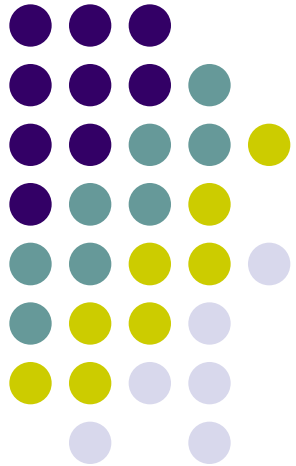
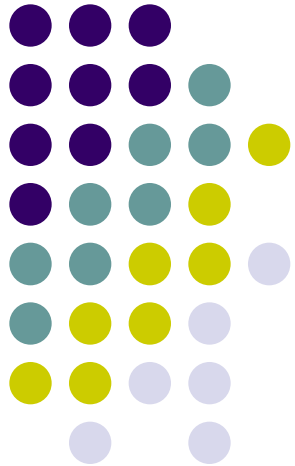
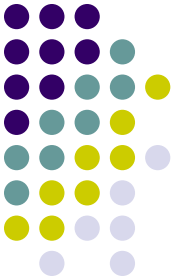
Атаки на информационные ресурсы и защита от них



Компьютерные атаки

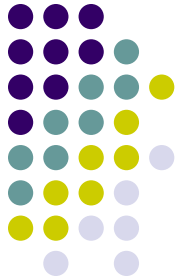


Компьютерная атака



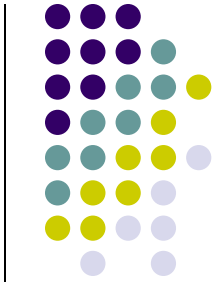
- это целенаправленное воздействие на АИС, осуществляемое программными средствами с целью нарушения конфиденциальности, целостности или доступности информации
- Осуществление компьютерных атак становится возможным благодаря наличию в компьютерной системе *уязвимостей*

Примеры уязвимости КС



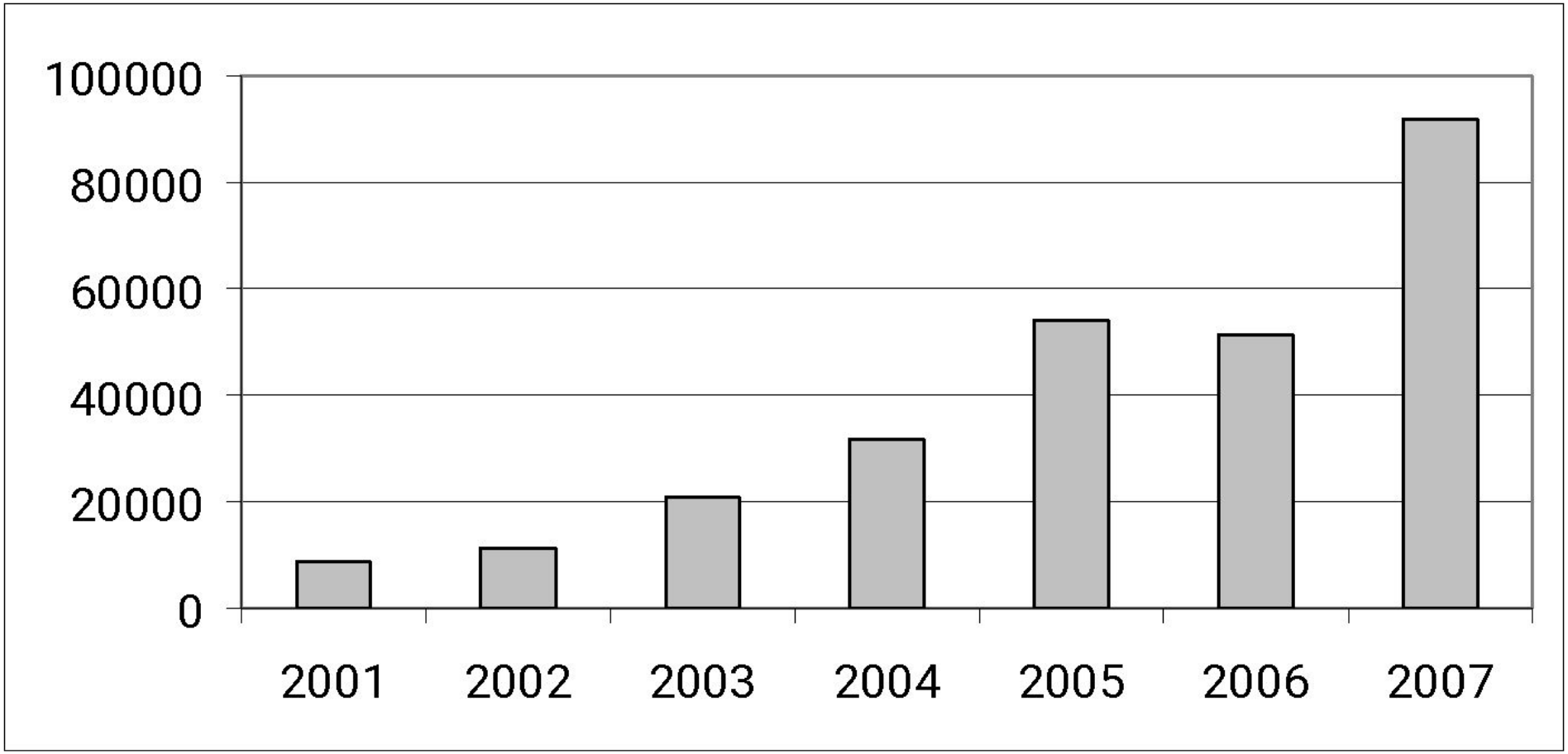
- ошибки, допущенные в ходе разработки ПО или протоколов обмена
  - например, отсутствие механизмов защиты информации от несанкционированного доступа
- ошибки в программном коде, позволяющие тем или иным образом обойти систему защиты
  - (например, ошибки программирования, создающие возможность выполнить атаку на переполнение буфера)
- ошибки конфигурирования и администрирования
  - (неправильная настройка системы защиты, слишком короткий пароль и т. д.).

