

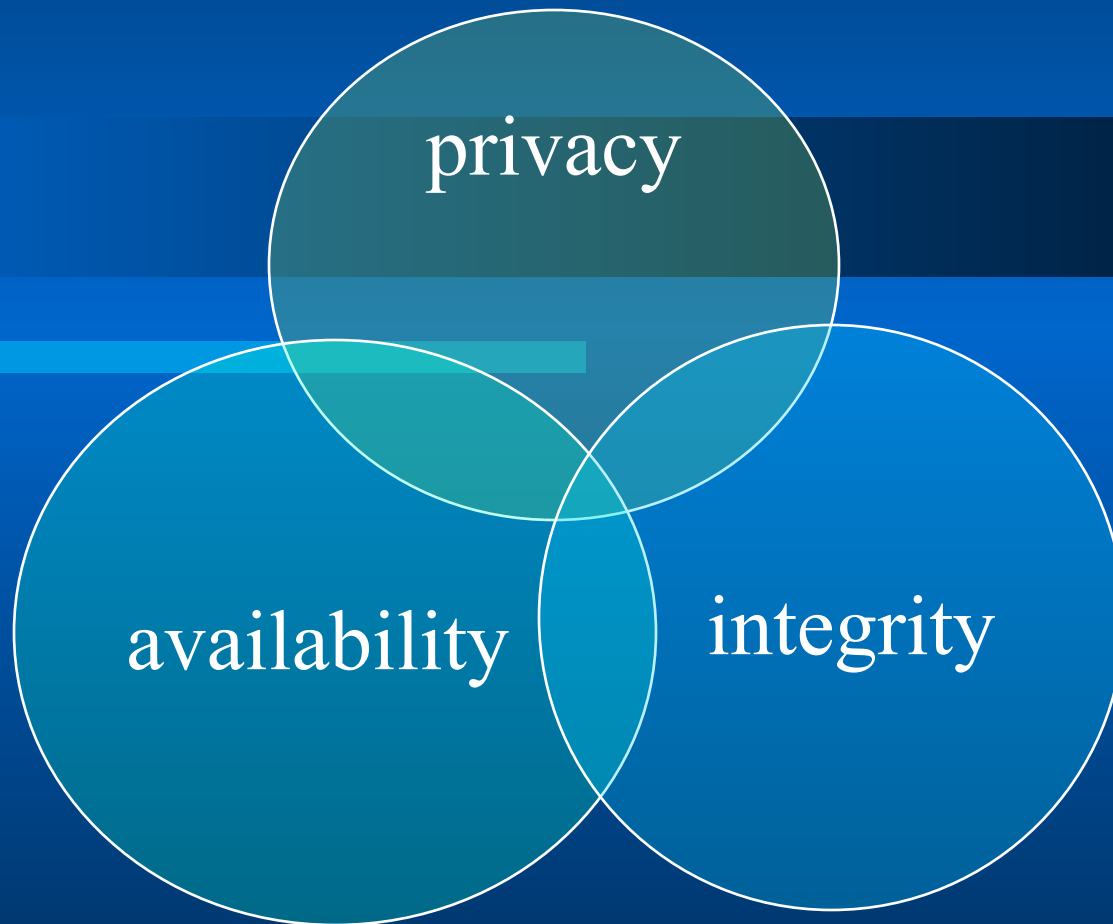
# Администрирование ИС

Полищук М.В.

ПГУПС

2018г.

# Основные характеристики информационной системы



# Основные задачи системного администратора

- ✓ Добавление и удаление пользователей
- ✓ Подключение и удаление аппаратных средств
- ✓ Резервное копирование
- ✓ Установка новых программ
- ✓ Мониторинг системы
- ✓ Поиск неисправностей
- ✓ Ведение локальной документации
- ✓ Наблюдение за безопасностью системы
- ✓ Оказание помощи пользователям

