Оглавление

[Тема 1.1. Введение в операционные системы 2](#_Toc156174038)

[1. Операционные системы: определение, назначение, состав, функции. 2](#_Toc156174039)

[2. Операционные системы: классификация, основные этапы развития, особенности современного этапа развития. 3](#_Toc156174040)

[Тема 1.2. Архитектура вычислительных систем 7](#_Toc156174041)

[3. Компоненты архитектуры вычислительных систем, их назначение и взаимодействие. 7](#_Toc156174042)

[4. Система прерываний. 14](#_Toc156174043)

[Тема 1.3. Архитектура операционных систем 18](#_Toc156174044)

[5. Структура ядра и его функции. Объекты ядра. Основные операции над объектами ядра. 18](#_Toc156174045)

[6. Утилиты. Системные обрабатывающие программы. Библиотеки процедур. Программы дополнительных услуг. 21](#_Toc156174046)

[Тема 2.1. Процессы операционных систем 23](#_Toc156174047)

[7. Понятие процесса. Системные и пользовательские процессы. Операции над процессами. 23](#_Toc156174048)

[8. Организация межпроцессного взаимодействия в ОС. Сигналы. Каналы. Классические проблемы межпроцессного взаимодействия. 25](#_Toc156174049)

[Тема 2.2. Потоки операционных систем 27](#_Toc156174050)

[9. Концепция потока. Параллельное исполнение потоков. Главный поток процесса. 27](#_Toc156174051)

[10. Диаграммы состояния потоков. Понятие контекста и переключения контекста. 29](#_Toc156174052)

[Тема 2.3. Диспетчеризация потоков 30](#_Toc156174053)

[11. Многозадачность в ОС. Типы многозадачности. 30](#_Toc156174054)

[12. Иерархия, приоритеты и планирование потоков. Динамические уровни приоритетов. 33](#_Toc156174055)

[Тема 2.4. Синхронизация и взаимоблокировка ресурсов 36](#_Toc156174056)

[13. Синхронизация и взаимоблокировка ресурсов. Механизмы синхронизации. 36](#_Toc156174057)

[14. Взаимоблокировка ресурсов в многозадачных системах. Решение задачи взаимоблокировки ресурсов 38](#_Toc156174058)

[Тема 2.5. Компьютерное время 39](#_Toc156174059)

[15. Компьютерное время. Ожидаемые таймеры. 39](#_Toc156174060)

[Тема 3.1. Управление памятью 42](#_Toc156174061)

[16. Управление памятью: адресное пространство процесса, организация памяти, основные механизмы управления памятью, концепция рабочего множества. 42](#_Toc156174062)

[17. Классификация запоминающих устройств. Иерархия памяти. Оперативные и постоянные запоминающие устройства. 45](#_Toc156174063)

[Тема 3.2. Организация виртуальной памяти 47](#_Toc156174064)

[18. Виртуальная память. Структуризация адресного пространства виртуальной памяти. Задачи управления виртуальной памятью. 47](#_Toc156174065)

[19. Подкачка. Алгоритмы замещения страниц. Куча (heap). Стек. 51](#_Toc156174066)

[Тема 3.3. Управление вводом-выводом и файлами 55](#_Toc156174067)

[20. Типы устройств ввода/вывода. Обработка внешних прерываний. Синхронный и асинхронный ввод/вывод. 55](#_Toc156174068)

[21. Файловые системы. Файлы и директории. Управление внешней памятью. 58](#_Toc156174069)

[Тема 4.1. Введение в операционную систему Windows 62](#_Toc156174070)

[22. Принципы организации и структура ОС Windows. Обзор версий Windows. Методы инсталляции ОС Windows. 62](#_Toc156174071)

[23. ОС Windows: организация рабочей среды пользователя, работа с учетными записями пользователей и групп, работа с профилями пользователей. 68](#_Toc156174072)

[Тема 4.2. Администрирование в ОС Windows 71](#_Toc156174073)

[24. Системный реестр ОС Windows, его назначение и использование. 71](#_Toc156174074)

[25. ОС Windows: планирование и назначение разрешений NTFS, списки управления доступом. 73](#_Toc156174075)

[26. Средства автоматической настройки в ОС Windows. 74](#_Toc156174076)

[Тема 4.3. UNIX-подобные и другие POSIX-совместимые операционные системы 77](#_Toc156174077)

[27. Основные понятия системы UNIX. Пользователи системы, атрибуты пользователя. Файловая структура ОС. 77](#_Toc156174078)

[28. ОС UNIX: особенности процессов, сигналы, обработка сигналов. 82](#_Toc156174079)

[Тема 4.4. Операционная система ОС Linux 85](#_Toc156174080)

[29. Основные принципы функционирования Linux. Основные компоненты Linux. Дистрибутивы Linux. Файловая система Linux. 85](#_Toc156174081)

[30. ОС Linux: управление процессами, выполнение задач в фоновом режиме, изменение приоритетов выполняющихся программ. 88](#_Toc156174082)

[Тема 5.1. Безопасность и контроль доступа 90](#_Toc156174083)

[31. Понятие безопасности ОС. Основные угрозы безопасности ОС. Методы и защитные механизмы операционных систем. 90](#_Toc156174084)

[Тема 5.2. Механизмы безопасности в операционных системах семейства Windows 93](#_Toc156174085)

[32. Механизмы безопасности в операционных системах семейства Windows. 93](#_Toc156174086)

[Тема 5.3. Механизмы безопасности в операционных системах семейства Linux 97](#_Toc156174087)

[33. Механизмы безопасности в операционных системах семейства Linux. 97](#_Toc156174088)

# Тема 1.1. Введение в операционные системы

# 1. Операционные системы: определение, назначение, состав, функции.

**Операционная система** — это комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем.

ОС предоставляет прикладным программам удобный интерфейс для работы с аппаратными ресурсами, скрывая от них сложность управления этими ресурсами. Конечные пользователи взаимодействуют с ОС через пользовательский интерфейс, который может быть командной строкой или графическим интерфейсом.

**Назначение** ОС:

ОС управляет всеми устройствами компьютерной системы (процессорами, оперативной памятью, дисками, клавиатурой, монитором, принтерами, сетевыми устройствами и др.) и обеспечивает пользователя удобным интерфейсом для работы с аппаратурой.

Она выполняет две основные функции:

* предоставляет удобный интерфейс для работы с компьютером;
* управляет ресурсами компьютера.

**Состав ОС**

• подсистема управления процессами,

• подсистема управления памятью,

• подсистема управления файлами,

• подсистема управления внешними устройствами,

• подсистема пользовательского интерфейса,

• подсистема защиты данных и администрирования

Функции: Перефразированные из лк:

1. **Прием заданий**: ОС принимает команды от пользователя и обрабатывает их.
2. **Загрузка программ**: ОС загружает программы в оперативную память для выполнения.
3. **Управление задачами**: ОС управляет запуском, приостановкой и остановкой программ. Она также координирует взаимодействие между различными задачами.
4. **Управление файлами и базами данных**: ОС обеспечивает работу систем управления файлами и базами данных.
5. **Многозадачность**: ОС позволяет одновременно выполнять несколько задач.
6. **Планирование задач**: ОС определяет, какие задачи должны быть выполнены и в каком порядке.
7. **Управление вводом/выводом**: ОС управляет операциями ввода и вывода, такими как чтение и запись на диск.
8. **Управление памятью**: ОС управляет использованием оперативной и виртуальной памяти.
9. **Обмен сообщениями**: ОС обеспечивает обмен данными между программами.
10. **Защита данных**: ОС защитит одну программу от влияния другой и обеспечит сохранность данных.
11. **Безопасность**: ОС обеспечивает аутентификацию, авторизацию и другие меры безопасности.
12. **Обработка сбоев**: ОС предоставляет услуги для восстановления после частичных сбоев системы.
13. **Поддержка программирования**: ОС обеспечивает работу систем программирования.

# 2. Операционные системы: классификация, основные этапы развития, особенности современного этапа развития.

Существует несколько классификаций ОС.

В зависимости от **способа организации вычислений**:

* + *Системы пакетной обработки* – основной задачей является организация наибольшего количества вычислительных процессов за единицу времени. Определенные процессы объединяются в пакет, который затем обрабатывает ОС.
  + *Системы разделения времени* – создание возможности единовременного взаимодействия с устройством сразу несколькими людьми. В порядке очереди каждый пользователь получает определенный промежуток процессорного времени.
  + *Системы реального времени* – организация работы каждой задачи за определенный промежуток времени, присущий каждой конкретной задаче.

