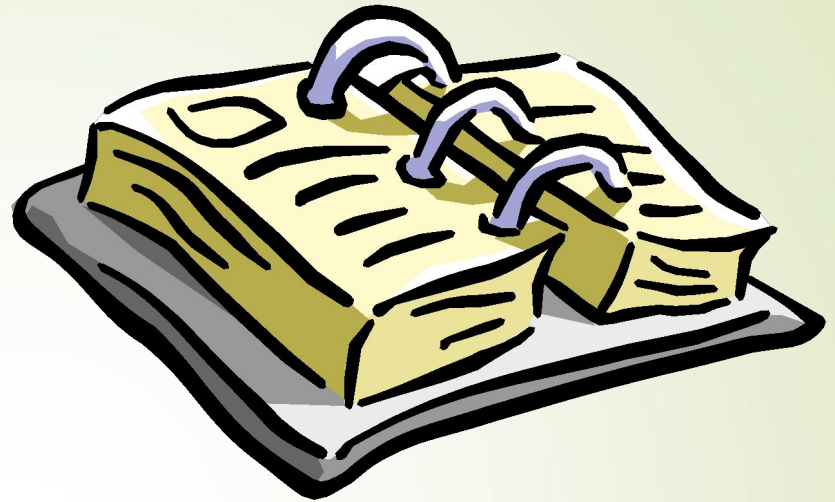


Компьютерные преступления и защита от них.

Содержание работы:

- введение;
- три главы;
- заключение;
- приложение;
- библиография;
- презентация.



Направления в работе:

Компьютерные преступления, вирусология в мировом масштабе

Методы и способы защиты от компьютерных преступлений в мире

Состояние законодательства и правоприменительная практика, способы защиты от вирусов на предприятии. Лекция



Часть 1

Компьютерные преступления - это преступления, совершенные с использованием компьютерной информации. При этом, компьютерная информация является предметом и (или) средством совершения преступления

Классификация компьютерных преступлений:

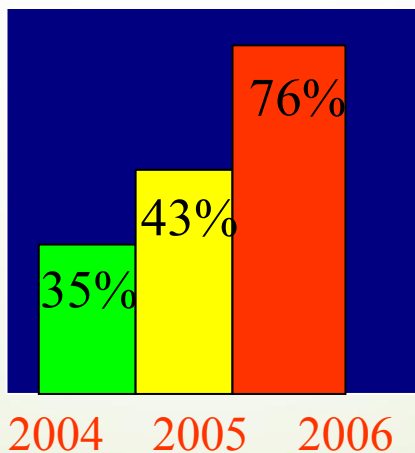
- Неправомерный доступ к охраняемой законом компьютерной информации.
- Создание, использование и распространение вредоносных программ для ЭВМ или машинных носителей с такими программами.
- Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Статистика компьютерных преступлений

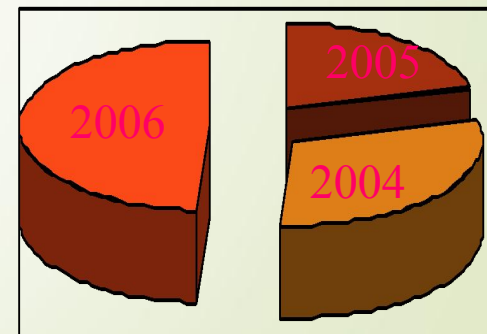
Кража денег



Утечка информации



Ущерб от компьютерной преступности



46% -2006 г

Компьютерные преступники

(хакеры)



Крэкеры(хакер)

Кардеры

Фрэкеры

Крэкеры (cracker-от слова «ВЗЛОМ»)

Крэкеры(хакеры) – лица, занимающиеся «взломом» (модификацией, блокированием, уничтожением) программно-аппаратных средств защиты компьютерной информации, охраняемых законом.

The screenshot shows a web browser window with the address bar containing 'eXPress Hak'. The page title is 'Взлом - просто и доступно' and the time is 15:35. The main content is titled 'Методы хакеров' and lists three methods: Спуфинг, Сниффинг, and Угон TCP. The author is listed as Радик Усманов and the email is unknown. The page footer includes copyright information: 'Copyright (c) 2001-2003 by HakerXP Designed by DesignXP'.

Методы хакеров

Спуфинг. Известно, что любая система защиты типа Firewall позволяет "жить" только определенным адресам IP. Это весьма серьезное препятствие для проникновения в сеть. Поэтому хакера нашли метод для преодоления этого барьера - спуфинг IP. Сначала хакер выясняет, какие IP проходят через firewall, затем использует один из вычисленных адресов для входа в систему. И firewall - M. D.

Сниффинг - один из самых популярных методов воровства данных в сети посредством специальных прог (снифферов). Снифферы, как правило, очень дорогое удовольствие, но рабруют безотказно!

Угон TCP. Хакеры-профи используют более действенные методы, например, угон TCP. Схема проста. Как только реальный юзер идентифицируется узлом, хакер переключает соединение на себя и передает в циклическом режиме по TCP ряд цифр до тех пор, пока не получает последовательность номеров, через которую можно подойти к середине сеанса связи, а затем отконнектить юзера. То есть, хакер угоняет весь сеанс регистрации!
Это далеко не все методы, используемые хакерами в наше время!

Автор: Радик Усманов
E-mail: неизвестен

Copyright (c) 2001-2003 by HakerXP
Designed by DesignXP

Фрэкеры (phreaker)



Фрэкеры — лица, специализирующиеся на совершении преступлений в области электросвязи с использованием конфиденциальной вариационной информации и специальных технических средств разработанных для негласного получения информации с технических каналов.



Кардеры (card)



Кардеры – профессиональные преступники, специализирующиеся на незаконной деятельности в сфере оборота пластиковых карт и их электронных реквизитов.

