

Информационная безопасность

Информационные преступления и информационная безопасность

Жизненно важной для общества становится проблема информационной безопасности действующих систем хранения, передачи и обработки информации.



Потери от хищения или повреждения компьютерных данных составляют более 100 млн. долларов в год



Каждые 20 секунд в США происходит преступление с использованием программных средств

Более 80 % компьютерных преступлений осуществляется через глобальную сеть Интернет

Информационная среда – это совокупность условий, средств и методов на базе компьютерных систем, предназначенных для создания и использования информационных ресурсов

Информационная безопасность – совокупность мер по защите информационной среды общества и человека.

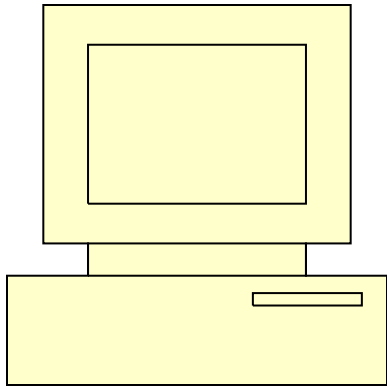


Цели обеспечения информационной безопасности

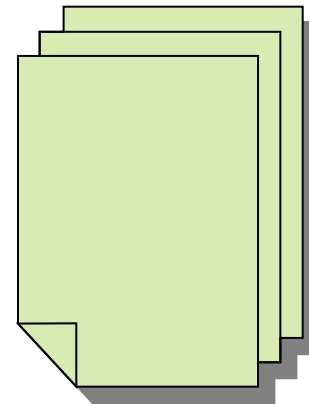
**Защита
национальных
интересов**

Обеспечение
человека и
общества
достоверной и
полной
информацией

Правовая защита
человека и общества
при получении,
распространении и
использовании
информации.



Компьютер – инструмент для совершения преступления



Информация – объект преступления



Виды компьютерных преступлений:

1. Несанкционированный (неправомерный) доступ к информации.
2. Нарушение работоспособности компьютерной системы
3. Подделка (искажение или изменение), т.е. нарушение целостности компьютерной информации.



Меры обеспечения информационной безопасности

«Защищенная система» - это информационная система, обеспечивающая безопасность обрабатываемой информации и поддерживающая свою работоспособность в условиях воздействия на нее заданного множества угроз.

Стандарты информационной безопасности:

Россия – документы Гостехкомиссии

США – «Оранжевая книга»

«Единые критерии безопасности информационных технологий»

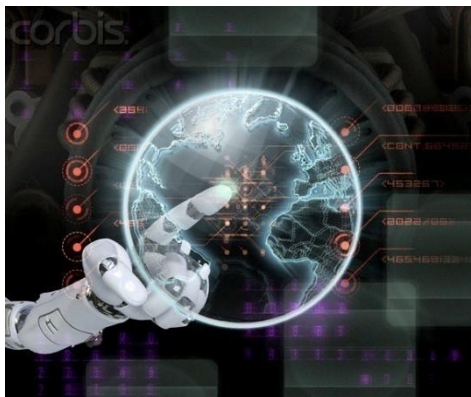
В 1996 году в России впервые в уголовный кодекс был внесен раздел «Преступления в сфере компьютерной информации»

К защите информации относится также и осуществление авторских и имущественных прав на интеллектуальную собственность, каковым является программное обеспечение.

Информационные угрозы

**ВНЕШНИЕ
ФАКТОРЫ**

**ВНУТРЕННИЕ
ФАКТОРЫ**



К источникам
основных внешних
угроз для России
относятся

политика стран,
противодействующая доступу к
мировым
достижениям в области
информационных технологий

«информационная война»,
нарушающая функционирование
информационной среды в стране

преступная деятельность,
направленная против
национальных интересов

К источникам
основных
внутренних угроз
для России относятся

отставание от ведущих стран мира
по уровню информатизации

технологическое отставание электронной
промышленности в области производства
информационной и
телекоммуникационной техники

снижение уровня образованности
граждан, препятствующее работе
в информационной среде

Информационные угрозы



ПРЕДНАМЕРЕННЫЕ

СЛУЧАЙНЫЕ

ПРЕДМАРЕННЫЕ УГРОЗЫ

1

хищение информации, уничтожение информации;

2

распространение компьютерных вирусов

3

физическое воздействие на аппаратуру: внесение изменений в аппаратуру, подключение к каналам связи, порча или уничтожение носителей, преднамеренное воздействие магнитным полем.