В зависимости от **типа ядра**:

* + *OС с монолитным ядром* (ядро ОС выполняет все функции, включая управление памятью, устройствами ввода-вывода и файловой системой, в одном монолитном модуле);
  + *OС с микроядром* (ядро ОС содержит только основные функции, такие как планирование задач, управление памятью и межпроцессное взаимодействие, а остальные функции реализуются в виде отдельных модулей, работающих в привилегированном или пользовательском режиме);
  + *OС с гибридным ядром* (комбинация монолитного и микроядерного подходов, где некоторые компоненты, такие как драйверы устройств, могут работать в пространстве ядра, в то время как другие функции, такие как файловая система и сетевые протоколы, могут работать в виде отдельных модулей, загружаемых по требованию).

В зависимости от **количества единовременно решаемых задач**:

* + однозадачные: выполняют одну задачу за раз.;
  + многозадачные: могут выполнять несколько задач одновременно;

В зависимости от **количества пользователей**:

* + однопользовательские: предназначены для одного пользователя;
  + многопользовательские: позволяют одновременную работу нескольких пользователей.

В зависимости от **количества поддерживаемых процессоров**:

* + однопроцессорные
  + многопроцессорные: могут работать с несколькими процессорами одновременно

В зависимости от **возможности работы в компьютерной сети**:

* + локальные – автономные ОС, которые не позволяют работать с компьютерными сетями;
  + сетевые – ОС с поддержкой компьютерных сетей.

В зависимости от **роли в сетевом взаимодействии**:

* + серверные – ОС, открывающие доступ к ресурсам сети и осуществляющие управление сетевой инфраструктурой (управляют ресурсами сети);
  + клиентские – получают доступ к ресурсам сети

В зависимости от **типа лицензии**:

* + открытые – ОС с открытым исходным кодом, который можно изучать и редактировать;
  + проприетарные – ОС, связанные с определенным правообладателем и, как правило, имеющие закрытый исходный код.

В зависимости от **сферы использования**:

* + ОС мэйнфреймов – больших компьютеров;
  + ОС серверов;
  + ОС персональных компьютеров;
  + OC мобильных устройств;
  + встроенные OC;
  + OC маршрутизаторов.

**Основные этапы развития:**

**Первое поколение (1945-1955 гг.):** компьютеров строилось преимущественно на электронных лампах. В начале программы писались в машинных кодах и загружались в память компьютера ~~с панели переключателей~~ вручную. Позже появилась возможность загрузки с перфокарт.

Вычислительная система выполняла **одновременно только одну операцию**. **На этом этапе не было ни языков программирования, ни операционных систем** как таковых. Электронные лампы часто выходили из строя.

В самом конце этого периода появляется первое системное ПО, например, компилятор Fortran и ассемблер.

В целом, первый период характеризуется крайне высокой стоимостью вычислительных систем, их малым количеством и низкой эффективностью использования. Существенная часть времени уходила на подготовку запуска программы, а сами программы выполнялись строго последовательно (такой режим работы называется **последовательной обработкой данных**).

**Второе поколение (1955-1965 гг.)** Второе поколение компьютеров характеризуется использованием **транзисторов**, что повысило их надёжность и продлило время непрерывной работы.

для записи заданий для вычислений использовали **магнитную ленту**. Программа, которая считывала задания с ленты и запускала их на выполнение, является прообразом современной операционной системы.

Системное программное обеспечение обычно хранилось на магнитных лентах. Большие компьютеры второго поколения использовались главным образом для научных и технических вычислений, таких как решение дифференциальных уравнений в частных производных, часто встречающихся в физике и инженерных задачах. В основном программы для них составлялись на языке Фортран и ассемблере, а типичными операционными системами были FMS и IBSYS.

Появлялись новые языки программирования, первые настоящие компиляторы, редакторы связей, библиотеки математических и служебных подпрограмм

**Третье поколение (1965-1980 гг.)** Компьютеры третьего поколения использовали **малые интегральные схемы**, что улучшило качество и снизило стоимость компьютеров.

Самым важным достижением явилась **многозадачность**. В компьютерах предыдущего поколения вычисления останавливались на время ввода-вывода. Проблема была решена разбиением памяти на несколько частей, называемых разделами, в каждом из которых выполнялось отдельное задание. Пока одно задание ожидало завершения работы устройства ввода-вывода, другое могло использовать центральный процессор..

Другим важным плюсом операционных систем третьего поколения стала способность считывать задание с перфокарт на диск по мере того, как их приносили в машинный зал. При окончании выполнения каждого текущего задания операционная система могла загружать новое задание с диска в освободившийся раздел памяти и запускать это задание. (**подкачка данных**)

Многозадачность требует как аппаратной поддержки: (**реализации защитных механизмов, наличия прерываний и развития параллелизма в архитектуре**).

В системах третьего поколения промежуток времени между передачей задания и возвращением результатов часто составлял несколько часов. Желание сократить время ожидания ответа привело к **разработке режима разделения времени** — варианту многозадачности, при котором у каждого пользователя есть свой диалоговый терминал.

Примеры операционных систем третьего поколения — OS/360, CTSS, **MULTICS**. Упрощенная однопользовательская версия системы MULTICS позже переросла в операционную систему UNIX.

**Четвертое поколение (1980-2005 гг.**) Разработка **БИС (большие интегральные схемы**,— кремниевые микросхемы, содержащие тысячи транзисторов на одном квадратном сантиметре) привела к появлению микрокомпьютеров. Главная особенность таких компьютеров — весь процессор помещался в одной микросхеме. Размеры компьютера и его стоимость резко уменьшились, что предоставило возможность купить персональный компьютер каждому человеку. Поэтому со временем их и стали так называть — **персональные компьютеры**.

Компьютеры стали использоваться не только специалистами, что потребовало разработки «дружественного» программного обеспечения.

Операционные системы этого поколения, такие как CP/M и MS-DOS, были разработаны для этих микропроцессоров. С течением времени, по мере увеличения сложности задач, возникла необходимость в более сложных операционных системах, что привело к возрождению многих функций, характерных для больших вычислительных систем[1](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%AD%D0%B2%D0%BE%D0%BB%D1%8E%D1%86%D0%B8%D1%8F_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D1%85_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC)[2](https://bing.com/search?q=%D0%A7%D0%B5%D1%82%D0%B2%D0%B5%D1%80%D1%82%D0%BE%D0%B5+%D0%BF%D0%BE%D0%BA%D0%BE%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5+%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D1%85+%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC). В результате появились операционные системы с графическим интерфейсом, такие как **Mac OS X, Windows и UNIX**-подобные системы

Кроме того, развитие компьютерных сетей привело к появлению сетевых и распределенных операционных систем.

**Пятое поколение (2005 г. - по н.в.)**

* [**Смартфоны**: Появление смартфонов, которые объединяют функции телефона и компьютера](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D1%8B_%D0%BF%D1%8F%D1%82%D0%BE%D0%B3%D0%BE_%D0%BF%D0%BE%D0%BA%D0%BE%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F).
* **Многоядерные процессоры**: В 2005 году появились **многоядерные процессоры**, что потребовало создания многоядерных операционных систем. [Операционные системы, такие как Windows и Linux, были успешно адаптированы для работы на многопроцессорной (многоядерной) архитектуре1](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D1%8B_%D0%BF%D1%8F%D1%82%D0%BE%D0%B3%D0%BE_%D0%BF%D0%BE%D0%BA%D0%BE%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F)[2](https://sariola.ru/all_of_about_pc/na-poroge-patogo-pokolenia-vycislitelnoj-tehniki-kakie-izmenenia-zdut-zavtrasnie-pk.html).
* **Конкуренция мобильных ОС**: На рынке мобильных устройств возникла жесткая конкуренция между различными операционными системами. [На данный момент доминирующими являются Google Android и Apple iOS1](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D1%8B_%D0%BF%D1%8F%D1%82%D0%BE%D0%B3%D0%BE_%D0%BF%D0%BE%D0%BA%D0%BE%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F)[2](https://sariola.ru/all_of_about_pc/na-poroge-patogo-pokolenia-vycislitelnoj-tehniki-kakie-izmenenia-zdut-zavtrasnie-pk.html).
* **Виртуализация и облачные технологии**: Широкую популярность приобрела технология виртуализации, которая позволяет представлять вычислительные ресурсы, абстрагированные от аппаратной реализации. [Это привело к появлению облачных технологий, где потребности клиентов в вычислениях и хранении данных удовлетворяются специализированными дата-центрами](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D1%8B_%D0%BF%D1%8F%D1%82%D0%BE%D0%B3%D0%BE_%D0%BF%D0%BE%D0%BA%D0%BE%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F)

без особого труда подстраивать ее под свое собственное оборудование.

