Компьютерная преступность и безопасность

Первым человеком, применившим ЭВМ для совершения налогового преступления на сумму 620 тыс. долларов и в ***1969 г.*** представшим за это перед американским судом, стал Альфонсе Конфессоре.
Дальнейшая история компьютерных преступлений отмечена такими наиболее "яркими" событиями:
конец 70-х - "ограбление" "Секьюрити пасифик бэнк" (10,2 млн. долларов);
1979 г. - компьютерное хищение в Вильнюсе (78584 руб.);
1984 г. - сообщение о первом в мире "компьютерном вирусе";
1985 г. - вывод из строя при помощи "вируса" электронной системы голосования в
конгрессе США;
1987-1988 гг. - появление первого "компьютерного вируса" в СССР;
1989 г. - блокировка американским студентом 6000 ЭВМ Пентагона;
международный съезд компьютерных "пиратов" в Голландии с демонстрацией
возможности неограниченного внедрения в системы ЭВМ;
1991 г. - хищение во Внешэкономбанке на сумму в 125,5 тыс. долларов;
1992 г. - умышленное нарушение работы АСУ реакторов Игналинской АЭС;
1993 г. - неоконченное электронное мошенничество в Центробанке России (68 млрд. руб.);
1995 г. - попытка российского инженера украсть из Сити - банка 2,8 млн. долларов.

Виды компьютерных преступлений

Несанкционированный доступ к информации, хранящейся в компьютере

Несанкционированный доступ

- использование чужого имени;
- изменение физических адресов технических устройств;
- использование информации, оставшейся после решения задач;
- модификация программного и информационного обеспечения;
- хищение носителя информации;
- установка аппаратуры записи.

Несанкционированный доступ

Хакеры - Гудини информационных сетей.

Взлом и копание в чужой информации:

- развлечение;
- бизнес.

Несанкционированный доступ

Несанкционированный доступ к файлам законного пользователя осуществляется нахождением слабых мест в защите системы.

Несанкционированный доступ

Некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами **аутентичной идентификации** (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т.п.) , оказываются без защиты против этого приема. Самый простой путь его осуществления - получить **коды** и другие идентифицирующие **шифры** законных пользователей.

Несанкционированный доступ

Иногда случается, как, например, с ошибочными телефонными звонками, что пользователь с удаленного терминала подключается к чьей-то системе, будучи абсолютно уверенным, что он работает с той системой, с какой и намеривался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение определенного времени и таким образом получить некоторую информацию, в частности коды.

Несанкционированный доступ

В любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ, своеобразный аналог приспособлений, помещаемых в транспорте под надписью "Разбить стекло в случае аварии". Такая программа - мощный и опасный инструмент в руках злоумышленника.

Несанкционированный доступ

Несанкционированный доступ может осуществляться и в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных. Все происходит так, словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у хранилища нет одной стены. В таком случае он может проникнуть в чужие сейфы и похитить все, что в них хранится.

Ввод в программное обеспечение "логических бомб".

логическая бомба

Способ "троянский конь" состоит в тайном введении в чужую программу таких команд, которые позволяют осуществить новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность. С помощью "троянского коня" преступники, например, отчисляют на свой счет определенную сумму с каждой операции.

логическая бомба

В США получила распространение форма компьютерного вандализма, при которой "троянский конь" разрушает через какой-то промежуток времени все программы, хранящиеся в памяти машины. Во многих поступивших в продажу компьютерах оказалась "временная бомба", которая "взрывается" в самый неожиданный момент, разрушая всю библиотеку данных.

логическая бомба

Многие заказчики прекрасно знают, что после конфликтов с предприятием-изготовителем их программное обеспечение, которое до сих пор прекрасно работало, вдруг начинало вести себя самым непредсказуемым образом и, наконец, полностью отказывало. Нетрудно догадаться, что и копии на магнитных лентах или дисках, предусмотрительно сделанные, положения нисколько не спасали.