Классификация компьютерных атак

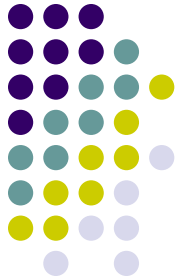


- По типу используемой уязвимости, то есть с позиции атакуемого
- По конечной цели злоумышленника, то есть с позиции атакующего
  - вывод компьютерной системы из строя или ее блокирование (отказ в обслуживании, Denial-of-Service, DoS),
  - копирование или подмена интересующей информации,
  - получение полномочий суперпользователя
- По признакам, позволяющим обнаружить атаку, то есть с позиции наблюдателя
  - наличие в журнале регистрации событий или сетевом трафике определенной информации,
  - подключение к определенной сетевой службе и пр.

Рост обнаруживаемых вредоносных программ

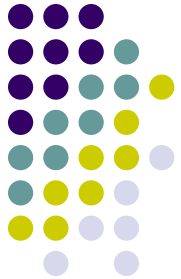


Распределение по ОС



Windows	97100
Linux	1230
SunOS	180
Unix	400
DOS	24
AndroidOS	190
IOS	100

Современные вирусные приложения

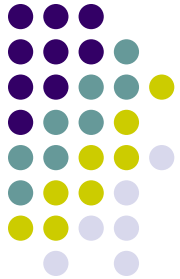


- Лидирует ОС Windows, что говорит главным образом о популярности самой ОС у конечных пользователей
- Технологии распространения
  - с помощью вложений в почтовые сообщения
  - с помощью уязвимостей ОС Windows и ее приложений

Современные ВП

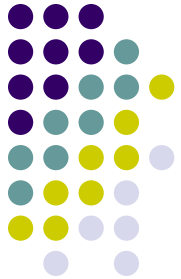
- узлы со старыми системами без обновления уязвимых компонентов, уязвимости «живут» 1-2 года;
- рост числа атак, конечной целью которых является рассылка спама;
- наличие «фонового шума» (15% трафика), вызванного большим количеством bot-сетей, ориентированных на устаревшие уязвимости;
- распространение вредоносных программ через веб-страницы;
- увеличение количества атак, основанных на подборе паролей (bruteforce), направленных на MSSQL, SSH, FTP

Сетевые атаки



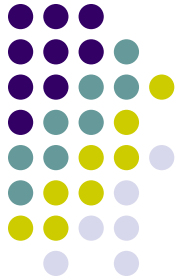
- сбор информации
  - изучение сетевой топологии,
  - определение типа и версии ОС атакуемого узла,
  - доступных сетевых сервисов
- выявление уязвимых мест атакуемой системы
  - анализ наличия уязвимостей в ПО и его настройках
- реализация выбранной атаки
  - отправка сетевых пакетов на определенные сетевые службы
  - SYN Flood, Teardrop, UDP Bomb, подбор паролей

Исследование сетевой топологии



- ICMP-сканирование
  - команда ECHO_REQUEST протокола ICMP
  - ответное сообщение ECHO_REPLY
- TCP-сканирование
  - последовательная установка сетевого соединения по определенному порту с перебором IP-адресов

Система обнаружения атак



- программный или программно-аппаратный комплекс, предназначенный для выявления и, по возможности, предупреждения, действий, угрожающих безопасности информационной системы
- СОА, СОКА, СОПКА
- Система обнаружения вторжений
- IDS, NIDS

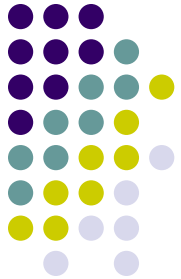
Классификация СОА

- по методу обнаружения:
  - системы сигнатурного анализа
  - системы обнаружения аномалий;
- по способу обработки данных:
  - системы реального времени
  - системы отложенной обработки;
- по типу анализируемых данных:
  - узловые (host-based)
  - сетевые (network-based);
- по конфигурации:
  - компактные
  - распределенные системы

COA Snort

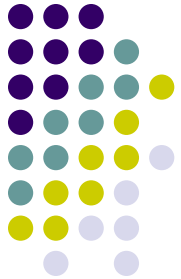
- по методу обнаружения:
  - система сигнатурного анализа
- по способу обработки данных:
  - система реального времени
- по типу анализируемых данных:
  - сетевая (network-based);
- по конфигурации:
  - компактная

COA Snort



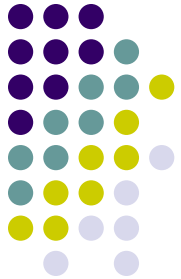
- Сигнатуры атак описываются при помощи правил (rules)
- Набор правил требует обновления
- Доступно зарегистрированным пользователям

Политика сетевой безопасности



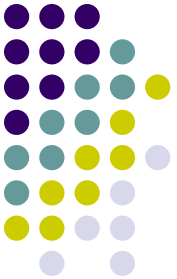
- Политика доступа к сетевым ресурсам
  - запретить доступ из Интернет во внутреннюю сеть, но разрешить доступ из внутренней сети в Интернет
  - разрешить ограниченный доступ во внутреннюю сеть из Интернет

Политика сетевой безопасности



- Политика реализации МЭ
  - запрещать все, что не разрешено
  - разрешать все, что не запрещено

Основные компоненты МЭ



- Фильтрующие маршрутизаторы
- Шлюзы сетевого уровня
- Шлюзы прикладного уровня