом переходят к лечению файлов. Среди фагов выделяют **полифаги**; т.е. **программы-доктора**, предназначенные для поиска и уничтожения большого количества вирусов (Aidstest, Scan, Norton Antivirus и Doctor Web). Требуют постоянного обновления.

Программы-ревизоры - самые надежные средства защиты.

Они запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивает текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора (Adinf фирма Диалог-Наука).

Программы-фильтры или сторожа - представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

- попытка коррекции файлов с расширениями COM, EXE;
- изменение атрибутов файлов;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

При попытке таких действий, сторож посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Полезны тем, что обнаруживают вирусы на ранней стадии, но не лечат, для этого необходимо применять фаги.

Вакцины или иммунизаторы - это резидентные программы, предотвращающие заражение файла. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет

воспринимать их зараженными и поэтому не внедриться. Имеют ограниченное применение.

Действия при обнаружении компьютерных вирусов.

Если будут обнаружены зараженные объекты, надо попробовать их лечить. К сожалению, лечение не всегда возможно, так как некоторые вирусы необратимо портят информацию. В этом случае инфицированные объекты придется удалить.

Если вирусы не обнаружены, а компьютер продолжает вести себя "странно", если AVP выдаст сообщения о подозрительных файлах/секторах, рекомендуется обратиться к системному программисту или в отдел технической поддержки AVP.

Подробности действий пользователя в данном случае можно получить из справочной системы программы.