Компьютерная преступность и безопасность. Компьютерные преступления в Уголовном кодексе РФ.

Виды компьютерных преступлений

Несанкционированный доступ к информации.

Разработка и распространение вирусов.

Подделка компьютерной информации.

Ввод логических бомб.

Преступная небрежность в разработке.

Хищение компьютерной информации.

Предупреждение компьютерных преступлений

Известно много мер, направленных на предупреждение преступления:

- Технические
- Организационные
- Правовые

Технические

-защита от несанкционированного доступа к системе

-резервирование особо важных компьютерных подсистем

-организация вычислительных сетей

-установка противопожарного оборудования

-оснащение замками, сигнализациями

Организационные

-охрана вычислительного центра

-тщательный подбор персонала

-наличие плана восстановления работоспособности(после выхода из строя)

-универсальность средств защиты от всех пользователей

Правовые

-разработка норм, устанавливающих ответственность за компьютерные преступления

-защита авторских прав программистов

-совершенствование уголовного и гражданского законодательства

Классификация сбоев и нарушений:

- Сбои оборудования.
- Потеря информации из-за некорректной работы ПО.
- Потери, связанные с несанкционированным доступом.
- Потери, связанные с неправильным хранением архивных данных.
- Ошибки обслуживающего персонала и

Способы защиты информации:

- Шифрование.
- Физическая защита данных.Кабельная система.
- Системы электроснабжения.
- Системы архивирования и дублирования информации.

Шифрование

On-Line
(в темпе поступления информации)

Off-Line
(автономном)

-DES(правительственный стандарт для шифрования цифровой информации)

-RSA(стандарт Национального Бюро Стандартов)

Физическая защита. Кабельная система.

- Структурированные кабельные системы.
- Аппаратные кабельные системы.
- Административные подсистемы.

Программные и программно-аппаратные методы защиты

Защита от компьютерных вирусов.

Защита от несанкциони - рованного доступа

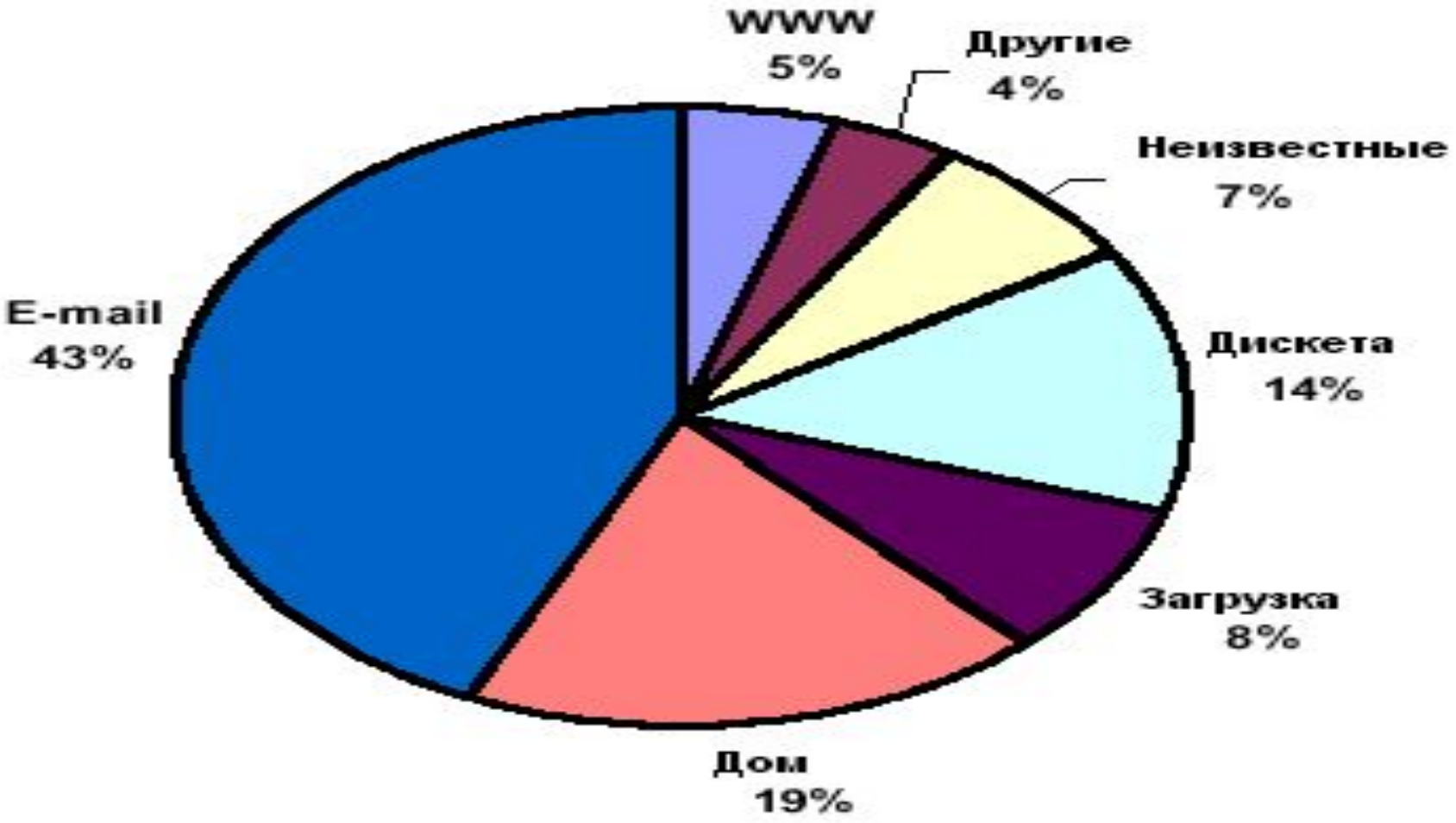
Защита информации при удаленном доступе

Защита от компьютерных вирусов.

- 64% из 451 специалистов испытали «на себе» их действие
- 100-150 новых штаммов ежемесячно
- Методы защиты - антивирусные программы


0,3%
2,7%
40,9%
56,1%
Windows-вирусы
Макро-вирусы
Скрипт-вирусы
Другие

Источники вирусной инфекции (Бюллетень ICSA, 1999 год)



Защита от несанкционированного доступа

- Обострилась с распространением локальных, глобальных компьютерных сетей.
- Разграничение полномочий пользователя.
- Используют встроенные средства сетевых операционных систем.
- Комбинированный подход – пароль +идентификация по персональному ключу.
- Смарт – карты.

Защита информации при удалённом доступе

- Используются кабельные линии и радиоканалы.
- Сегментация пакетов.
- Специальные устройства контроля.
- Защита информации от хакеров.

Неправомерный доступ к информации

- «Законодательство в сфере информации»
- С 1991 по 1997-10 основных законов:

-определяются основные термины и понятия.

-регулируются вопросы о распространении информации.

-охрана авторских прав.

-имущественные и неимущественные отношения.

Ст.273 УК РФ.

- Предусматривает уголовную ответственность за создание программ для ЭВМ или их модификацию, приводящие к несанкционированному уничтожению.
- Защищает права владельца.
- Уголовная ответственность – в результате создания программы.
- Для привлечения достаточен сам факт создания программ.

Каков же итог?

- Никакие аппаратные, программные решения не смогут гарантировать абсолютную безопасность.
- Свести риск к минимуму - при комплексном подходе.
- Позитивность произошедших перемен в правовом поле очевидна.