Разработка и распространение компьютерных вирусов.

компьютерные вирусы

Все вирусы можно разделить на две разновидности, обнаружение которых различно по сложности: "вульгарный вирус" и "раздробленный вирус". Программа "вульгарного вируса" написана единым блоком, и при возникновении подозрений в заражении компьютера эксперты могут обнаружить ее в самом начале эпидемии (размножения).

компьютерные вирусы

Программа "раздробленного вируса" разделена на части, на первый взгляд, не имеющие между собой связи. Эти части содержат инструкции которые указывают компьютеру как собрать их воедино, чтобы воссоздать и, следовательно, размножить вирус. Таким образом, он почти все время находится в "распределенном" состоянии, лишь на короткое время своей работы, собираясь в единое целое. Как правило, создатели вируса указывают ему число репродукций, после достижения которого он становится агрессивным.

компьютерные вирусы

Вирусы могут быть внедрены в операционную систему, в прикладную программу или в сетевой драйвер.

компьютерные вирусы

В августе 1984 года студент Калифорнийского университета Фред Коуэн, выступая на одной из конференций, рассказал про свои опыты с тем, что один его друг назвал "компьютерным вирусом". Когда началось практическое применение вирусов, неизвестно, ибо банки, страховые компании, предприятия, обнаружив, что их компьютеры заражены вирусом, не допускали, чтобы сведения об этом просочились наружу.

компьютерные вирусы

Распространение компьютерных вирусов имеет и некоторые положительные стороны. В частности, они являются, по-видимому, лучшей защитой от похитителей программного обеспечения. Зачастую разработчики сознательно заражают свои дискеты каким-либо безобидным вирусом, который хорошо обнаруживается любым антивирусным тестом. Это служит достаточно надежной гарантией, что никто не рискнет копировать такую дискету.

Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.

небрежность

Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти недостижима.

Подделка компьютерной информации

Подделка компьютерной информации

Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

Подделка компьютерной информации

К подделке информации можно отнести также подтасовку результатов выборов, голосований, референдумов и т.п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые

Хищение компьютерной информации

Хищение компьютерной информации

Присвоение компьютерной информации, в том числе программного обеспечения, путем несанкционированного копирования не квалифицируется как хищение, поскольку хищение сопряжено с изъятием ценностей из фондов организации. Не очень далека от истины шутка, что у нас программное обеспечение распространяется только путем краж и обмена краденым.