# Поддержка пользователей

пользователи

администратор

аппаратное  
обеспечение

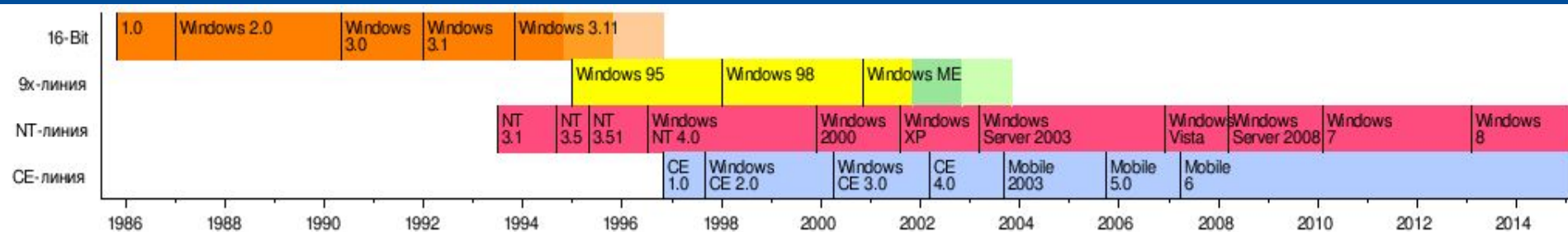
программное  
обеспечение



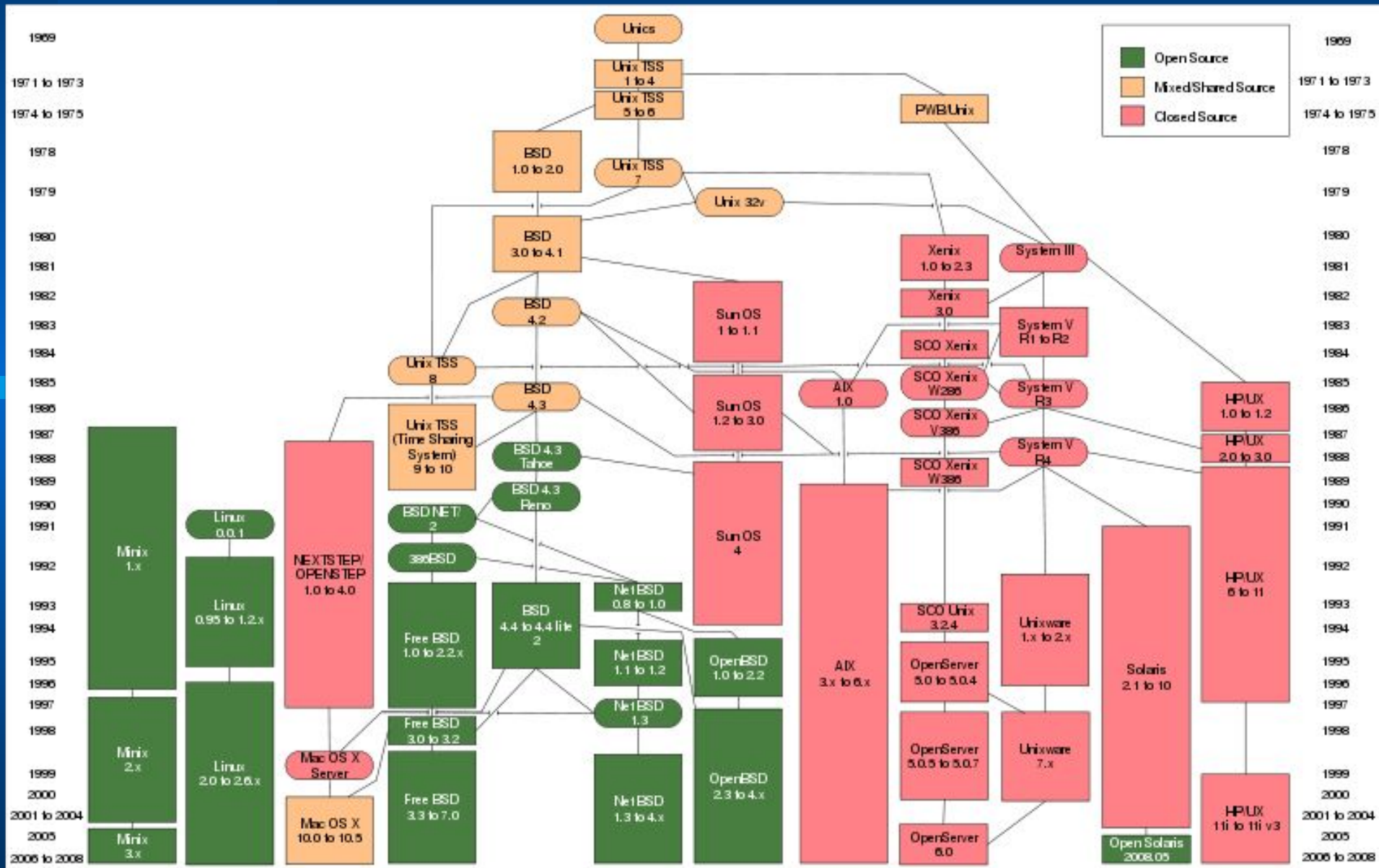
# Microsoft Windows

Наиболее распространенная операционная система в мире - Microsoft Windows.

Все версии традиционно делятся на 4 группы: 16-разрядные (расширения MS-DOS), Windows9x (с остатками MS-DOS), WindowsNT (современная линейка для ПК) и WindowsCE (для карманных компьютеров и смартфонов).



# Unix



# Наиболее распространенные современные версии \*nix

Sun Solaris – наиболее успешная коммерческая версия Unix для RISC-процессоров.

