

Муниципальное образовательное учреждение:
«Средней общеобразовательной школы №4»

Компьютерные преступления и защита от них.

Работу выполнил:

Солодкий А. С,
ученик 10-Б класса

Руководитель проекта:

Тимофеева Е. Р,
учитель ОИВТ

Цель исследования:

Классификация и анализ компьютерных правонарушителей и преступлений; методы противодействия компьютерным правонарушениям.

Объект исследования:

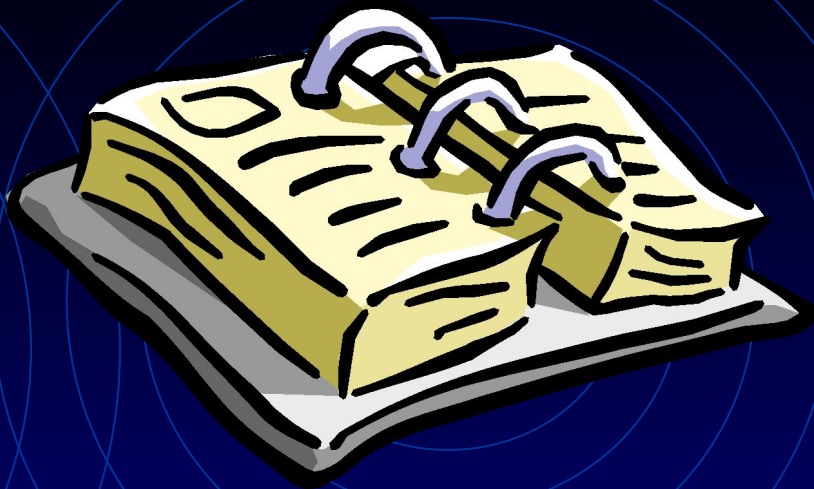
Правонарушения в компьютерной области, нормативно-правовая база данной сферы, меры защиты информации.

Задачи исследования:

1. Изучение научной, учебной литературы по исследуемому предмету.
2. Систематизация и обобщение опыта работ по данной проблеме.
3. Изучение причин и сущности совершения компьютерных преступлений в мировом масштабе, а также нормативно-правовую базу и методы защиты от компьютерных преступлений.
4. Изучение состояния аппаратных и программных средств, а также наиболее серьезных вирусов, причиняющих вред ПК, анализ способов и методов защиты программного обеспечения, применяемых на предприятиях города Покачи.

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 статистики и прогнозности обеспечения, способы защиты от вирусов на предприятиях России



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.

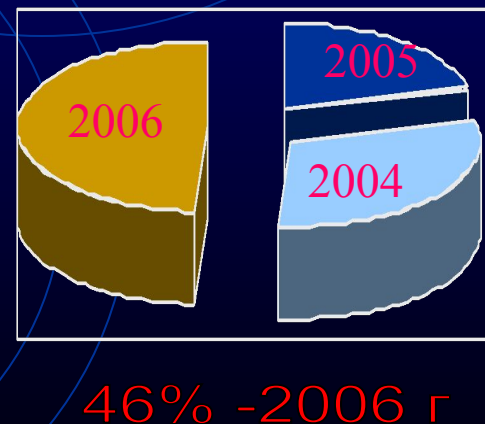
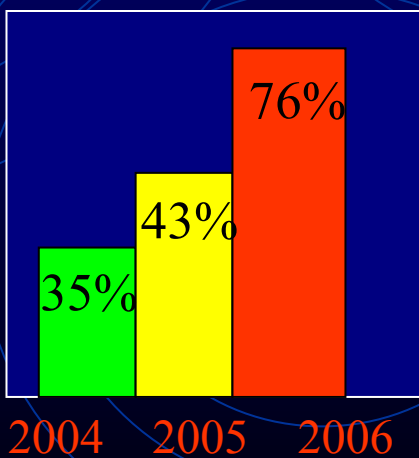
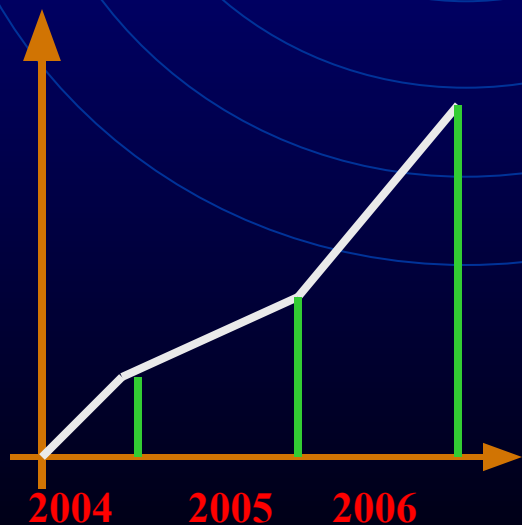
Статистика компьютерных преступлений