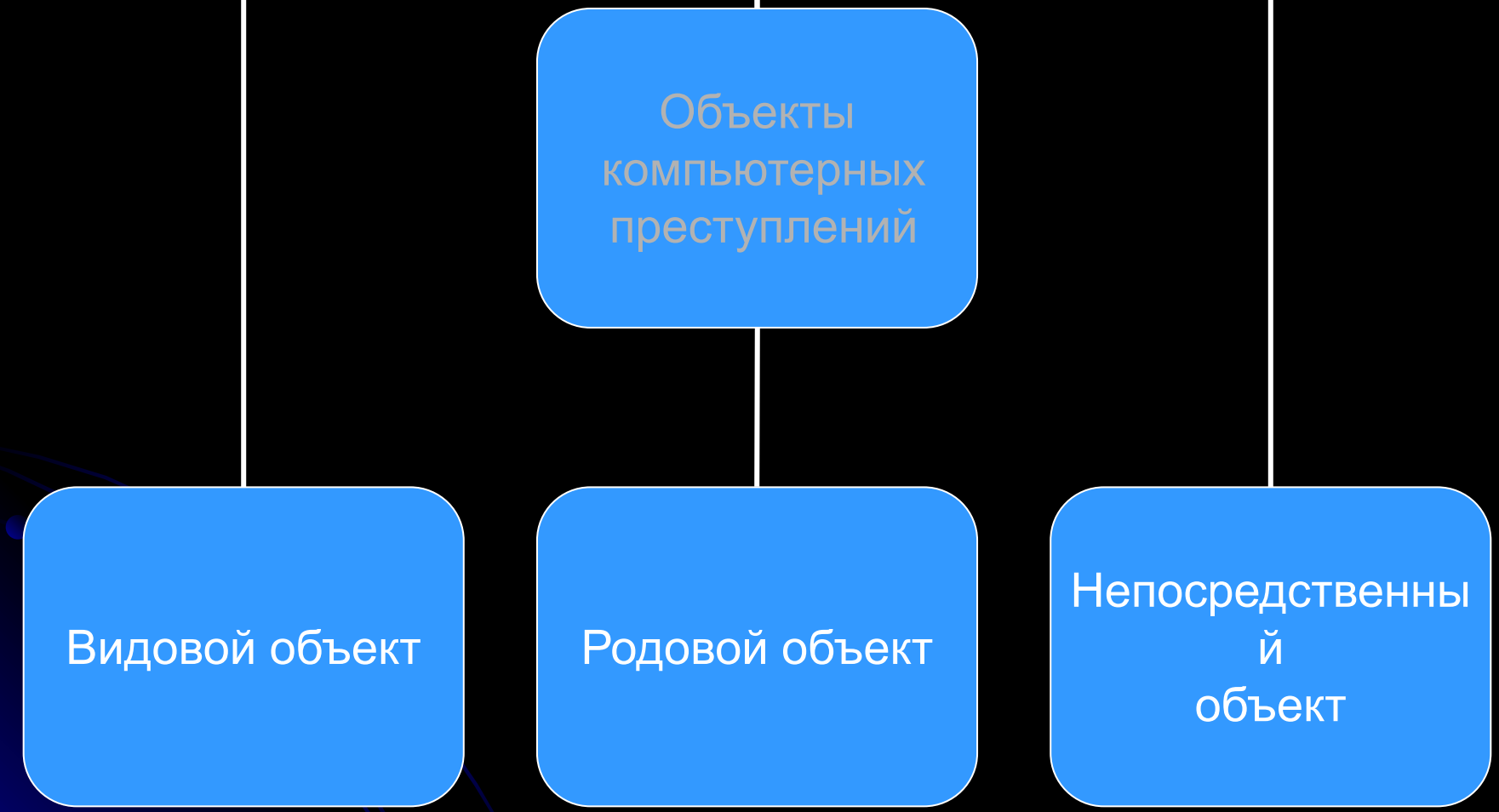
Хищение компьютерной информации

Вторая категория преступлений, в которых компьютер является "средством" достижения цели. Здесь можно выделить разработку сложных математических моделей, входными данными, в которых являются возможные условия проведения преступления, а выходными данными -- рекомендации по выбору оптимального варианта действий преступника.

Хищение компьютерной информации

Другой вид преступлений с использованием компьютеров получил название "воздушный змей".

Объекты компьютерных преступлений



Видовой объект компьютерных преступлений

общественные отношения, нарушающие формирование и использование автоматизированных информационных ресурсов и средств их обеспечения

- права и законные интересы владельцев и пользователей информации, компьютеров, средств обеспечения
- права и законные интересы физических и юридических лиц
- права и законные интересы общества и государства

Объективная сторона компьютерных преступлений

- действие
- бездействие

Субъективная сторона

- умышленная вина
- ч. 2 ст. 273 УК РФ и ч. 2 ст. 274 УК РФ – две формы вины: в целом являются умышленными

Субъект компьютерного преступления

Общий	***Специальный субъект*** (ст. 274; ч. 2 ст. 272 УК РФ)
лицо, достигшее 16 лет	лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети

Компьютерная информация

сведения о лицах, предметах, фактах, событиях, явлениях и процессах

Записанные в электронном виде

Хранящиеся на машинном носителе

Хранящиеся в ЭВМ

Компьютерное преступление

Преступление в сфере компьютерной информации – это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных.

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 пользователей.