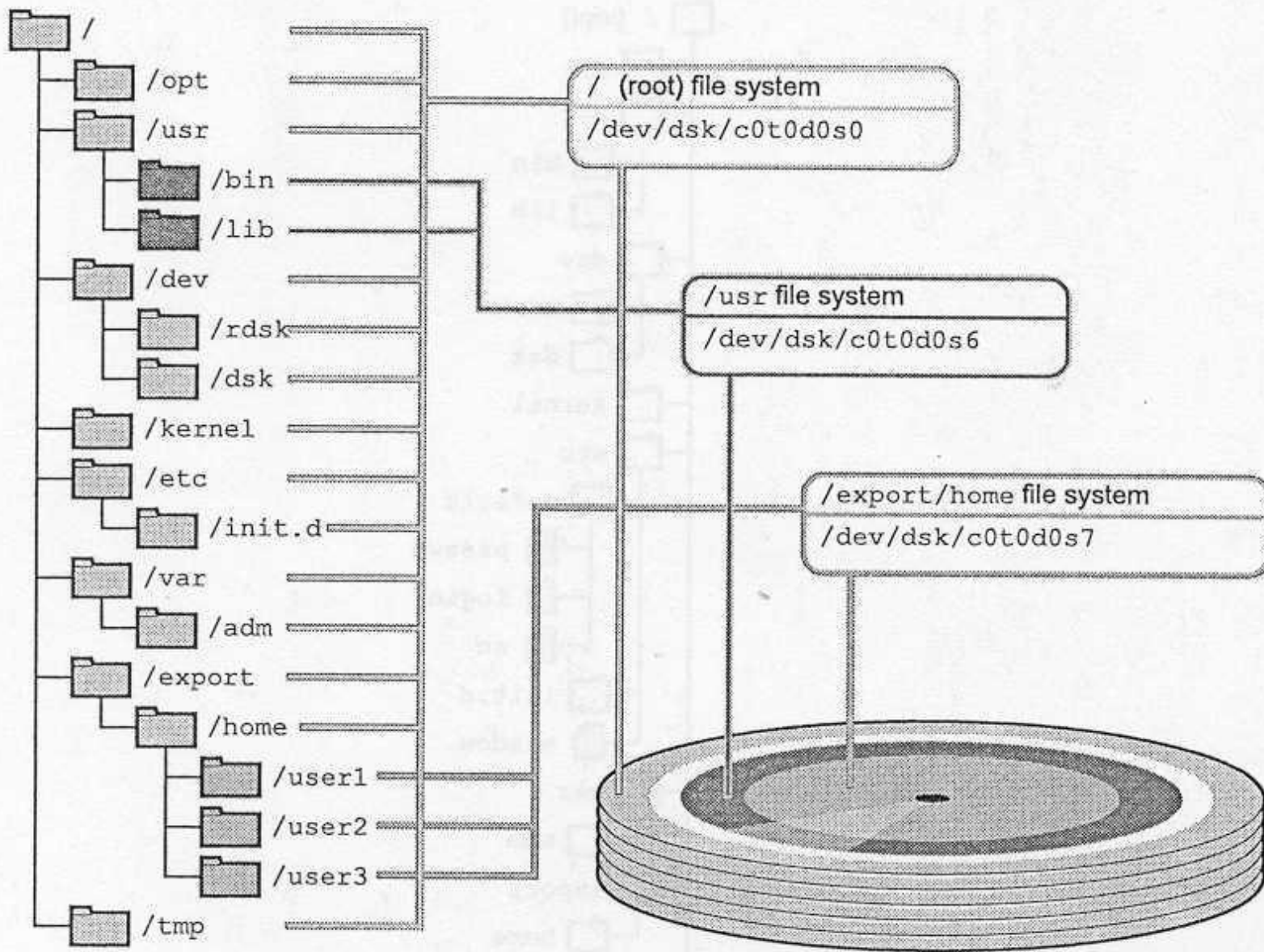
Linux – самая распространенная версия \*nix для ПК.

FreeBSD - версия Unix для коммуникационных серверов.

Mac OS X – проприетарная ОС компании Apple (с использованием ядра FreeBSD).