Кража денег



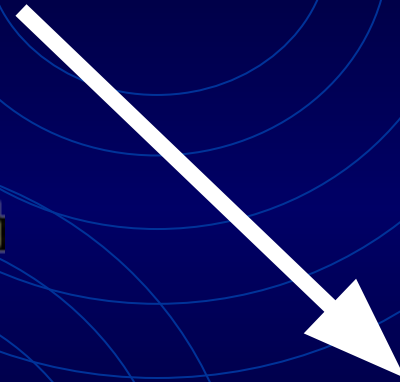
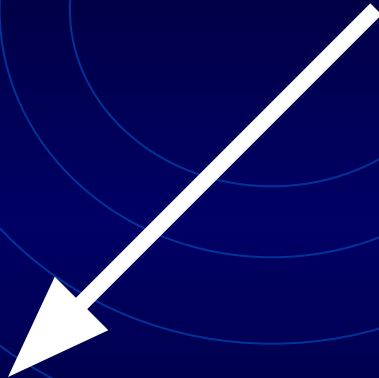
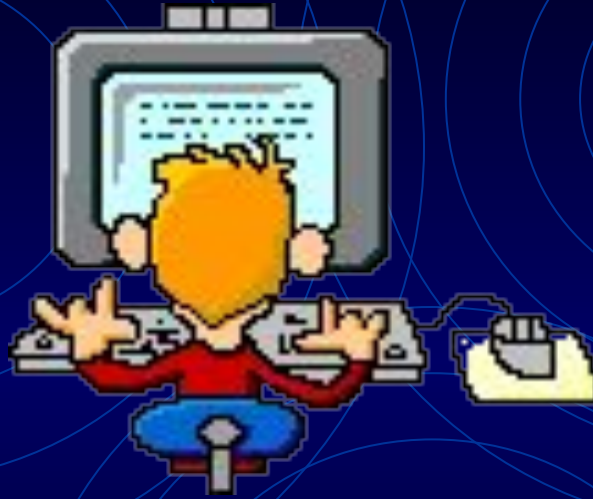
Ущерб от компьютерной преступности

Утечка информации



Компьютерные преступники

(хакеры)



Крэкеры

Кардеры



Фрэкеры

Крэкеры (cracker)

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

<http://www.xakerxp.by.ru/>

eXPress Hak Взлом - просто и доступно 15:35

Друзья

- Основы
- Взлом софта
- Windows
- Интернет

Ваша кнопка

Добавить в избранное : Сделать стартовой :

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 рабтрают 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

Навигация

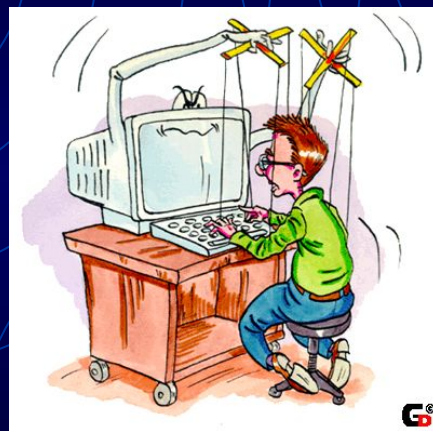
- Домой
- Валют
- Защита
- Проги
- Магазин
- Ссылки
- Форум
- Знаквы
- ЧВВ
- Гостевая
- Контакты

Copyright (c) 2001-2003 by XakerXP
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.