**Особенности современного этапа и перспективы развития ОС**

Современные операционные системы (ОС) развиваются в нескольких ключевых направлениях:

1. **Безопасность**: С учетом растущей ценности информации и угроз безопасности, современные ОС активно развивают и улучшают механизмы защиты, включая шифрование данных, аутентификацию и авторизацию.
2. **Многоплатформенность**: Современные ОС способны работать на различных типах компьютеров, что делает их более универсальными.
3. **Удобство использования**: Удобство работы пользователя с компьютером становится все более важным, поэтому современные ОС стремятся упростить интерактивную работу с компьютером, включая развитие графических интерфейсов и интеллектуальных систем, которые могут направлять действия пользователя и принимать за него рутинные решения.
4. **Прозрачность сетевых ресурсов**: Сетевые ОС стремятся обеспечить высокий уровень прозрачности сетевых ресурсов, чтобы пользователи и администраторы сети могли легко определить местоположение ресурсов, а разработчики сетевых приложений могли легко определить местоположение данных и программных модулей в сети. Ожидается, что будущие ОС смогут организовать распределенные вычисления, превратив сеть в виртуальный компьютер.

# Тема 1.2. Архитектура вычислительных систем

# 3. Компоненты архитектуры вычислительных систем, их назначение и взаимодействие.

Понятие общей шины. Контроллеры. Компоненты компьютера: процессор, память и др.

**Для связи между отдельными функциональными узлами ЭВМ используется общая шина (англ. bus, часто ее называют магистралью).**

**Шина** - это несколько проводников, соединяющих несколько устройств. Шины можно разделить на категории в соответствии с выполняемыми функциями. Они могут быть внутренними по отношению к процессору и служить для передачи данных в АЛУ и из АЛУ, а могут быть внешними по отношению к процессору и связывать процессор с памятью или устройствами ввода-вывода.

Любая шина состоит из трех частей:

* **шина данных**, по которой передается информация;
* **шина адреса**, определяющая, кому передаются данные;
* **шина управления**, регулирующая процесс обмена информацией. По шине управления передаются сигналы, определяющие характер обмена информацией по магистрали.
* Также может присутствовать шина питания.



**---**

**Контроллер** - специализированный процессор, управляющий работой внешнего устройства по специальным встроенным программам обмена.

**Контроллеры** (это устройство или программа для передачи данных между функциональными блоками компьютера\ Например, контроллер клавиатуры получает информацию о нажатии клавиши и передает ее в центральный процессор для дальнейшей обработки)

Cхему легко пополнять новыми устройствами - это свойство называют **открытостью архитектуры**. Для пользователя открытая архитектура означает возможность свободно выбирать состав внешних устройств для своего компьютера, т.е. конфигурировать его в зависимости от круга решаемых задач

---

**Классическая архитектура ЭВМ**, построенная по принципу фон Неймана (фон-неймановская архитектура) и реализованная в вычислительных машинах двух (трех) поколений, представлена и содержит следующие основные блоки:

• арифметическо-логическое устройство (АЛУ), выполняющее арифметические и логические операции;

• управляющее устройство (УУ), организующее процесс выполнения программ;

• внешнее запоминающее устройство (ВЗУ), или память, для хранения программ и данных;

• оперативное запоминающее устройство (ОЗУ);

• устройства ввода и вывода информации (УВВ).



Современный компьютер в типичной конфигурации включает в себя:

• Системный блок

* блок питания: поставляет электроэнергию всем компонентам компьютера.
* Корпус: оболочка, которая содержит и защищает внутренние компоненты компьютера
* материнская плата: основная плата, на которой устанавливаются ЦП, ОЗУ, разъемы для подключения устройств и другие компоненты.
* процессор: выполняет вычислительные операции и управляет работой компьютера.
* жесткий диск: хранит операционную систему, программы и файлы пользователя.
* оперативная память: используется для временного хранения данных и выполнения программ
* видеоадаптер: обрабатывает графическую информацию и отправляет ее на монитор для отображения
* звуковой адаптер: обрабатывает аудиоинформацию и управляет звуковым выводом.
* приводы дисков: например, оптический привод (CD/DVD) или SSD-накопитель для чтения и записи данных на диски
* шлейфы, кабели для подключения и связи устройств между собой и с материнской платой.

• Монитор: отображает информацию и графику компьютера пользователю.

• Клавиатура: позволяет пользователю вводить текст и команды в компьютер.

• Мышь

• Периферийные устройства (принтеры, сканеры, веб-камеры, акустические системы и другие устройства, которые расширяют функциональность компьютера)

**Центральный процессор** выбирает команды из памяти и выполняет их. Обычный цикл работы центрального процессора выглядит так:

* выборка из памяти первой команды,
* ее декодирование для определения ее типа и операндов,
* выполнение этой команды,
* а затем выборка, декодирование и выполнение последующих команд.

Этот цикл повторяется до тех пор, пока не закончится программа.

Для каждого типа центрального процессора существует определенный набор команд, которые он может выполнять. Поскольку доступ к памяти для получения команды или данных занимает намного больше времени, чем выполнение команды, у всех центральных процессоров есть несколько собственных регистров для хранения основных переменных и промежуточных результатов.

Среди специальных регистров процессора стоит выделить **счетчик команд IP** (Instruction Pointer), который содержит адрес ячейки памяти со следующей выбираемой командой, **указатель стека SP** (Stack Pointer), который ссылается на вершину текущего стека в памяти и **слово состояния программы PSW** (Program Status Word).

Есть несколько архитектур процессоров с различными наборами команд. **Аббревиатура CISC обозначает Complex Instruction Set Computer, а RISC — Reduced Instruction Set Computer**

Процессоры CISC имеют большой набор разных команд, включая сложные, а длина команды в байтах для наиболее часто использующихся команд минимальна. Это было вызвано в первую очередь экономией оперативной памяти. Идея RISC заключается в замене сложных инструкций на комбинацию простых. Еще одна основная идея RISC - это конвейеризация. Инструкции разделены на этапы, каждый из которых выполняется примерно одинаковое количество времени.

Если рассмотреть ARM RISC-процессор, то мы обнаружим пятиступенчатый конвейер инструкций.

• **(Fetch)** Извлечение инструкции из памяти и увеличение счетчика команд, чтобы извлечь следующую инструкцию в следующем такте.

• **(Decode)** Декодирование инструкции — определение, что эта инструкция делает. То есть активация необходимых для выполнения этой инструкции частей микропроцессора.

• **(Execute)** Выполнение включает использование арифметико-логического устройства (АЛУ) или совершение сдвиговых операций.

• **(Memory)** Доступ к памяти, если необходимо. Это то, что делает инструкция load.

• **(Write Back)** Запись результатов в соответствующий регистр.

Характеристики RISC [4]:

1. Более простые инструкции, следовательно, простое декодирование инструкций.

2. Инструкция состоит из одного слова.

3. Для выполнения инструкции требуется один такт.

4. Большее количество универсальных регистров.

5. Простые режимы адресации.

6. Меньше типов данных.

7. Конвейер может быть реализован.

Характеристики CISC:

1. Сложные инструкции, следовательно, сложное декодирование инструкций.

2. Инструкции обычно имеют размер, превышающий одно слово.

3. Для выполнения инструкции может потребоваться более одного такта.

4. Меньше количества регистров общего назначения, поскольку операции могут выполняться в оперативной памяти.

5. Сложные режимы адресации.

6. Дополнительные типы данных.

**Преимущества RISC:**

**Более простые инструкции**. RISC-процессоры используют меньший набор простых инструкций, что упрощает их декодирование и быстрое выполнение. Это приводит к ускорению времени обработки.

**Более быстрое выполнение**: поскольку процессоры RISC имеют более простой набор команд, они могут выполнять инструкции быстрее, чем процессоры CISC.

**Более низкое энергопотребление**: процессоры RISC потребляют меньше энергии, чем процессоры CISC, что делает их идеальными для портативных устройств.

**Недостатки RISC:**

**Требуется больше инструкций**: процессорам RISC требуется больше инструкций для выполнения сложных задач, чем процессорам CISC.

**Увеличение использования памяти**: процессорам RISC требуется больше памяти для хранения дополнительных инструкций, необходимых для выполнения сложных задач.

**Более высокая стоимость**. Разработка и производство процессоров RISC может быть дороже, чем процессоров CISC.

**Преимущества CISC:**

**Уменьшенный размер кода**: процессоры CISC используют сложные инструкции, которые могут выполнять несколько операций, что уменьшает объем кода, необходимого для выполнения задачи.

**Более эффективное использование памяти**. Поскольку инструкции CISC более сложны, для выполнения сложных задач требуется меньше инструкций, что может привести к более эффективному использованию памяти.