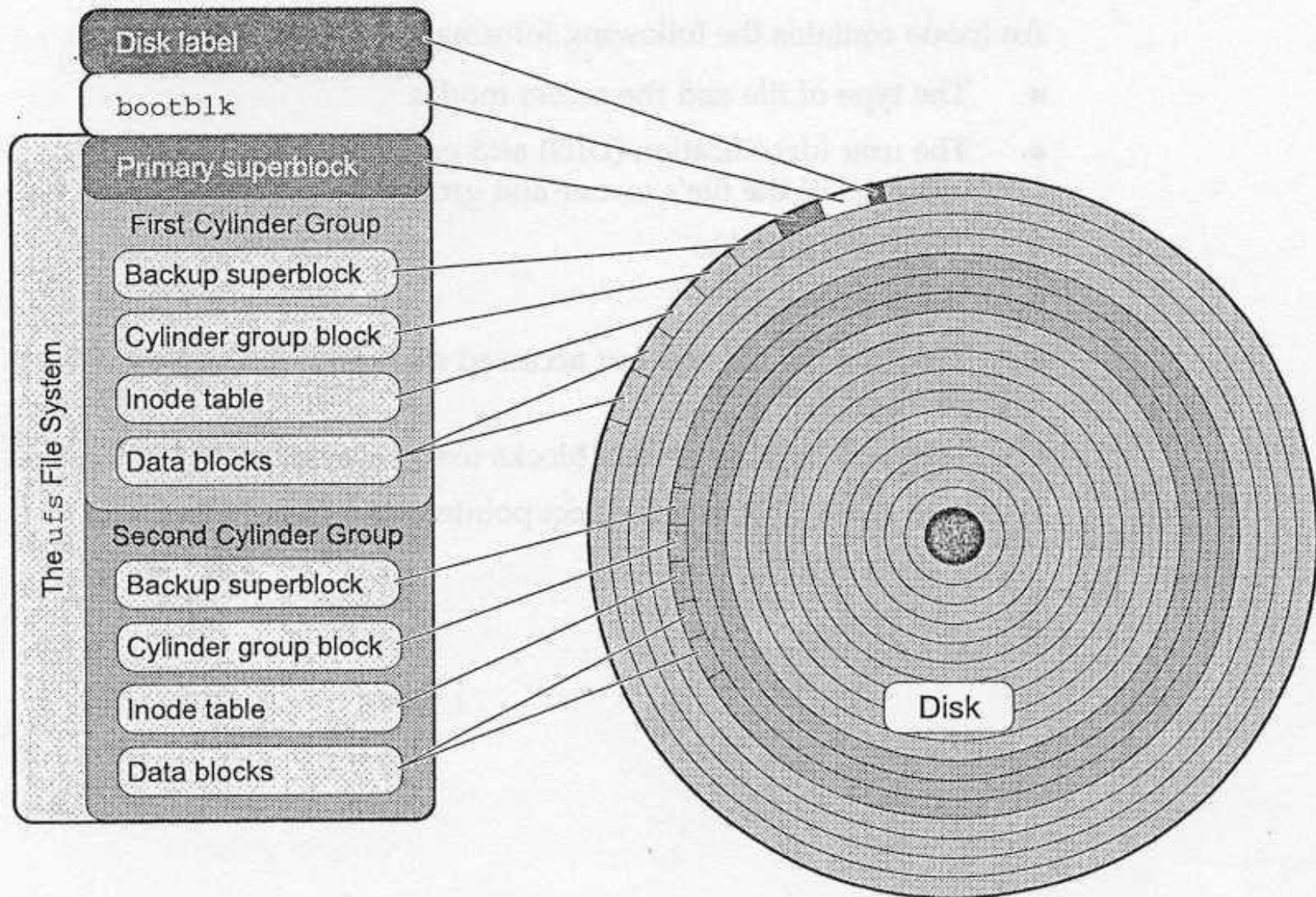
Android - самая распространенная ОС для портативных устройств (на базе ядра Linux).