Пранки

Боксирьы

Кардеры (card)



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

<http://www.geocities.com/SiliconValley/Park/8783/>

The screenshot shows the website 'ХАКЕР.RU' with a navigation menu and several content sections:

- Журнал**: 'Скоро в продаже Хакер #01'. Description: 'Первый номер 2005 года порадует тебя следующими интересными темами: Хакерский конвейер, IDS под микроскопом, Банка с медом, Рандеву с Мирандой, WebMoney: ставим точки над Е, Забавы с OpenSSH'. Buttons: 'О ЖУРНАЛЕ', 'ПОДПИСКА'.
- Железо**: 'Открыта редакционная подписка'. Description: 'Новый журнал о компьютерном железе от создателей Хакер'a'. Includes 'Большой тест PCI-Express видеокарт среднего диапазона, Открытый тест LCD мониторов, Deathmatch: дешевые кулеры против дорогих - МФУ - комбо из принтера и сканера для дома - Материнские платы для AMD Athlon 64 и Sempron - определяемся с socketом - Беспроводные комплекты "клава+мышь"'. Buttons: 'О ЖУРНАЛЕ', 'ПОДПИСКА'.
- Новости**: 'Человек в чате: 9'. 'Рейтинг статей Подписка на Новости'. 'Bug Track': 'Взломанные сайты: 06.01.2005', 'Подмена ссылки при загрузке файлов в Mozilla', 'Обход каталога в OWikiWiki', 'Взломанные сайты: 05.01.2005', 'Просмотр конфигурационных файлов в MySQL', 'Загрузка и выполнение произвольных сценариев в PHPexec', 'Отсылка писем через FTP клиенты IE и Konqueror', 'Эксплоит для WINS', 'Эксплоит для NetDDE', 'Неавторизованная рассылки'.
- ЖЕЛЕЗО**: 'ЖЕЛЕЗО Deathmatch'.
- Уже в продаже СПЕЦ #01**: 'Теория дизайна - Цвета, шрифты, основы композиции'.

21 ВЕК

Громкие компьютерные преступления



Компьютерные вирусы

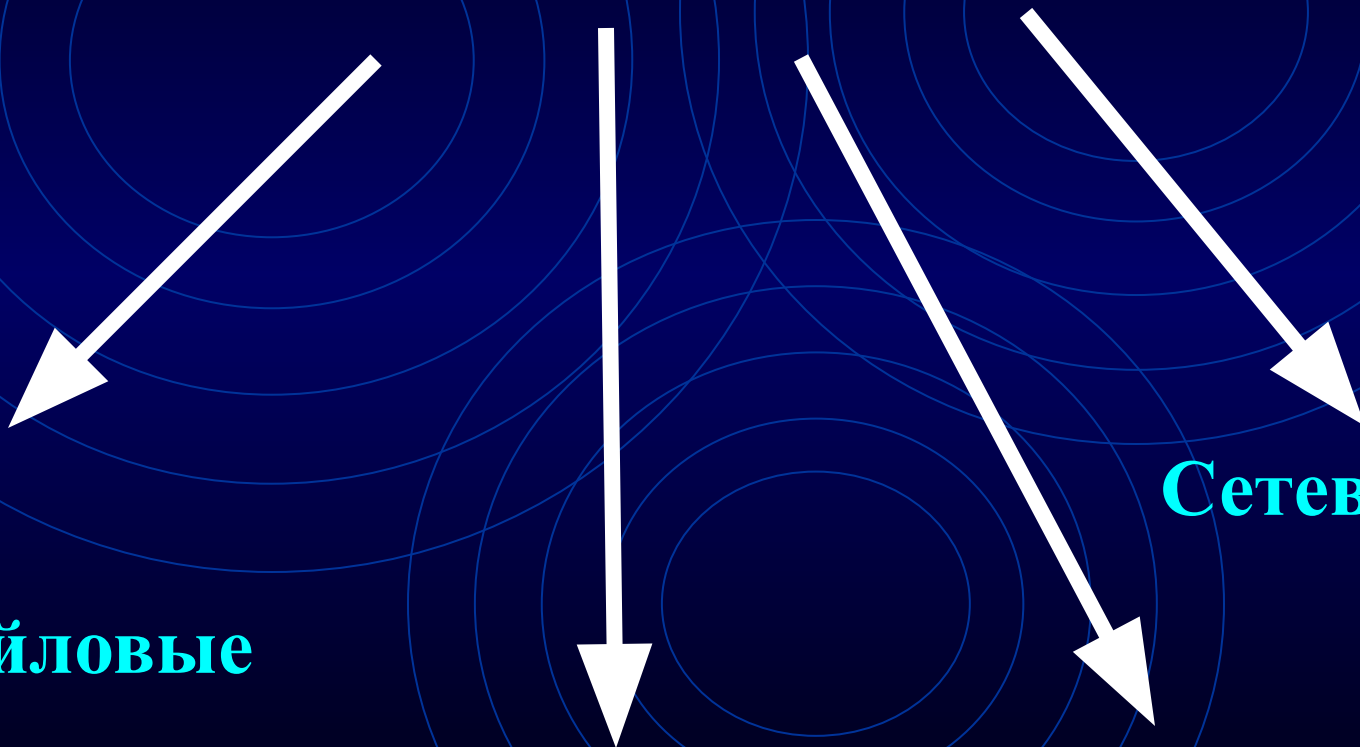
(классификация)