Преднамеренные угрозы в компьютерных системах могут осуществляться через каналы доступа к информации



1 компьютерное рабочее место служащего



2 компьютерное рабочее место администратора
компьютерной системы



3 внешние носители информации (диски, ленты, бумажные носители)

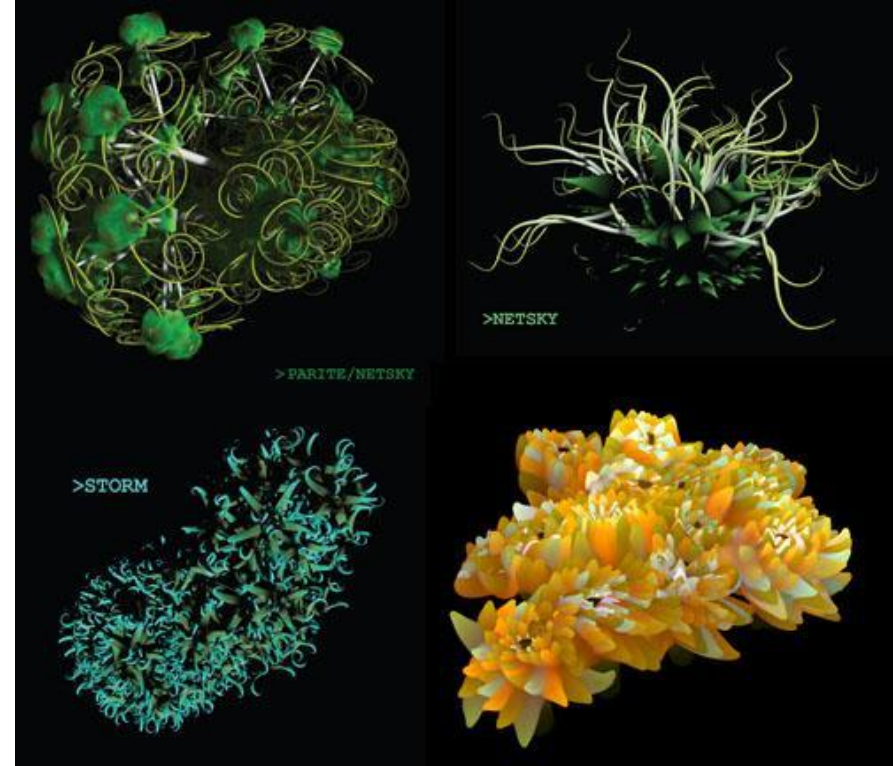


4 внешние каналы связи



Наиболее серьезная угроза исходит от компьютерных вирусов. Каждый день появляется до 300 новых вирусов.

Вирусы не признают государственных границ, распространяясь по всему миру за считанные часы. Ущерб от компьютерных вирусов может быть разнообразным, начиная от посторонних надписей, возникающих на экране монитора, и заканчивая хищением и удалением информации, находящейся на зараженном компьютере. Причем это могут быть как системные файлы операционной среды, так и офисные, бухгалтерские и другие документы, представляющие для пользователя определенную ценность.



Финансовый ущерб от вирусов в 2003 году, по предварительным оценкам, достиг 12 миллиардов долларов.



Среди вредоносных программ особое место занимают *«тройанские кони»*, которые могут быть незаметно для владельца установлены и запущены на его компьютере. Различные варианты *«тройанских коней»* делают возможным просмотр содержимого экрана, перехват вводимых с клавиатуры команд, кражу и изменение паролей и файлов и т. п.



Все чаще причиной информационных «диверсий» называют Интернет. Это связано с расширением спектра услуг и электронных сделок, осуществляемых через Интернет. Все чаще вместе с электронной почтой, бесплатными программами, компьютерными играми приходят и компьютерные вирусы.



В 2003 году произошли две глобальные эпидемии, крупнейшие за всю историю Сети. Примечательно, что причиной эпидемий стали не классические почтовые черви, а их сетевые модификации — черви, распространяющиеся в виде сетевых пакетов данных. Они стали лидерами в рейтинге вредоносных программ



Доля «сетевых червей» в общей массе подобных программ, появившихся, например, в 2003 году, превышает 85 %, доля вирусов — 9,84 %, на троянские программы пришлось 4,87 %.





В последнее время среди распространенных компьютерных угроз стали фигурировать *сетевые атаки*. Атаки злоумышленников имеют целью выведение из строя определенных узлов компьютерной сети. Эти атаки получили название «отказ в обслуживании». Выведение из строя некоторых узлов сети даже на ограниченное время может привести к очень серьезным последствиям.

СЛУЧАЙНЫЕ УГРОЗЫ

- 1 ошибки пользователя компьютера
- 2 ошибки профессиональных разработчиков информационных систем: алгоритмические, программные, структурные
- 3 отказы и сбои аппаратуры, в том числе помехи и искажения сигналов на линиях связи;
- 4 форс-мажорные обстоятельства (авария, пожар, наводнение и другие так называемые воздействия непреодолимой силы)

МЕТОДЫ ЗАЩИТЫ

Расширение областей использования компьютеров и увеличение темпа роста компьютерного парка (то есть проблема защиты информации должна решаться на уровне технических средств)

Высокая степень концентрации информации в центрах ее обработки и, как следствие, появление централизованных баз данных, предназначенных для коллективного пользования

Расширение доступа пользователя к мировым информационным ресурсам (современные системы обработки данных могут обслуживать неограниченное число абонентов, удаленных на сотни и тысячи километров);

Усложнение программного обеспечения вычислительного процесса на компьютере.



на уровне среды обитания человека, то есть путем создания искусственной преграды вокруг объекта защиты: выдачи допущенным лицам специальных пропусков, установки охранной сигнализации или системы видеонаблюдения

Ограничение доступа

на уровне защиты компьютерных систем, например, помощью разделения информации, циркулирующей в компьютерной системе, на части организации доступа к ней лиц в соответствии с их функциональными обязанностями.

