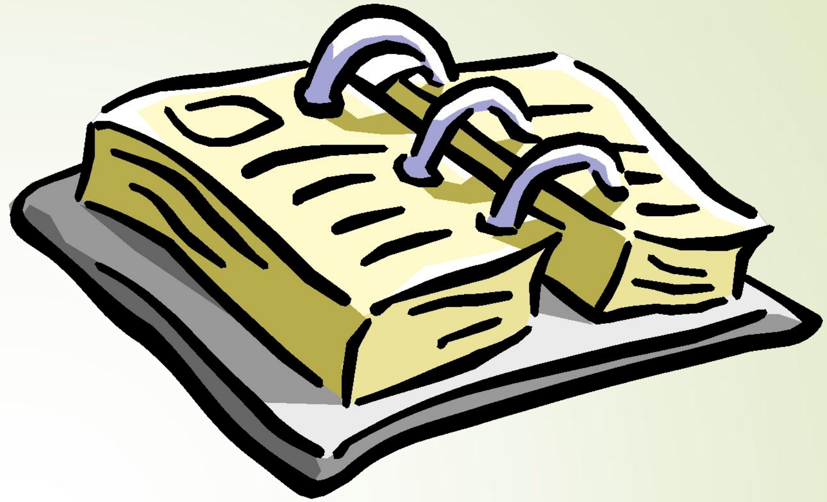
Компьютерные преступления и защита от них.

Содержание работы:

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



Направления в работе:

Компьютерные преступники, вирусология в мировом масштабе

Методы и способы защиты от компьютерных преступлений в мире

Состояние аппаратного и программного обеспечения, способы защиты от вирусов на предприятиях г. Покачи

Часть 1

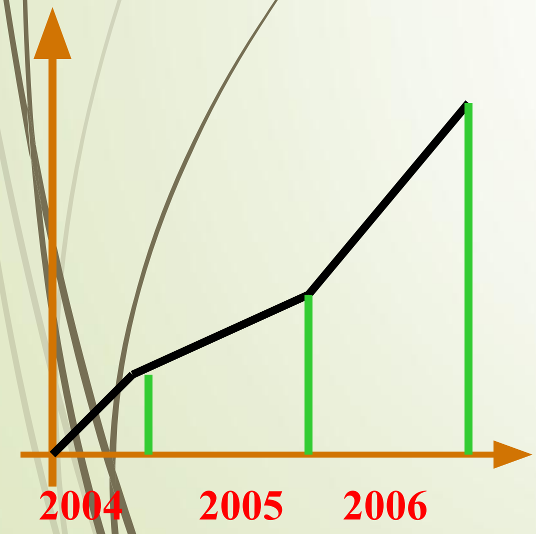
Компьютерные преступления - это преступления, совершенные с использованием компьютерной информации. При этом, компьютерная информация является предметом и (или) средством совершения преступления

Классификация компьютерных преступлений:

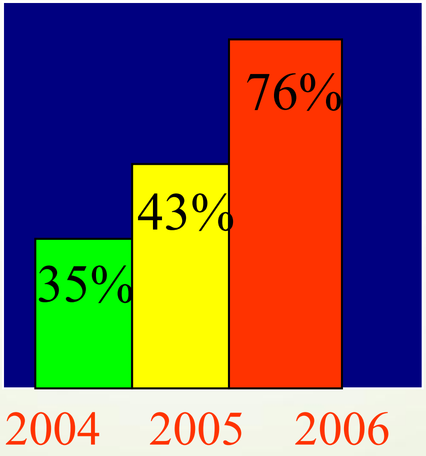
- Неправомерный доступ к охраняемой законом компьютерной информации.
- Создание, использование и распространение вредоносных программ для ЭВМ или машинных носителей с такими программами.
- Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Статистика компьютерных преступлений

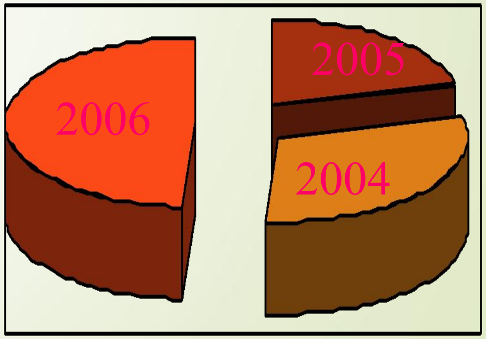
Кража денег



Утечка информации



Ущерб от компьютерной преступности



46% -2006 г

2004-2006 г (по данным журнала Message Labs)

Компьютерные преступники

(хакеры)