The screenshot shows the Haker.ru website. The top navigation bar includes links for HOME, SEARCH, CHAT, FORUMS, ADVERTISING, CONTACTS, and FOR AUTHORS. The main content area is divided into several sections:

- ЖУРНАЛ**: A sidebar menu with categories like КОЛОНКИ, ВЭЛОН, ЗАЩИТА, ЗАПАДЛО-СТРОЕНИЕ, ЖЕЛЕЗО, СОФТ, ОС, ЮМОР, ПОРНО, ХАЛЯВА, ЛИНКИ, МРЗ, Товары в Стиле "X", and Вакансии.
- Скоро в продаже Хакер #01**: A featured article about a new magazine issue, mentioning it's the first issue of 2005 and includes a subscription link.
- Открыта редакция Железо #01**: A sidebar advertisement for a magazine issue, mentioning a review of the Intel Celeron processor.
- Новости**: A section with several news items, including "Работа на сайте", "Новый обзор на нашем сайте", "Хакер подвергается в Великобритании жесткому контролю", "Рандом в 2004 г. самый популярный коллоид был Polydispersed", "С Новым Годом!", "Тема: Миссия выполнена, что 2005 г.д. назначается с вирусных атак", "В 2010 году 20% японцев будут телекоммуникации", "Впервые в мире с 2004 г. Рандом Software", "Независимая Инспекционная система независимыми в течение трех месяцев", "IDE: 3 технологии будущего", and "Китай уже построил себе сеть".
- Человек и чата 9**: A section with a "Войти, стат!" button and a link to "Повторяю на Новости".
- BUG TRACK/**: A section with several bug reports, including "Взломанный сайт 88.8.1.2003", "Поврежден сканер при загрузке файлов в Mozilla", "Обновляемость в OJINWiki", "Взломанный сайт 05.01.2005", "Простор конфигурационных файлов в MySQL", "Данная и выложена проанализированная информация в GNUWord", "Открыта психика сайта FTP клиента IE и Konqueror", "Экспloit для WINS", "Экспloit для Win2000", and "Назвонившая Рассветы".

Компьютерные вирусы

(классификация)

```
graph TD; A[Компьютерные вирусы] --> B[Файловые]; A --> C[Загрузочные]; A --> D[Макро-вирусы]; A --> E[Сетевые];
```

Файловые

Загрузочные

Макро-вирусы

Сетевые

«ТРОЯНСКИЙ КОНЬ»



Троянский конь -

заключается в тайном введении в чужое программное обеспечение вредоносной программы для ЭВМ, которая позволяют негласно осуществлять иные, не планировавшиеся разработчиком программы функции. Эти средства совершения преступления используют для негласного добывания конфиденциальных сведений, например, логина и пароля доступа в сеть ЭВМ "Интернет"

«ЛОГИЧЕСКАЯ БОМБА»

Логическая бомба - тайное встраивание в программу для ЭВМ потерпевшего вредоносной программы для ЭВМ (программного модуля), которая должна сработать лишь однажды при наступлении определенных логических условий. При этом "бомба" автоматически ликвидируется при окончании исполнения заданного преступником вредоносного алгоритма.



«КОМПЬЮТЕРНЫЙ ЧЕРВЬ»

Червь - саморазмножающийся и самораспространяющийся вирус, который специально создан для функционирования в сети ЭВМ. Он хранит свои модули на нескольких компьютерах - рабочих станциях сети. При уничтожении модулей на соответствующем числе рабочих станций, она автоматически воссоздает их после каждого подключения "вылеченного" компьютера к сети - как разрезанный на части дождевой червяк отращивает новые, недостающие участки тела. Червь, помимо своего оригинального алгоритма, может являться "средством передвижения" обычных вирусов, троянских коней, логических бомб.



«ЗЛЫЕ ШУТКИ НА ПК»



«Шутки» - программы, которые не причиняют компьютеру какого-либо вреда, однако выводят сообщения о том, что он уже причинён или компьютеру грозит несуществующая опасность.



Часть 2

Меры противодействия компьютерным преступлениям

Технические

- Защита от несанкционированного доступа
- Создание резервных копий
- Спецпрограммы безопасности

Организационные

- Охрана компьютерных систем
- Подбор персонала
- Другие оргмеры

Правовые

- Совершенствование законодательства
- Защита авторских прав
- Информированность пользователей ПК

Нормативно-правовая база РФ в области компьютерных преступлений

Законы



Указы



Положения



Законы

- О правовой охране программ для ЭВМ и баз данных
 - О правовой охране топологий интегральных микросхем
 - Об информации, информатизации и защите информации
 - Об участии в международном информационном обмене
 - О государственной тайне
 - Об авторском праве и смежных правах
- И т.д.

УКАЗЫ И ПОЛОЖЕНИЯ

О Концепции правовой информатизации России
Доктрина информационной безопасности России
Утверждение Положения о Межведомственной комиссии
по защите гос. тайны
Об упорядочении организации и проведения
оперативно-розыскных мероприятий
с использованием технических средств
И т.д.

Типы антивирусных программ (классификация)

```
graph TD; A[Типы антивирусных программ (классификация)] --> B[Полифаги]; A --> C[Ревизоры]; A --> D[Блокировщики];
```

Полифаги

Ревизоры

Блокировщики



Часть 3

Как уберечься от компьютерных вирусов?

1. Покупайте только лицензионное ПО.
2. Создайте системную дискету (или диск).
3. Делайте регулярное резервное копирование наиболее важных файлов.
4. Проверяйте перед использованием все дискеты, диски и флэшки, принесенные из вне.
5. Ограничьте доступ к ПК.
6. Проверяйте ПК на наличие вирусов постоянно (*не забывайте обновлять антивирусные программы*)