# Дерево каталогов ФС

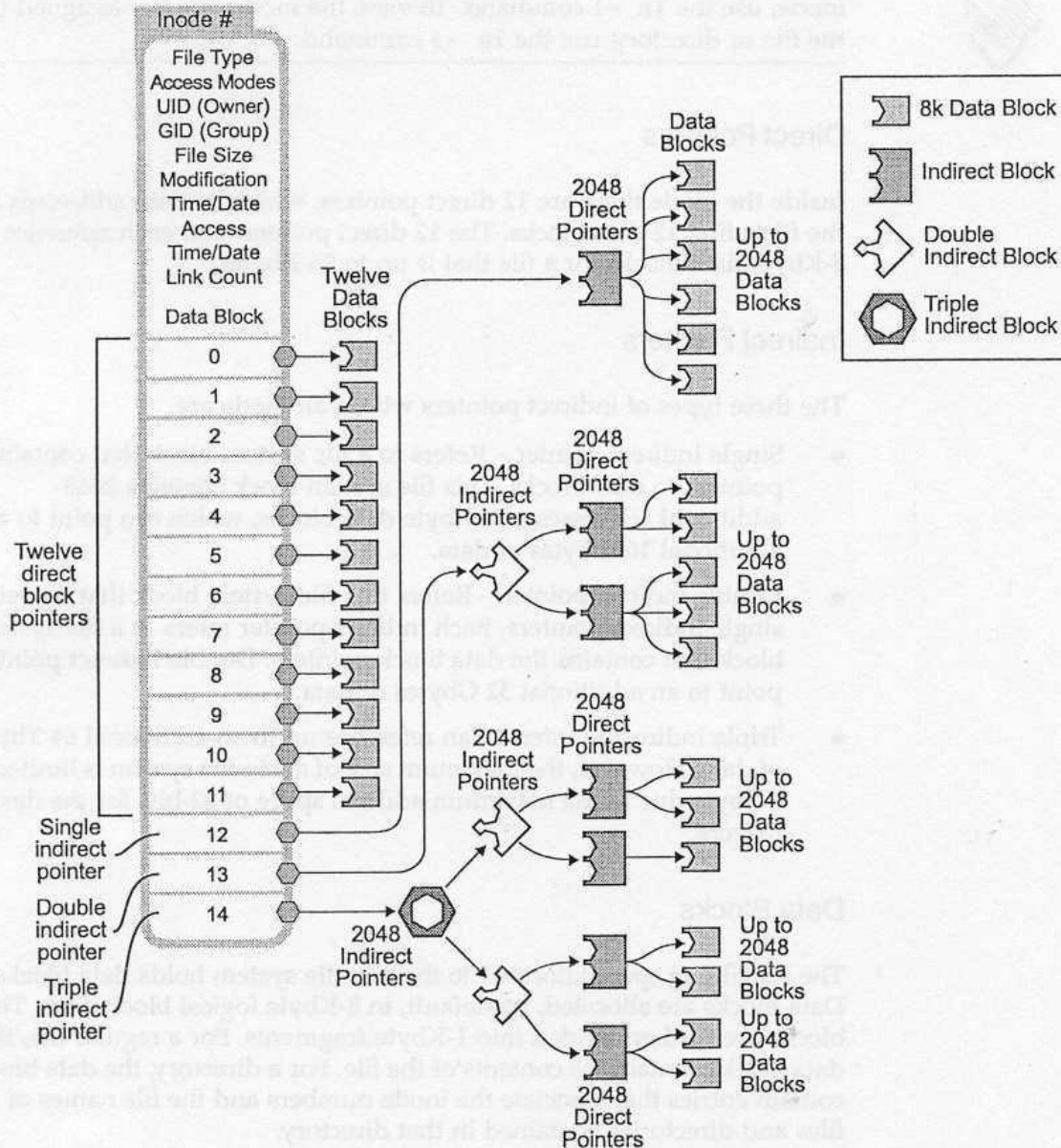




# Файловая система UFS



# Структура inode



# Права доступа в Unix

Право		Доступ к файлам	Доступ к каталогам
Чтение	R	Можно просматривать содержимое файлов, копировать файлы	Можно просматривать список файлов в каталоге (ls)
Запись	W	Можно менять содержимое файлов	При наличии прав WX можно добавлять и удалять файлы
Выполнение	X	Можно запускать файлы на исполнение	Можно «переходить» в данный каталог (cd)

# Права доступа в Windows

Права на чтение и выполнение – аналогично Unix.

Право на запись поделено на три самостоятельных:

- 1) Запись данных / Создание файлов
- 2) Дозапись данных / Создание каталогов
- 3) Удаление

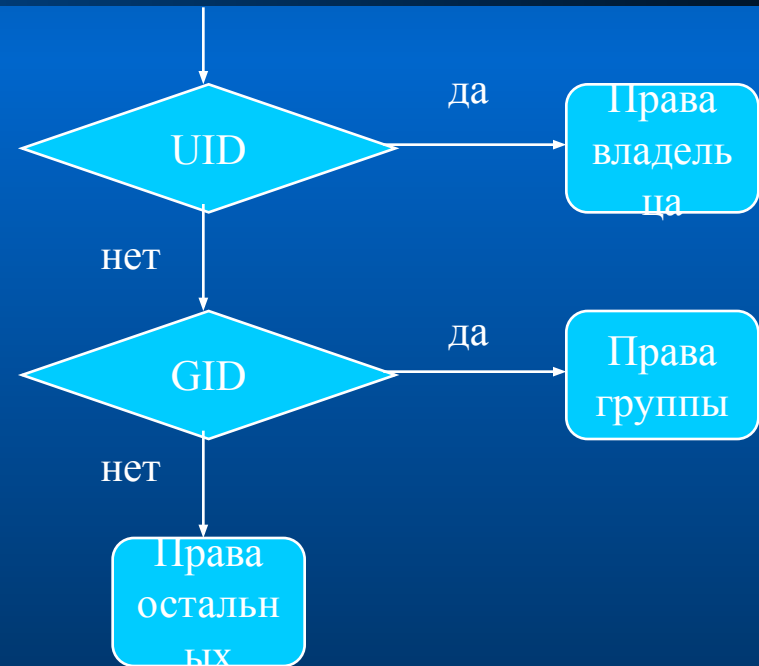
Дополнительные права:

- Смена владельца
- Чтение / изменение прав доступа
- Чтение / запись атрибутов и дополнительных атрибутов

# Эффективные права доступа

В Windows все права суммируются, запретительные права имеют приоритет над разрешительными.

В Unix какое из прав доступа будет задействовано определяется в зависимости от текущего идентификатора процесса по следующему алгоритму



# Основные понятия компьютерной безопасности

- *Угроза* безопасности компьютерной системы - это потенциально возможное происшествие, независимо, преднамеренное или нет, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.
- *Уязвимость* компьютерной системы - это некая ее неудачная характеристика, которая делает возможным возникновение угрозы.
- *Атака* на компьютерную систему - это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости.

# Основные виды угроз безопасности

- Угроза *раскрытия* заключается том, что информация становится известной тому, кому не следовало бы ее знать.
- Угроза *целостности* включает в себя любое умышленное изменение (модификацию или даже удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую.
- Угроза *отказа в обслуживании* возникает всякий раз, когда в результате некоторых действий блокируется доступ к некоторому ресурсу вычислительной системы.