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»

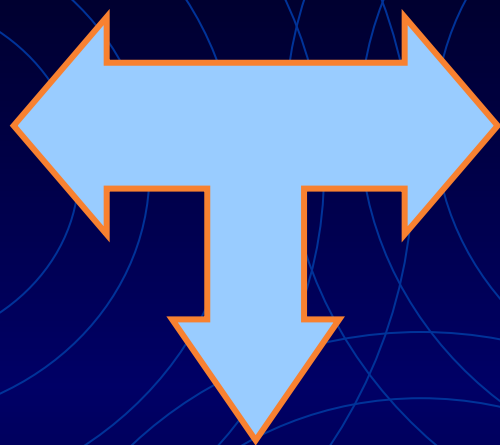


«Шутки» - программы, которые не причиняют компьютеру какого-либо вреда, однако выводят сообщения о том, что он уже причинён или компьютеру грозит несуществующая опасность.



Часть 2

Меры противодействия компьютерным преступлениям



Технические

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

Организационные

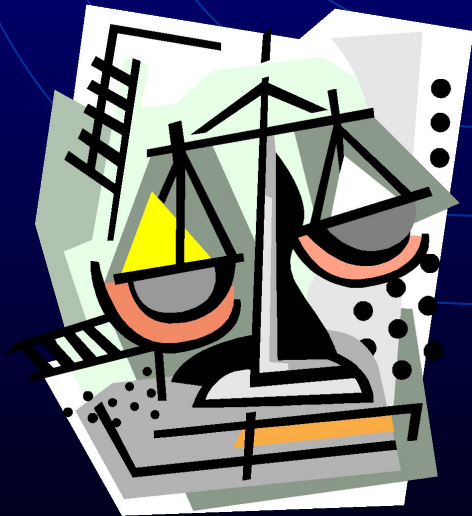
- Охрана компьютерных систем
- Подбор персонала
- Другие оргмеры

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
- Об электронной цифровой подписи
- О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт
- Об органах федеральной службы безопасности (ФСБ)
- О связи
- Об оперативно-розыскной деятельности
- О милиции

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
- Об обороте специальных технических средств (СТС), предназначенных для негласного получения информации
- О мерах по соблюдению законности в области оборота шифровальных средств и предоставления услуг в области шифрования информации
- Соглашение стран СНГ о сотрудничестве в борьбе с компьютерными преступлениями

Типы антивирусных программ (классификация)

The diagram features a central title at the top. Three white arrows originate from the title area and point downwards to three separate labels. The background consists of several overlapping, concentric circles in a light blue color.

Полифаги

Блокировщики

Ревизоры

Адреса сайтов организаций по защите информации

<http://www.fssr.ru/> - Институт криптографии, связи и информатики ФСБ РФ;

<http://www.infosec.ru/> - НИП "Информзащита";

<http://www.novocom.ru/> - Учебно-технический центр "НОВО-УТЦ";

<http://www.confident.ru/> - ООО "Конфидент"; журнал "Защита информации.";

<http://www.spymarket.com/> - Компания "Смерш Техникс";

<http://www.pps.ru/> - Лаборатория "ППШ" (профессиональная защита тайны);

<http://www.kiberpol.ru/> - Сайт киберполиции

<http://www.ankey.ru/> - Фирма "Анкей" (криптографические системы защиты);

<http://www.ssl.stu.neva.ru/> - Санкт-Петербургский центр защиты информации;

<http://www.security.ru/> - Московское отделение НИИ защиты информации

<http://www.infotecs.ru/gtc> - Государственная техническая комиссия при
Президенте РФ;