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

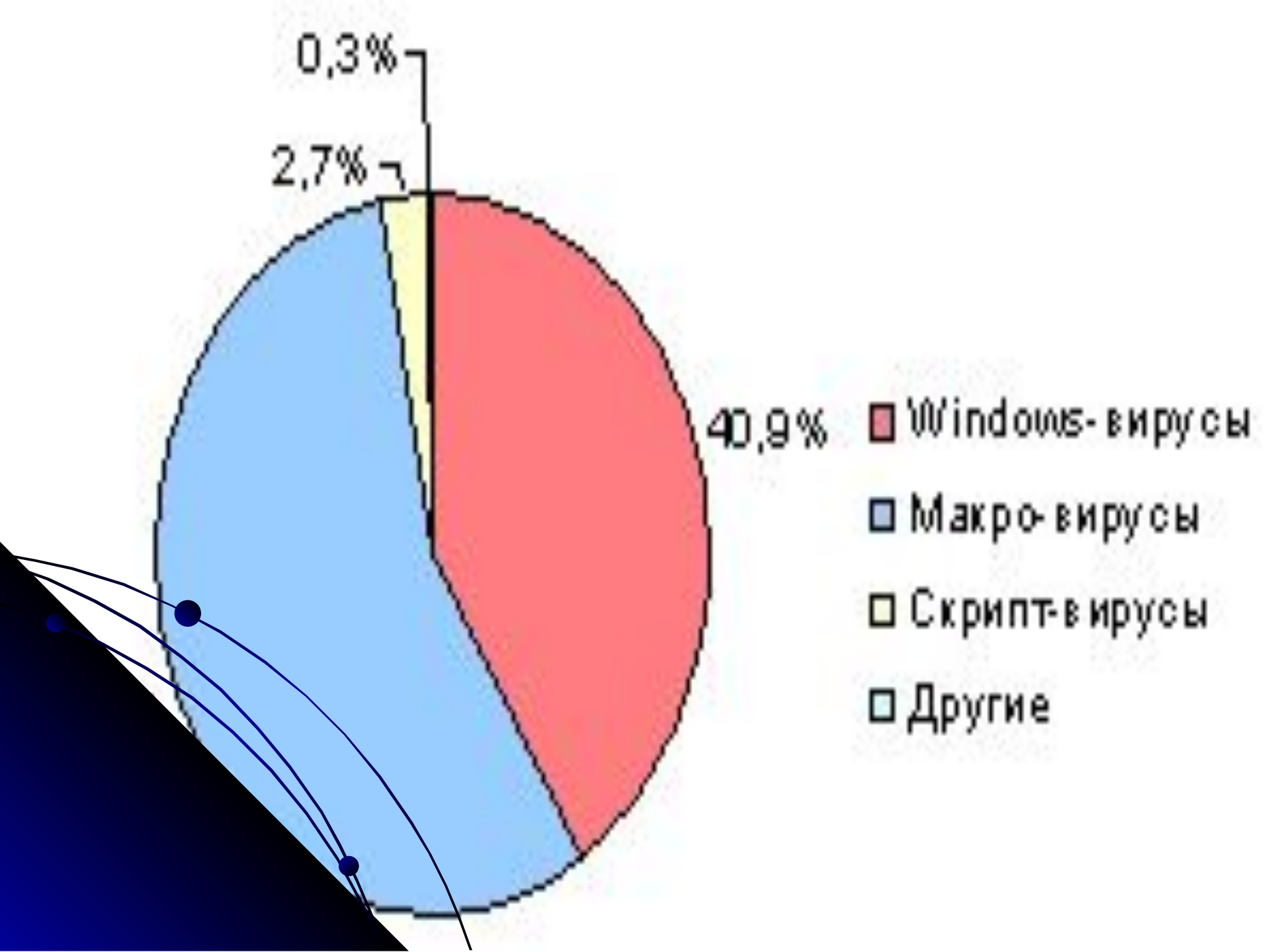
Защита от компьютерных вирусов.

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%
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.

Компьютерные преступления в Уголовном кодексе РФ

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?

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.