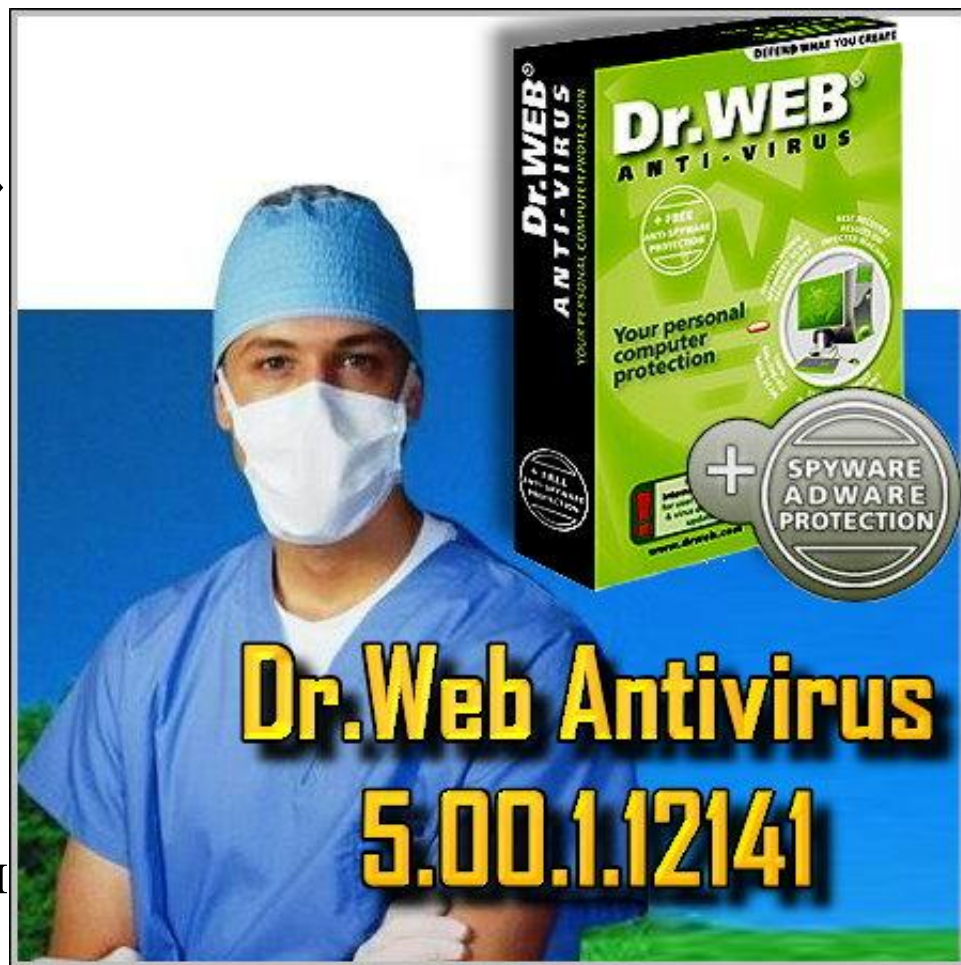
Политика безопасности — это совокупность технических, программных и организационных мер, направленных на защиту информации в компьютерной сети.



Защита от хищения информации обычно осуществляется с помощью специальных программных средств. Несанкционированное копирование и распространение программ и ценной компьютерной информации является кражей интеллектуальной собственности. Защищаемые программы подвергаются предварительной обработке, приводящей исполняемый код программы в состояние, препятствующее его выполнению на «чужих» компьютерах (шифрование файлов, вставка парольной защиты, проверка компьютера по его уникальным характеристикам и т. п.).



Для защиты от компьютерных вирусов применяются «иммуностойкие» программные средства (программы-анализаторы), предусматривающие разграничение доступа, самоконтроль и самовосстановление. Антивирусные средства являются самыми распространенными средствами защиты информации.



В качестве физической защиты компьютерных систем используется специальная аппаратура, позволяющая выявить устройства промышленного шпионажа, исключить запись или ретрансляцию излучений компьютера, а также речевых и других несущих информацию сигналов. Это позволяет предотвратить утечку информативных электромагнитных сигналов за пределы охраняемой территории.



Для защиты информации от случайных информационных угроз, например, в компьютерных системах, применяются средства повышения надежности аппаратуры:

- повышение надежности работы электронных и механических узлов и элементов;
- структурная избыточность — дублирование или утроение элементов, устройств, подсистем;
- функциональный контроль с диагностикой отказов, то есть обнаружение сбоев, неисправностей и программных ошибок и исключение их влияния на процесс обработки информации, а также указание места отказавшего элемента.



Вопросы

1. Что такое информационная безопасность?
2. Какие действия относятся к области информационных преступлений?
3. Какие существуют меры предотвращения информационных преступлений?
4. Какие меры вы бы могли предложить сами?
5. Почему использование «пиратских» копий программного обеспечения является преступлением?