**Широкое использование**: процессоры CISC используются дольше, чем процессоры RISC, поэтому они имеют большую базу пользователей и более доступное программное обеспечение.

**Недостатки CISC:**

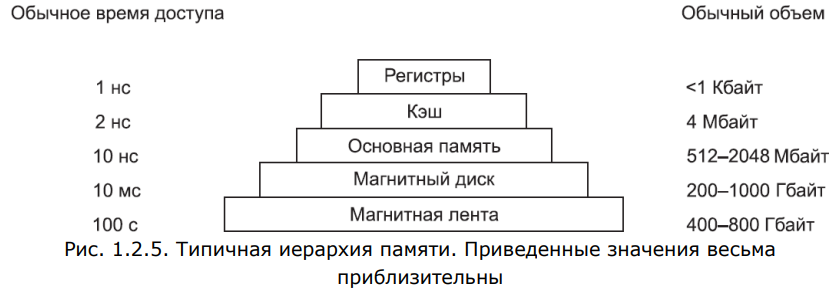
**Медленное выполнение**: процессорам CISC требуется больше времени для выполнения инструкций, поскольку они имеют более сложные инструкции и требуют больше времени для их декодирования.

**Более сложная конструкция**: процессоры CISC имеют более сложные наборы команд, что усложняет их проектирование и производство.

**Более высокое энергопотребление**: процессоры CISC потребляют больше энергии, чем процессоры RISC, из-за более сложных наборов команд

**Память**

Система памяти создается в виде иерархии уровней. Верхние уровни обладают более высоким быстродействием, меньшим объемом и более высокой удельной стоимостью хранения одного бита информации, чем нижние уровни, иногда в миллиарды и более раз.



Верхний уровень состоит из внутренних **регистров процессора**. Они выполнены по той же технологии, что и сам процессор, и поэтому не уступают ему в быстродействии. Следовательно, **к ним нет и задержек доступа**.

Затем следует **кэш-память**, которая управляется главным образом аппаратурой. Оперативная память разделяется на кэш-строки, обычно по 64 байт, с адресами от 0 до 63 в кэш-строке 0, адресами от 64 до 127 в кэш-строке 1 и т. д. Наиболее интенсивно используемые кэш-строки оперативной памяти сохраняются в высокоскоростной кэш-памяти, находящейся внутри процессора или очень близко к нему. Когда программе нужно считать слово из памяти, аппаратура кэша проверяет, нет ли нужной строки в кэш-памяти. Если строка в ней имеется, то происходит результативное обращение к кэш-памяти (**cache hit — кэш-попадание),** запрос удовлетворяется за счет кэш-памяти без отправки запроса по шине к оперативной памяти. Занимает по времени два такта. Отсутствие слова в кэш-памяти вынуждает обращаться к оперативной памяти, что приводит к существенной потере времени. Кэш-память из-за своей высокой стоимости ограничена в объеме. Некоторые машины имеют два или даже три уровня кэша, причем каждый из последующих медленнее и объемнее предыдущего. Доступ к кэшу первого уровня осуществляется без задержек, а доступ к кэшу второго уровня требует задержки в один или два такта.

Следующей в иерархии **идет оперативная память**. Это главная рабочая область системы памяти машины. Оперативную память часто называют оперативным запоминающим устройством (ОЗУ), или памятью с произвольным доступом (Random Access Memory (RAM)).

Дополнительно к оперативной памяти многие компьютеры оснащены небольшой по объему неизменяемой памятью с произвольным доступом — постоянным запоминающим устройством (ПЗУ), оно же память, предназначенная только для чтения (Read Only Memory (ROM)). В отличие от ОЗУ она не утрачивает своего содержимого при отключении питания, то есть является энергонезависимой. ПЗУ программируется на предприятии-изготовителе и впоследствии не подлежит изменению. Эта разновидность памяти характеризуется высоким быстродействием и дешевизной.

**Магнитный жесткий диск** состоит из одной или нескольких металлических пластин, вращающихся со скоростью до 15 000 оборотов в минуту. Информация записывается на диск в виде последовательности концентрических окружностей. В каждой заданной позиции привода каждая из головок может считывать кольцеобразный участок, называемый **дорожкой**. Из совокупности всех дорожек в заданной позиции привода **составляется цилиндр**. Каждая дорожка поделена на определенное **количество секторов**, обычно по 512 байт на сектор.

С целью дальнейшей увеличения плотности записи дорожки стали частично накладывать друг на друга. Такие диски эффективны при последовательной записи данных и редком их чтении (например, системы видеорегистрации). **При черепичной магнитной записи** (SMR - Shingled Magnetic Recording) на жесткий диск дорожки размещаются друг над другом, подобно черепице на крыше. Это позволяет повысить плотность записи. Увеличивается количество дорожек на дюйм (TPI). При перпендикулярной магнитной записи (PMR), используемой в большинстве современных дисков, данные размещаются на параллельных дорожках. Увеличение TPI путем уменьшения расстояния между дорожками благодаря технологии SMR открывает огромный простор для роста емкости жестких дисков. Конечный продукт физически выглядит и ведет себя как обычный жесткий диск с PMR, но при этом имеет большую емкость.

**Твердотельные накопители** (SSD — Solid State Disks), которые хранят данных во флэш-памяти и не имеют движущихся частей. У них то же назначение, что и у магнитных дисков, и с точки зрения операционной системы выглядят так же. SSD-диски обладают большим быстродействием, чем магнитные, но и стоимость таких дисков выше. Гибридные диски используют обе технологии. SSD-диски могут в одной ячейке хранить несколько бит данных. Чем больше бит данных в одной ячейке, тем выше емкость, ниже цена и меньше количество циклов перезаписи. SLC-ячейки выдерживают до 100000 циклов перезаписи, но хранят в одной ячейке ровно один бит. MLC - 2 бита на ячейку, TLC - 3 бита на ячейку, QLC - 4 бита на ячейку, PLC - 5 битов на ячейку.

**Видеокарта** - устройство, преобразующее цифровую информацию в форму, пригодную для дальнейшего вывода на экран монитора. Обычно видеокарта выполнена в виде печатной платы (плата расширения) и вставляется в слот расширения материнской платы, универсальный либо специализированный (AGP, PCI Express), но может быть реализована и на системной плате. Видеокарты не ограничиваются простым выводом изображения, они имеют встроенный графический процессор, который может производить дополнительную обработку, снимая эту задачу с центрального процессора компьютера.

# 4. Система прерываний.

Аппаратная поддержка в процессорах x86. Различие работы в реальном и защищенном режимах процессора. Векторы прерываний.

**Система прерываний** обеспечивающие временное прекращение выполнения последовательности команд для перехода к выполнению др. последовательности команд или для возвращения к ранее прерванной программе.

**Системный вызов**: Пользовательская программа делает системный вызов для получения услуг от ОС. Этот вызов перехватывается внутри ядра ОС и запускает соответствующую службу.

Не по вопросу

Задачи операционной системы по управлению и организации работы компьютера. Выделим три важные группы функций.

1. **Виртуальная память**. Механизм виртуальной памяти используется многими операционными системами. Она позволяет создать впечатление, будто у машины больше памяти, чем есть на самом деле.
2. **Файловый ввод-вывод**.
3. **Параллелизм** (как организовано одновременное выполнение нескольких процессов, обмен информацией и синхронизация). Под процессом можно понимать работающую программу и всю информацию об ее состоянии (памяти, регистрах, счетчике команд, вводе-выводе и т. д.).

Самыми важными задачами управления компьютерным оборудованием, осуществляемыми операционной системой, являются:

* + Параллельное функционирование модулей ввода, вывода информации и процессора.
  + Организация кэширования данных и выполнение согласования скоростей информационного обмена.
  + Разбиение модулей и информационных данных среди процессов.
  + Организация удобной работы логического интерфейса между модулями и оставшейся частью системы.
  + Организация поддержки различных устройств с обеспечением возможности просто их добавить.
  + Режим динамической загрузки и выгрузки драйверов.
  + Обеспечение поддержки набора файловых систем.

Модули, предназначенные для ввода и вывода информации, подразделяются на следующие типы:

* + Модули, ориентированные на работу с блоками.
  + Модули, ориентированные на работу с байтами.

Ориентированное на работу с блоками оборудование сохраняет данные в блоках, имеющих фиксированный размер и свой уникальный адрес. Примером такого устройства может служить жёсткий диск. Модули, работающие с байтами, не имеют адресации и не обеспечивают возможность поиска информации. Они только могут генерировать или потреблять байтовую очерёдность. В качестве примера таких устройств можно привести сетевые адаптеры, терминалы и так далее.