# Особенности безопасности компьютерных сетей

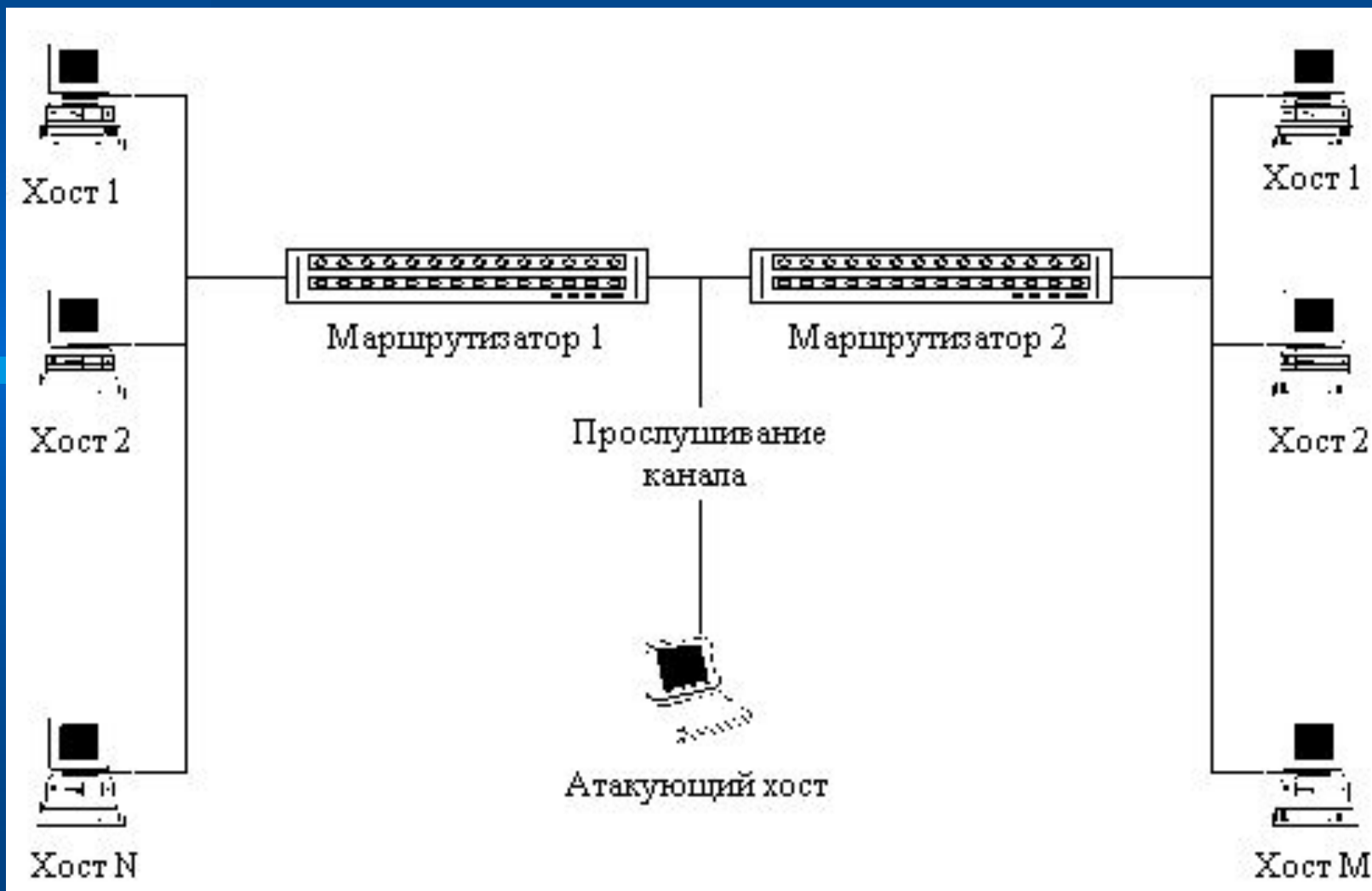
- Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений и программно при помощи механизма сообщений.
- Сетевые системы характерны тем, что, наряду с обычными (локальными) атаками, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид атак, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые (или удаленные) атаки.
- Специфика распределенных ВС состоит в том, что если в локальных ВС наиболее частыми были угрозы раскрытия и целостности, то в сетевых системах на первое место выходит угроза отказа в обслуживании.



# Основные причины уязвимости хостов сети

- ✓ открытость системы, свободный доступ к информации по организации сетевого взаимодействия, протоколам и механизмам защиты;
- ✓ наличие ошибок в программном обеспечении, операционных системах и утилитах, которые открыто публикуются в сети;
- ✓ разнородность используемых версий программного обеспечения и операционных систем;
- ✓ сложность организации защиты межсетевого взаимодействия;
- ✓ ошибки конфигурирования систем и средств защиты;
- ✓ неправильное или ошибочное администрирование систем;
- ✓ несвоевременное отслеживание и выполнение рекомендаций специалистов по защите;
- ✓ "экономия" на средствах и системах обеспечения безопасности или игнорирование их;
- ✓ умолчание о случаях нарушения безопасности хоста или сети.

# Анализ сетевого трафика



# Ложный ARP-сервер

## Структура TCP-пакета

заголовок Ethernet
заголовок IP
заголовок TCP
данные

## Схема ложного ARP-сервера

- ожидание ARP-запроса;
- при получении ARP-запроса передача по сети на запросивший хост ложного ARP-ответа, в котором указывается адрес сетевого адаптера атакующей станции (ложного ARP-сервера);
- прием, анализ, воздействие и передача пакетов обмена между взаимодействующими хостами.