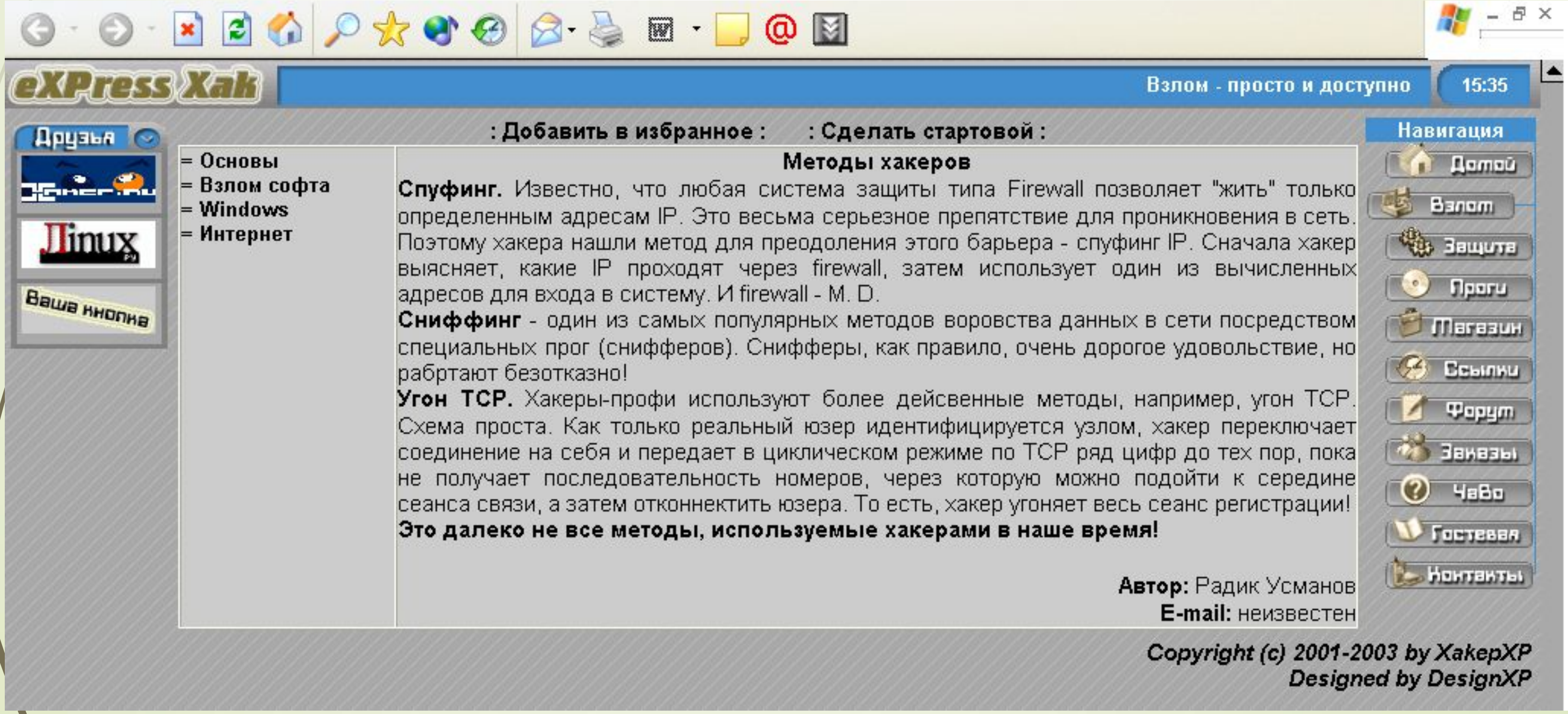
Крэкеры(хакер)

Кардеры

Фрэкеры

Крэкеры (cracker-от слова «взлом»)

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

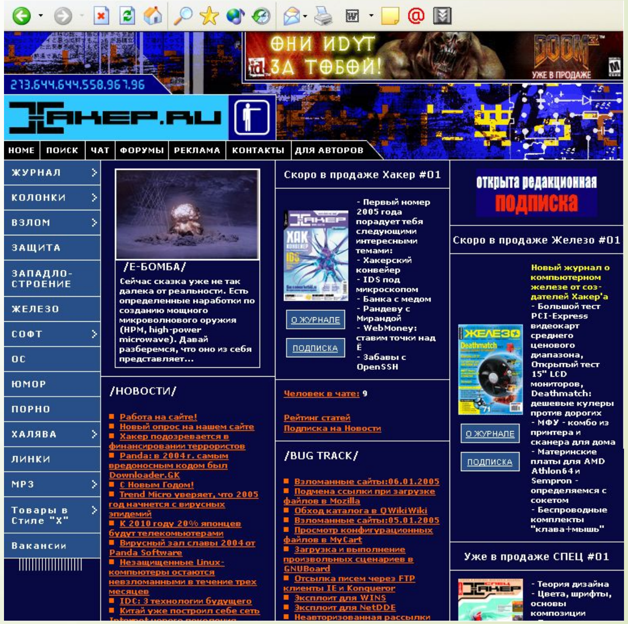


Фрэкеры (phreacker)

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.



Компьютерные вирусы

(классификация)

Сетевые

Файловые

Загрузочные

Макро-вирусы

«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 несанкциониро-ванного доступа
- Создание резервных копий
- Спецпрограммы безопасности

Организационные

- Охрана компьютерных систем
- Подбор персонала
- Другие оргмеры

Правовые

- Совершенствова-ние Законодательства
- Защита авторских прав
- Информирован-ность 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)

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)*