Главным принципом построения программного обеспечения ввода и вывода информации является разбиение его на отдельные уровни. При этом нижние уровни должны обеспечивать защиту особенностей своего оборудования от влияния верхних уровней, которые призваны только осуществлять удобное интерфейсное обслуживание пользователей.

Ещё одним базовым вопросом в организации программ информационного ввода и вывода считается обработка ошибок. Общеизвестно, что обработку ошибок нужно осуществлять максимально близко к оборудованию. Когда контроллер находит ошибку чтения, то ему необходимо сделать попытку её коррекции. Если эта попытка окажется неудачной, то дальше коррекцией ошибки занимается драйвер модуля.

Программное обеспечение ввода и вывода информации делится на следующие уровни:

* + Уровень обработки прерываний.
  + Уровень драйверов оборудования.
  + Уровень независимого от оборудования слоя операционной системы.
  + Пользовательский уровень программного обеспечения.

**Система прерываний**

Вектор прерывания

Все прерывания и особые ситуации имеют уникальные идентификационные номера. Эти номера называются векторами прерываний и лежат в пределах от 0 до 255. Векторы от 0 до 31 отведены для особых ситуаций и немаскируемого прерывания, причем некоторые из них зарезервированы и не должны использоваться программами. Векторы от 32 до 255 свободны для любого использования пользовательскими программами и внешними устройствами

Классификация прерываний

Существует два источника поступления прерываний (interrupt) и три типа особых ситуаций (исключений, exception). Кроме того, различают внутренние (программные, software) и внешние (аппаратные, hardware) источники генерации прерываний и особых ситуаций**.**

**В зависимости от источника**, прерывания делятся на:

* **аппаратные** - возникают как реакция микропроцессора на физический сигнал от некоторого устройства (клавиатура, системные часы, клавиатура, жесткий диск и т.д.), по времени возникновения эти прерывания асинхронны, т.е. происходят в случайные моменты времени;
* **программные** - вызываются искусственно с помощью соответствующей команды из программы (int), предназначены для выполнения некоторых действий операционной системы, являются синхронными;
* **исключения** - являются реакцией микропроцессора на нестандартную ситуацию, возникшую внутри микропроцессора во время выполнения некоторой команды программы (деление на ноль, прерывание по флагу TF (трассировка)).

**Общая классификация прерываний:**

• **внешние** — вызываются внешними по отношению к микропроцессору событиями (это группа аппаратных прерываний) Вложенных прерываний нет!

• **внутренние** — возникают внутри микропроцессора во время вычислительного процесса (по существу это исключительные ситуации и программные прерывания).

Внешние прерывания возникают по сигналу какого-нибудь внешнего устройства. Внешние прерывания подразделяются на не­маскируемые и маскируемые.

**Маскируемые** прерывания генерируются контроллером прерываний по заявке определенных периферийных устройств.

**Немаскируемые** прерывания (говорят, что оно одно, т.к. подается на вывод микропроцессора NMI) инициируют источники, требующие безотлагательного вмешательства со стороны микропроцессора.

**Особые ситуации**, генерируемые процессором, подразделяются на три типа — ошибки, ловушки и сбои. В зависимости от типа особой ситуации различается реакция процессора на ее возникновение.

• **Ошибка (Fault)** — это особая ситуация, которая может быть исправлена обработчиком особой ситуации. При встрече ошибки состояние процессора сохраняется в том виде, каким оно было до начала выполнения команды, инициировавшей генерацию ошибки, а значения CS:EIP, указывающие на эту команду сохраняются в стеке обработчика. Прерванная программа после исправления ошибки может быть продолжена непосредственно с команды, вызвавшей эту ошибку.

• **Ловушка (Trap)** — особая ситуация, которая генерируется после выполнения соответствующей команды. В этом случае сохраняемые в стеке значения CS:EIP, указывают на команду, которая будет выполняться вслед за командой, вызвавшей ловушку; например, если ловушка произошла во время команды JMP, то сохраненные значения CS:EIP указывают на команду, являвшуюся целью команды JMP.

• **Сбой (Abort)** — это особая ситуация, которая не допускает точную локализацию вызвавшей ее команды и не допускает перезапуска. Сбои используются для сообщений о некоторых ошибках, таких как: технические неисправности и наличие некорректных значений в системных таблицах.

Обработка прерываний в процессорах x86

Обработка прерывания в реальном режиме производится в три этапа:

1. **Прекращение выполнения текущей программы**. Для этого необходимо сохранить содержимое регистров, так как они являются ресурсами, разделяемыми между программами. Обязательными для сохранения являются регистры cs, ip, flags (пара CS:IP содержит адрес команды, с которой необходимо начать выполнение после возврата, flags — состояние флагов после выполнения последней команды прерванной программы). Эти регистры сохраняются микропроцессором автоматически. Сохранение остальных регистров - должно обеспечиваться программистом. Наиболее удобным местом хранения регистров является стек. После сохранения регистров в стеке микропроцессор сбрасывает бит флага IF (т.е.=0) Этим предотвращается возможность возникновения вложенных внешних прерываний и порча регистров исходной программы вследствие неконтролируемых действий со стороны программы - обработчика вложенного прерывания. После того как необходимые действия по сохранению контекста завершены, обработчик аппаратного прерывания может разрешить вложенные прерывания командой sti.

2. **Переход к выполнению и выполнение программы обработки прерывания.** Здесь определяется источник прерывания и вызывается соответствующий обработчик прерывания. В реальном режиме микропроцессора допускается 256 источников - по количеству элементов таблицы векторов прерываний. Структура одного элемента в таблице векторов прерываний: WORD (2 байта) — значение смещения начала программы-обработчика прерывания от начала кодового сегмента WORD (2 байта) — значение базового адреса сегмента, в котором находится программа-обработчик.

Фактически, на втором этапе микропроцессор:

• по номеру источника прерывания определяет смещение в таблице векторов прерываний;

• помещает первые два байта в регистр IP;

• помещает вторые два байта в регистр CS;

• передает управление по адресу CS:IP.

Далее выполняется сама программа обработки прерывания. (Она тоже может быть прервана поступлением запроса от более приоритетного источника. Все источники прерывания имеют приоритеты.)

**3. Возврат управления прерванной программе после восстановления ее состояния из стека.** Необходимо привести стек в состояние, в котором он был сразу после передачи управления данной процедуре. Для этого программист должен указать необходимые действия по восстановлению регистров и очистке стека. Этот участок необходимо защитить от возможного искажения содержимого регистров (в результате появления аппаратного прерывания) с помощью команды cli. Последние команды в обработчике прерывания — sti, iret (sti — разрешить аппаратные прерывания, устанавливает флаг IF=1, не имеет операндов), iret — извлечь последовательно три слова из стека и поместить их соответственно в регистры ip, cs, flags.

Реальный и защищенный режимы процессора отличаются по следующим основным параметрам:

1. **Реальный режим**: В этом режиме обращение к оперативной памяти происходит по реальным (действительным) адресам. [Набор доступных операций не ограничен, и защита памяти не используется1](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B6%D0%B8%D0%BC_%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D1%8B_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%BE%D1%80%D0%B0).
2. **Защищенный режим**: В защищенном режиме обращение к памяти происходит по виртуальным адресам с использованием механизмов защиты памяти. [Набор доступных операций определяется уровнем привилегий1](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B6%D0%B8%D0%BC_%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D1%8B_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%BE%D1%80%D0%B0).

# Тема 1.3. Архитектура операционных систем

# 5. Структура ядра и его функции. Объекты ядра. Основные операции над объектами ядра.

**Ядро (kernel)**— низкоуровневая основа любой операционной системы, выполняемая аппаратурой в особом привилегированном режиме. Ядро загружается в память один раз и находится в памяти резидентно (постоянно), по одним и тем же адресам.



**Виды структуры ядра операционной системы**

**Возможны следующие типы структуры (архитектуры) ядра операционной системы:**

* Монолитная структура ядра.
* Модульная структура ядра.
* Микроструктура ядра.
* Экзо структура ядра.
* Нано структура ядра.
* Гибридная структура ядра.
* Комбинированная структура ядра.

*Модули ядра выполняют базовые функции ОС*

• управление процессами;

• управление памятью;

• управление устройствами ввода-вывода.

Функции, входящие в состав ядра, можно разделить на два класса.

**1 класс.** Функции для решения внутрисистемных задач организации вычислительного процесса (переключение контекстов процессов, загрузка/выгрузка страниц, обработка прерываний). Эти функции недоступны для приложений.