# Ложный DNS-сервер

- 1 по умолчанию служба DNS функционирует на базе протокола UDP, что делает ее менее защищенной
- 2 значение поля "порт отправителя" в UDP-пакете вначале принимает значение  $\geq 1023$  и увеличивается с каждым переданным DNS-запросом
- 3 значение идентификатора (ID) DNS-запроса зависит от конкретного сетевого приложения, вырабатывающего DNS-запрос

# Навязывание хосту ложного маршрута с использованием протокола ICMP

- В сети Internet удаленное управление маршрутизацией реализовано в виде передачи с маршрутизатора на хост управляющего ICMP-сообщения: **Redirect Message**. Оно бывает двух типов: **Redirect Net** уведомляет хост о необходимости смены адреса маршрутизатора, **Redirect Host** информирует хост о необходимости создания нового маршрута к указанной в сообщении системе и внесения ее в таблицу маршрутизации.
- Для осуществления этой удаленной атаки необходимо подготовить ложное ICMP **Redirect Host** сообщение, в котором указать конечный IP-адрес маршрута и IP-адрес ложного маршрутизатора, и передать его на атакуемый хост от имени маршрутизатора.

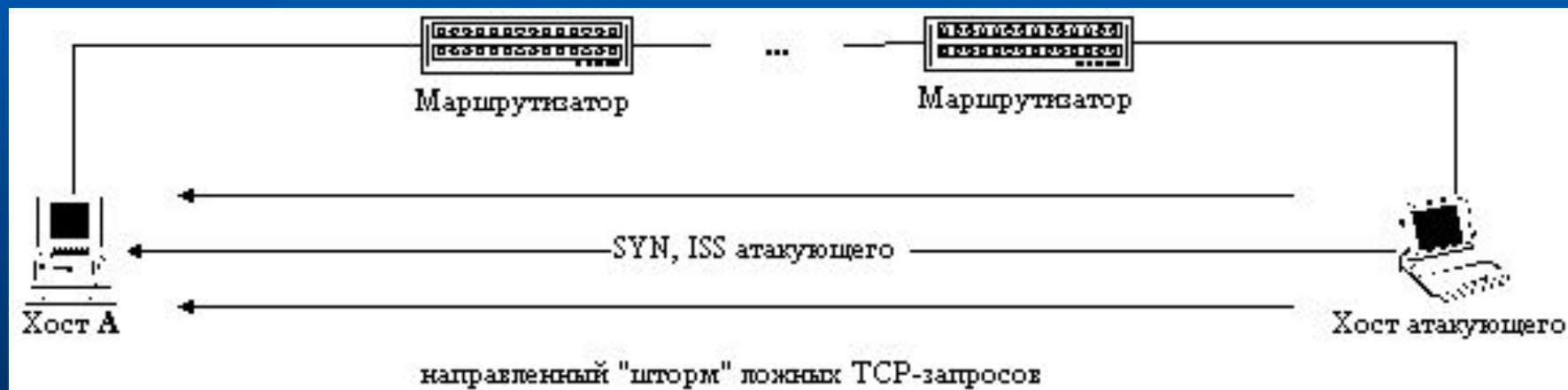
# Подмена одного из субъектов ТСР-соединения в сети *Internet* (hijacking)

## Создание ТСР-соединения



# «Шторм» ложных TCP-запросов на создание соединения

Из рассмотренной ранее схемы создания TCP соединения следует, что на каждый полученный TCP-запрос на создание соединения ОС должна сгенерировать начальное значение идентификатора ISN и отослать его в ответ на запросивший хост. При этом, так как в сети Internet (стандарта IPv4) не предусмотрен контроль за IP-адресом отправителя сообщения, то невозможно отследить истинный маршрут и нет возможности ограничить число возможных запросов, принимаемых в единицу времени от одного хоста.



# Использование средств безопасности в сетях

- Сетевые фильтры/ фильтрующие маршрутизаторы
- Проxy-устройства
- NAT:
  - статический
  - динамический
  - PAT
- Специализированное устройство (firewall)
- Персональный брандмауэр



# Классификация пользователей

## Unix

## Windows

- Суперпользователь

- Обычные пользователи

- Специальные пользователи

- Псевдопользователи

- Администраторы

- Обычные пользователи

- Специальные пользователи

- Псевдопользователи

- Анонимный пользователь

# Уязвимости

## Unix

- Наличие демонов
- Механизм SUID/SGID-процессов
- Излишнее доверие
- Человеческий фактор

## Windows

- Серверы
- Системные процессы
- Анонимный пользователь
- Человеческий фактор
- Совместимость с другими ОС

# Шифрование пароля в Unix

- Из исходного пароля берутся первые восемь байт. Также выбирается 12-битная случайная привязка (salt). Затем к этим двум параметрам применяется специальная функция шифрования, состоящая из 25 повторений чуть измененного алгоритма DES, которая дает на выходе 64-битное значение.
- Привязка преобразуется в два читабельных ASCII-символа, а хэш - в 11 символов.
- При входе пользователя в систему вызывается та же функция с введенным паролем и привязкой, полученной из /etc/passwd. Если результат оказывается равным значению, хранящемуся в файле, то аутентификация считается состоявшейся.