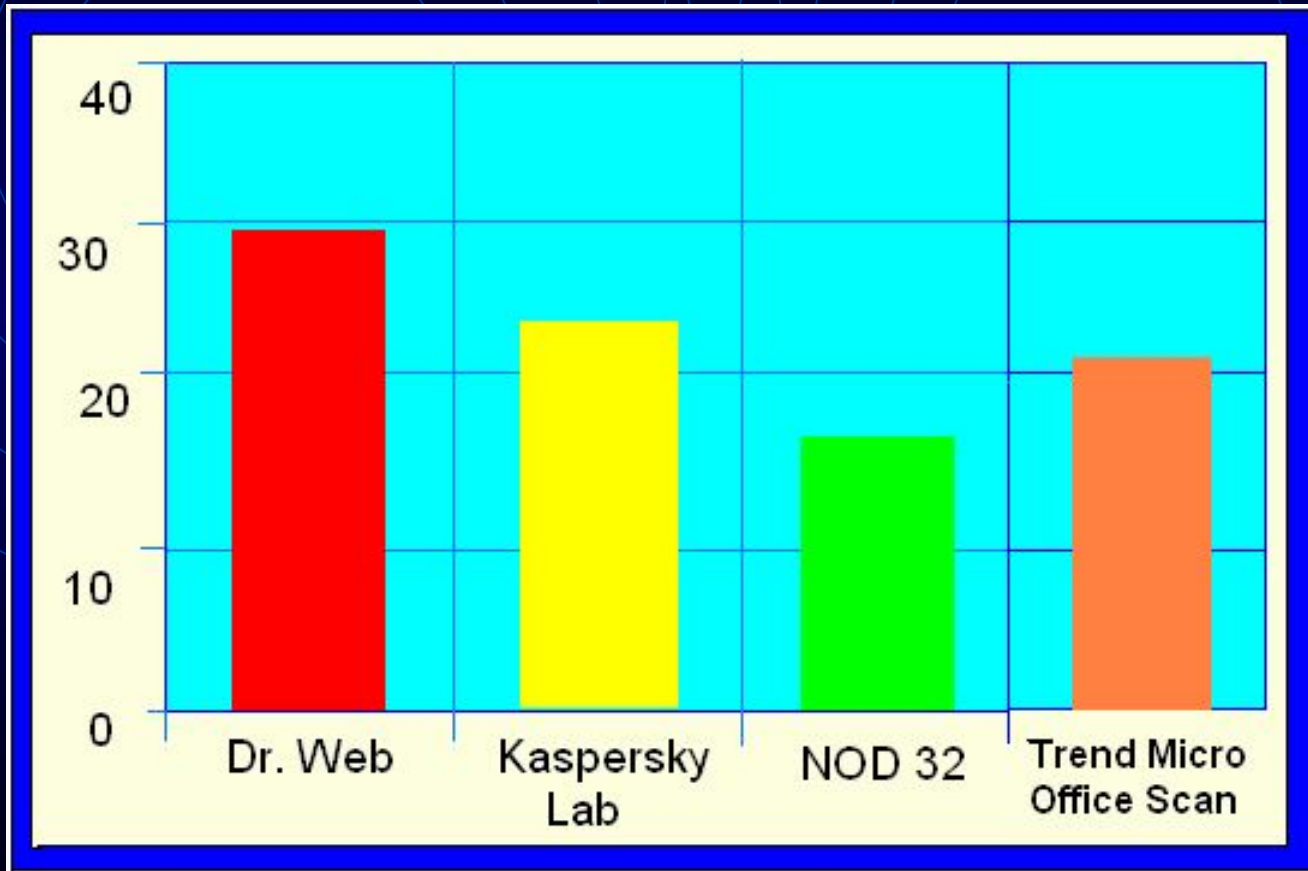
Часть 3

Вирусы, встречающиеся в программном обеспечении предприятий г.Покачи:

- 1 место – Компьютерные черви (TWIKER's, Worm)
- 2 место – Троянские кони (Trojan's)
- 3 место – Логические бомбы замедленного действия (Wilkers - Word)



Популярность антивирусных программ на
предприятиях г. Подачи
(по критерию эффективности) :



Помни!!!



Абсолютной защиты не существует!

Но!!!

**Свести риск потерь к минимуму
возможно!**



Там, где есть преступление - там есть и наказание!

Безопасности не бывает много.

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*)



Спасибо за внимание!