**2 класс.** Функции для поддержки приложений (доступны приложениям). Эти функции создают для приложений так называемую прикладную программную среду и образуют интерфейс прикладного программирования — API. Приложения обращаются к ядру с запросами — системными вызовами. Функции API обслуживают системные вызовы — предоставляют доступ к ресурсам системы в удобной и компактной форме, без указания деталей их физического расположения. Приложение не может напрямую обращаться к объектам ядра читать и изменять их содержимое.

**Главные задачи, решаемые ядром**

Ядро операционной системы включает в свой состав следующие программы, решающие соответствующие задачи:

* Программа обработки прерываний.
* Программа для формирования и ликвидации различных процессов.
* Программа переключения состояний процессов.
* Программа, выполняющая диспетчеризацию процессов.
* Программа для приостановки и последующей активации процесса.
* Программа синхронизации выполняемых процессов и организации обменов данными между ними.
* Программа по выполнению ввода и вывода данных.
* Программа управления функциями распределения ресурсов памяти.
* Программа поддержки файловых систем.
* Программа обеспечения вызова и возврата при работе с процедурами.
* Программа поддержки операций по учёту работ ЭВМ.

**Объекты ядра** используются системой и приложениями для управления множеством разных ресурсов: процессами, потоками, файлами и т.д.

**Объект** — это коллекция данных, являющихся частью режима ядра операционной системы, которыми управляет Диспетчер объектов Windows (Windows Object Manager).

Типичные объекты режима ядра включают следующие категории объектов:

* объекты устройств;
* объекты файлов;
* символические ссылки;
* разделы реестра;
* потоки и процессы;
* объекты диспетчера ядра, такие как объекты событий и объекты мьютексов;
* объекты обратного вызова;
* объекты section.

Для взаимодействия с объектами ядра у операционной системы предусмотрен набор функций, обрабатывающих структуры объектов ядра по строго определенным правилам. Например, когда мы создаем объект ядра в операционной системе Windows, функция возвращает описатель, идентифицирующий созданный объект (HANDLE). Все операции с текущим объектом ядра возможны только при указании этого описателя управляющей функции.

**Объекты ядра принадлежат ядру, а не процессу**. Это говорит о том, что, завершая работу с процессом, мы не обязательно разрушаем объект ядра. В большинстве случаев объект разрушается, но, если созданный вами объект ядра используется другим процессом, ядро запретит разрушение объекта до тех пор, пока от него не откажется последний пользователь.

Создание новых объектов, или открытие по имени уже существующих, приложение может осуществить при помощи Win32-функций, таких, как **CreateFile**, **CreateSemaphore**, **OpenSemaphore** и т.д. Полученный описатель затем нужно использовать как первый параметр в различных функциях, например, **ReadFile** и **WriteFile**, для работы с реальным файлом. Во избежание утечки памяти всегда рекомендуется закрывать объект, когда в нем отпала надобность. Впрочем, по окончании работы процесса система закрывает все его объекты. Одной из таких функций является функция **CloseHandle**. Некоторые дескрипторы требуют своей функции закрытия, например, функция **FindClose** должна применяться для закрытия дескриптора, полученного от функции **FindFirstFile**.

# 6. Утилиты. Системные обрабатывающие программы. Библиотеки процедур. Программы дополнительных услуг.

**Утилиты** — это системное программное обеспечение, которое помогает поддерживать правильное и бесперебойное функционирование компьютерной системы.

Утилиты выполняют определенные задачи, такие как обнаружение, установка и удаление вирусов, резервное копирование данных, удаление ненужных файлов и т. д.

Утилиты могут входить в состав операционных систем, идти в комплекте со специализированным оборудованием или распространяться отдельно.

**Интегрированные пакеты утилит** — набор нескольких программных продуктов объединенных в единый удобный инструмент.

Типы утилит

1. **Антивирусы**: Программы, предназначенные для обнаружения и удаления вредоносного программного обеспечения. Примеры: McAfee Antivirus, Quickheal Antivirus, Windows Defender.
2. **Системы управления файлами**: Инструменты для управления и организации файлов в системе. Примеры: Проводник Windows, Google Desktop, Double Commander.
3. **Инструменты сжатия**: Программы, используемые для сжатия файлов для экономии пространства хранения. Примеры: WinZip, WinRAR, 7-Zip.
4. **Инструменты управления дисками**: Программы для управления данными на дисках, включая разделение устройств на разделы. Примеры: MiniTool Partition Wizard, Paragon Partition Manager.
5. **Инструменты очистки диска**: Программы для освобождения дискового пространства путем удаления неиспользуемых файлов. Примеры: Razer Cortex, Piriform CCleaner.
6. **Дефрагментация диска**: Инструменты для уменьшения фрагментации и ускорения доступа к данным путем переупорядочения файлов. Примеры: Perfect disk, Deflaggler.
7. **Утилита резервного копирования**: Программы для создания резервных копий файлов, папок, баз данных или дисков для восстановления данных в случае их потери.

**Обрабатывающие системные программы** отличаются от управляющих программ как по своим функциям, так и по способу их инициирования (запуска).

Основные функции обрабатывающих программ:

**1) перенос информации.** Перенос может выполняться между различными устройствами или в пределах одного устройства. При этом под устройствами понимаются: ОП, устройства ВП, устройства ввода-вывода;

**2) преобразование информации**. То есть после считывания информации с устройства обрабатывающая программа преобразует эту информацию, а только затем записывает ее на это же или на другое устройство.

В зависимости от того, какая из этих двух функций является основной, обрабатывающие системные программы делятся **на утилиты и лингвистические процессоры.**

Основной функцией утилиты является перенос информации, а основная **функция лингвистического процессора** – перевод описания алгоритма с одного языка на другой. Сущность алгоритма при этом сохраняется, но форма его представления, ориентированная на программиста, преобразуется в форму, ориентированную на ЦП.

Лингвистические процессоры делятся на **трансляторы и интерпретаторы**. В результате работы транслятора алгоритм, записанный на языке программирования (исходная виртуальная программа), преобразуется в алгоритм, записанный на машинном языке. (На самом деле, машинная программа является результатом совместной работы нескольких лингвистических процессоров.)

**Трансляторы** делятся на компиляторы и ассемблеры. Исходная программа для транслятора–ассемблера записывается на языке-ассемблере. Один оператор данного языка транслируется в одну машинную команду. Исходная программа для компилятора записывается на языке программирования высокого уровня. Каждый оператор такого языка транслируется в несколько машинных команд. Примерами языков высокого уровня являются Паскаль и Си.

**Интерпретатор** в отличие от транслятора не выдаёт машинную программу целиком. Выполнив перевод очередного оператора исходной программы в соответствующую совокупность машинных команд, интерпретатор обеспечивает их выполнение. Затем преобразуется тот исходный оператор, который должен выполняться следующим по логике алгоритма, и так далее.

**Библиотеки процедур и функций** различного назначения включены в категорию вспомогательных модулей операционной системы. К ним можно отнести библиотеки математических функций, библиотеки функций ввода-вывода и т.д.

**Библиотеки** — это набор функций, которые могут использоваться в различных программах. Библиотеки могут быть статические (библиотека привязывается к определенной программе или софт содержит данную библиотеку в своем теле.) и динамическими (библиотеки грузятся в оперативную память и используются).

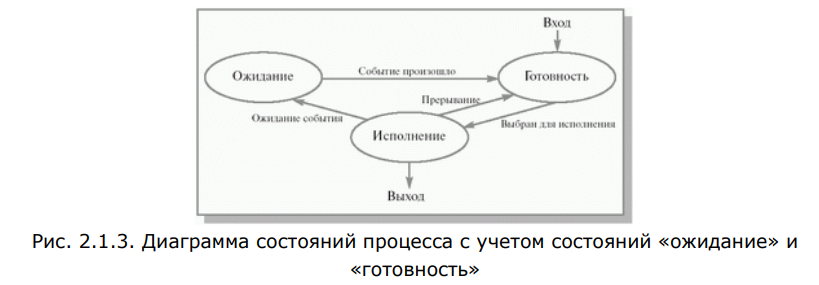
В категорию **программ дополнительных услуг** входит большое количество разнообразных программ: специальный вариант пользовательского интерфейса, *калькулятор*, некоторые игры (какие, например, поставляются в составе ОС).