# Шифрование пароля в Windows

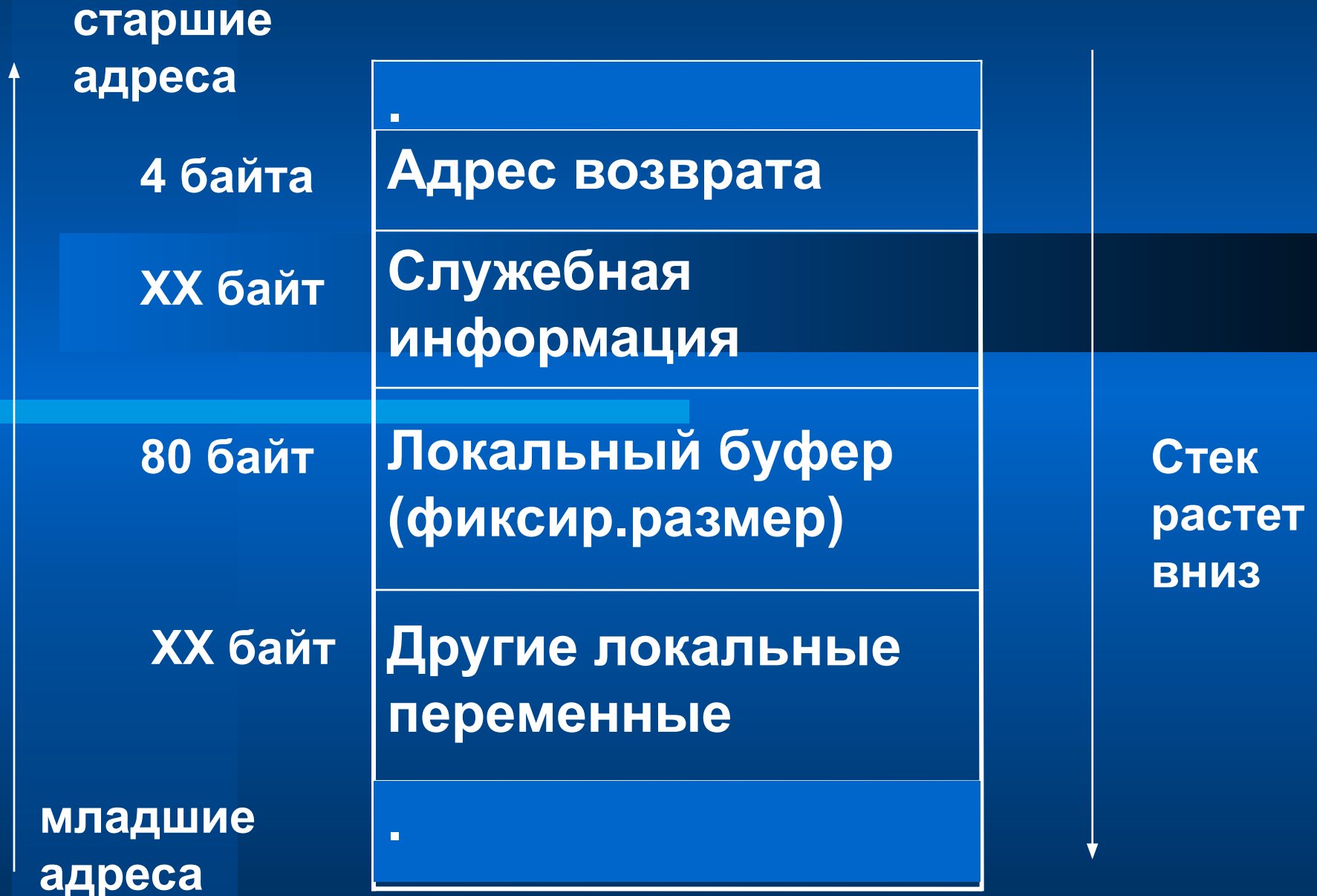
## NT-хэш:

Пароль до 128 символов (Unicode) хэшируется MD4.

## LM-хэш:

- Пароль = 14 символов (только верхний регистр);
- Делится на две половины (по 7 символов) и шифруется DES;
- После объединения получается 16-байтный хэш.

# Переполнение буфера



# Условия для переполнения буфера

- **параметры функций передаются через стек;**
- **адрес возврата также помещается в стек;**
- **локальные переменные располагаются в стеке;**
- **стек «растет» вниз;**
- **данные в стеке могут интерпретироваться как команды;**
- **должны существовать процессы или программы, имеющие уязвимый код;**
- **некоторые процессы или функции должны иметь высокие привилегии.**

# Средства повышения производительности системы

- ✓ Увеличение объема оперативной памяти
- ✓ Своевременное устранение проблем
- ✓ Правильная организация дисковой подсистемы
- ✓ Контроль сетевых операций
- ✓ Настройка конфигурации ядра / набора используемых сервисов
- ✓ Предупреждение критических ситуаций

# Оперативная и виртуальная память

Объем физической оперативной памяти

Виртуальная и физическая адресация

Страничная организация памяти

Организация области обмена на ВЗУ – swap  
файлы и разделы

Paging - процесс переноса страниц из  
оперативной памяти в область swap