# Тема 2.1. Процессы операционных систем

# 7. Понятие процесса. Системные и пользовательские процессы. Операции над процессами.

**Процесс — это экземпляр выполняемой программы, включая текущие значения счетчика команд, регистров и переменных**

**Процесс (process)** - это некоторая часть (единица) работы, создаваемая операционной системой. Чтобы некоторую часть работы можно было назвать процессом, она должна иметь **адресное пространство**, назначаемое операционной системой, и **идентификатор**, или идентификационный номер (id процесса). Процесс должен обладать определенным статусом и иметь свой элемент в таблице процессов. В соответствии со стандартом POSIX он должен содержать один или несколько потоков управления, выполняющихся в рамках его Процесс состоит из множества выполняющихся инструкций, размещенных в адресном пространстве этого процесса. Адресное пространство процесса распределяется между инструкциями, данными, принадлежащими процессу, и стеками, обеспечивающими вызовы функций и хранение локальных переменных.



Системные и пользовательские процессы

Процессы, которые выполняют системный код, называются **системными** и применяются к системе в целом. Они занимаются выполнением таких служебных задач, как распределение памяти, обмен страницами между внутренним и вспомогательным запоминающими устройствами, контроль устройств и т.п. Они также выполняют некоторые задачи «по поручению» пользовательских процессов, например, делают запросы на ввод-вывод данных, выделяют память и т.д.

**Пользовательские процессы** выполняют собственный код и иногда обращаются к системным функциям. Выполняя собственный код, пользовательский процесс пребывает в пользовательском режиме (user mode).

Процесс не может перейти из одного состояния в другое самостоятельно. Изменением состояния процессов занимается ОС, совершая операции над ними. Удобно объединить их в три пары:

• создание процесса – завершение процесса;

• приостановка процесса – запуск процесса;

• блокирование процесса – разблокирование.

Еще одна операция, не имеющая парной: **изменение приоритета процесса**. Операции создания и завершения процесса являются одноразовыми, так как применяются к процессу не более одного раза (некоторые системные процессы при работе вычислительной системы не завершаются никогда). Все остальные операции являются многоразовыми

**Основные операции над процессами:**

**Запуск процесса** (из числа процессов, находящихся в состоянии готовность, операционная система выбирает один процесс для последующего исполнения).

**Приостановка процесс**а (работа процесса, находящегося в состоянии исполнение, приостанавливается в результате какого-либо прерывания).

**Блокирование процесса** (процесс блокируется, когда он не может продолжать работу, не дождавшись возникновения какого-либо события в вычислительной системе).

**Разблокирование процесса** (после возникновения в системе какого-либо события операционной системе нужно точно определить, какое именно событие произошло).

**Переключение контекста.**

Информация, хранимая в блоке управления процессом, делится на две части: **регистровый контекст и системный контекст**. **Регистровым контекстом процесса** называется содержимое всех регистров общего назначения процессора (включая значение программного счетчика). Содержимое остальных регистров процессора называется **системным контекстом процесса**. Информации, получаемой с регистровых и системных контекстов, достаточно для управления работой процесса в операционной системе. С точки зрения пользователя, наибольший интерес вызывает вычислительная деятельность процесса, последовательность преобразования данных и полученные результаты.

**Пользовательским контекстом** называются данные, находящиеся в адресном пространстве процесса.

**Совокупность регистрового, системного и пользовательского контекстов процесса называется контекстом процесса**. В любой момент времени процесс полностью характеризуется своим контекстом

В Windows одним вызовом функции **CreateProcess** создается процесс, и в него загружается нужная программа.

В UNIX существует только один системный вызов для создания нового процесса — **fork**. Этот вызов создает точную копию вызывающего процесса. После выполнения системного вызова fork два процесса, родительский и дочерний, имеют единый образ памяти, единые строки описания конфигурации и одни и те же открытые файлы.

Для своего завершения процесс может вызвать функцию **exit**.

# 8. Организация межпроцессного взаимодействия в ОС. Сигналы. Каналы. Классические проблемы межпроцессного взаимодействия.

Для организации коммуникации между одновременно работающими процессами применяются средства межпроцессного взаимодействия (Interprocess Communication - IPC).

Выделяются три уровня средств IPC:

• локальный;

• удаленный;

• высокоуровневый.

Средства локального уровня IPC привязаны к процессору и возможны только в пределах компьютера. К этому виду IPC принадлежат практически все основные механизмы IPC UNIX, а именно, каналы, разделяемая память и очереди сообщений. Коммуникационное пространство этих IPC поддерживаются только в пределах локальной системы. Из-за этих ограничений для них могут реализовываться более простые и более быстрые интерфейсы.

Удаленные IPC предоставляют механизмы, которые обеспечивают взаимодействие как в пределах одного процессора, так и между программами на различных процессорах, соединенных через сеть. Сюда относятся удаленные вызовы процедур (Remote Procedure Calls - RPC), сокеты Unix, а также TLI (Transport Layer Interface - интерфейс транспортного уровня) фирмы Sun.

Под высокоуровневыми IPC обычно подразумеваются пакеты программного обеспечения, которые реализуют промежуточный слой между системной платформой и приложением. Эти пакеты предназначены для переноса уже испытанных протоколов коммуникации приложения на более новую архитектур

**Сигнал** в операционных системах семейства Unix — асинхронное уведомление процесса о каком-либо событии, один из основных способов взаимодействия между процессами. Отдельные сигналы подразделяются на три класса:

* системные сигналы (ошибка аппаратуры, системная ошибка и т.д.);
* сигналы от устройств;
* сигналы, определенные пользователем.

Механизм передачи сигналов состоит из следующих частей:

* установление и обозначение сигналов в форме целочисленных значений;
* маркер в строке таблицы процессов для прибывших сигналов;
* таблица с адресами функций, которые определяют реакцию на прибывающие сигналы.

Известно **три варианта реакции на сигналы**:

 вызов собственной функции обработки;

 игнорирование сигнала (не работает для SIGKILL);

 использование предварительно установленной функции обработки по умолчанию.

Сигналы посылаются:

 с терминала, нажатием специальных клавиш или комбинаций (например, нажатие

Ctrl-C генерирует SIGINT, Ctrl-\ SIGQUIT, а Ctrl-Z SIGTSTP);

 ядром системы:

o при возникновении аппаратных исключений (недопустимых инструкций,

нарушениях при обращении в память, системных сбоях и т. п.);

o ошибочных системных вызовах;

o для информирования о событиях ввода-вывода;

 одним процессом другому (или самому себе):

o из С-кода с помощью системного вызова kill():

o из shell, утилитой /bin/kill (она позволяет задавать сигнал как числом, так

и символьным обозначением).

**Канал** (pipe) представляет собой средство связи стандартного вывода одного процесса со стандартным вводом другого. После создания канала, процесс может при помощи обычного системного вызова **write**() выводить данные в него, а затем вводить их, вызывая соответственно функцию **read**(). При выполнении вызова **fork**() дескрипторы канала наследуются процессом-"потомком". Таким образом, оба процесса получают возможность обмениваться данными.

**Классические проблемы:**

**Синхронный доступ**. Если все процессы считывают данные из файла, то в большинстве случае проблем не возникает. Однако, при попытке одним из процессов изменить этот файл, могут возникнуть так называемые конкурентные ситуации (race conditions).

**Дисциплина доступа**. Если нужно, чтобы как можно большее количество пользователей могли записывать данные, организуется так называемая очередь (по правилу «один пишет, несколько читают»). Практически организуется две очереди: одна — для чтения, другая — для записи. Такую дисциплину доступа можно организовать с помощью **барьеров** (блокировок). При этом создается общий барьер для считывателей, так как несколько процессов могут одновременно считывать данные, а также отдельный барьер для процесса-писателя. Такая организация предотвращает взаимные помехи в работе.

**Голодание процессов**. Организация дисциплины доступа может привести к ситуации, когда процесс будет длительно ждать своей очереди для записи данных. Поэтому иногда нужно организовывать очереди с приоритетами.

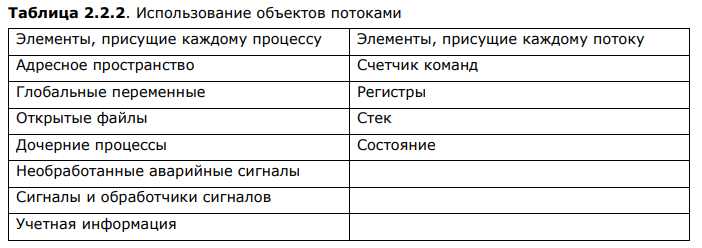
Если нельзя точно определить, какой из процессов запрашивает или возвращает свои данные в нужный компьютер первым, используется так называемое взаимодействие по модели "клиент-сервер". При этом используются один или несколько клиентов и один сервер. Клиент посылает запрос серверу, а сервер отвечает на него. После этого клиент должен дождаться ответа сервера, чтобы продолжать дальнейшее взаимодействие. Такое поведение называется **управлением потоком**. При одновременном доступе здесь также могут использоваться очереди с приоритетами.

**Классический тупик** возникает, если процесс A получает доступ к файлу A и ждет освобождения файла B. Одновременно процесс B, получив доступ к файлу B, ждет освобождения файла A. Оба процесса теперь ждут освобождения ресурсов другого процесса и не освобождают при этом собственный файл.

# Тема 2.2. Потоки операционных систем

# 9. Концепция потока. Параллельное исполнение потоков. Главный поток процесса.

**Поток выполнения** (англ. thread — нить) — наименьшая единица обработки, исполнение которой может быть назначено ядром операционной системы. Несколько потоков выполнения могут существовать в рамках одного и того же процесса и совместно использовать ресурсы, такие как память, тогда как процессы не разделяют этих ресурсов. В частности, потоки выполнения разделяют инструкции процесса (его код) и его контекст (значения переменных, которые они имеют в любой момент времени).



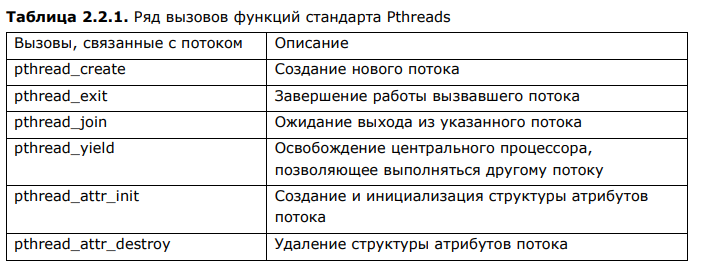
Параллельное исполнение потоков

Под словами "параллельный поток" или просто "поток" мы будем понимать объект, выполняемый параллельно с основным потоком приложения и с другими параллельными потоками. Термин "параллельность" рассматривается в контексте вытесняющей многозадачности операционной системы - то есть, операционная система выделяет потоку некоторый квант времени, а затем переключается на другой поток.

**Многопоточность**: процесс, порождённый в операционной системе, может состоять из нескольких потоков, выполняющихся «параллельно», то есть **без предписанного порядка во времени**.

По умолчанию процесс создается с одним потоком, называемым **главным** или основным потоком. В Linux потоки реализованы с помощью системного вызова **clone**(), который как минимум в 10 раз меньше занимает времени для создания еще одного потока, чем создание еще одного процесса при помощи **fork**(). Такая скорость достигается за счет того, что многие атрибуты процесса разделяются между потоками.

POSIX Threads – Это стандарт POSIX-реализации потоков



В Windows процесс может породить практически неограниченное количество потоков. Для этого используется функция **CreateThread**. Процесс будет активен, пока активен хотя бы один поток.

**Преимущества потоков**

1. Код программы может выполняться, даже если некоторые действия заблокированы.

2. Легкость и быстрота их создания (по сравнению с процессами).

3. Потоки довольно просто обмениваются данными по сравнению с процессами.

4. Улучшает общую производительность системы при ожиданиях завершения операций ввода-вывода.

5. На многопроцессорных системах могут повысить быстродействие за счет параллельных вычислений.

**Недостатки потоков**

1. При программировании приложения с множественными потоками необходимо постоянно думать о потокобезопасности (thread safety).

2. Один неправильно работающий поток может повредить остальные, так как потоки делят общее адресное пространство.

3. Потоки конкурируют друг с другом в адресном пространстве. Стек и thread-local storage, занимая часть виртуального адресного пространства процесса, тем самым делают его недоступным для других потоков.

Главный поток

По умолчанию процесс создается с одним потоком, называемым главным или основным потоком. Потоки в Unix по существу являются дешевой копией процессов и по аналогии с процессами предоставляют механизм для одновременного выполнения нескольких параллельных задач в рамках одного приложения

В Linux потоки реализованы с помощью системного вызова **clone**(), который как минимум в 10 раз меньше занимает времени для создания еще одного потока, чем создание еще одного процесса при помощи fork().

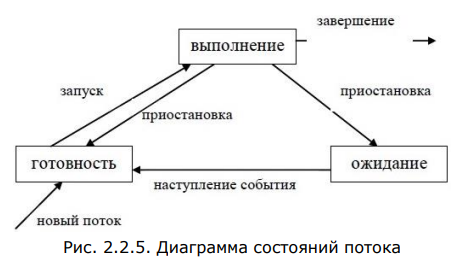
# 10. Диаграммы состояния потоков. Понятие контекста и переключения контекста.

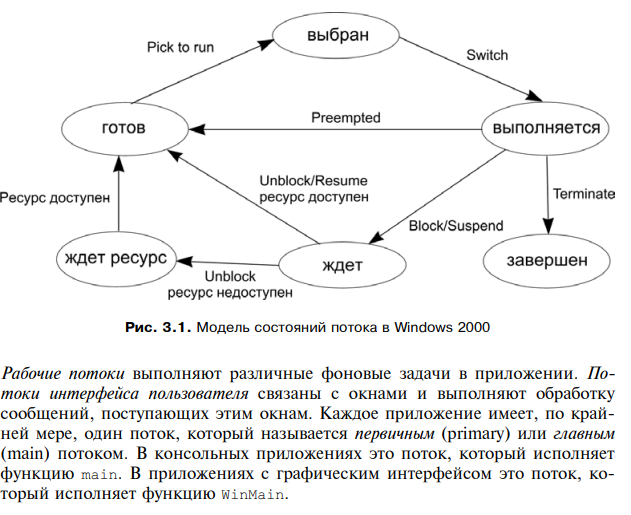
Для каждого созданного потока в системе предусматриваются три возможных его состояния:

• состояние **выполнения**, когда код потока выполняется процессором; на однопроцессорных платформах в этом состоянии в каждый момент времени может находиться только один поток;

• состояние **готовности** к выполнению, когда поток готов продолжать свою работу и ждет освобождения ЦП;

• состояние **ожидания** наступления некоторого события; в этом случае поток не претендует на время ЦП, пока не наступит определенное событие (завершение операции ввода/вывода, освобождение необходимого потоку занятого ресурса, сигнала от другого потока), часто такие потоки называют блокированными. Изменение состояния потока происходит в результате соответствующих действий. Удобно для этих целей использовать следующую диаграмму состояний и переходов (рис. 2.2.5)





**Переключение контекста** — в многозадачных ОС и средах — процесс прекращения выполнения процессором одной задачи (процесса, потока, нити) с сохранением всей необходимой информации и состояния, необходимых для последующего продолжения с прерванного места, и восстановления и загрузки состояния задачи, к выполнению которой переходит процессор.

В процедуру переключения контекста входит так называемое **планирование задачи** — процесс принятия решения, какой задаче передать управление. При переключении контекста происходит сохранение и восстановление следующей информации:

• Регистровый контекст регистров общего назначения (в том числе флаговый регистр)

• Контекст состояния сопроцессора с плавающей точкой / регистров MMX (x86)

• Состояние регистров SSE, AVX (x86)

• Состояние сегментных регистров (x86)

• Состояние некоторых управляющих регистров (например, регистр CR3, отвечающий за страничное отображение памяти процесса) (x86)

В ядре ОС с каждым потоком связаны следующие структуры:

* Общая информация pid, tid, uid, gid, euid, egid и т. д.
* Состояние процесса/потока
* Права доступа
* Используемые потоком ресурсы и блокировки
* Счетчики использования ресурсов (например, таймеры использованного

процессорного времени)

* Регионы памяти, выделенные процессу

# Тема 2.3. Диспетчеризация потоков

# 11. Многозадачность в ОС. Типы многозадачности.

**Многозадачность** — свойство операционной системы или среды выполнения обеспечивать возможность параллельной (или псевдопараллельной) обработки нескольких задач. Истинная многозадачность операционной системы возможна только в распределённых вычислительных системах.

Существует два типа многозадачности:

• Процессная многозадачность (основанная на процессах — одновременно выполняющихся программах). Здесь программа — наименьший элемент управляемого кода, которым может управлять планировщик операционной системы. Более известна большинству пользователей (работа в текстовом редакторе и прослушивание музыки).

• Поточная многозадачность (основанная на потоках). Наименьший элемент управляемого кода — поток (одна программа может выполнять 2 и более задачи одновременно)

К псевдопараллельной многозадачности можно отвести следующие типы: простое переключение, совместная (или кооперативная) многозадачность и вытесняющая (или приоритетная) многозадачность.

1. \*\*Простое переключение:\*\*

Тип многозадачности, при котором операционная система одновременно загружает в память два или более приложений, но процессорное время предоставляется только основному приложению. Для выполнения фонового приложения оно должно быть активизировано. Подобная многозадачность может быть реализована не только в операционной системе, но и с помощью программ-переключателей задач.

Преимущества: можно задействовать уже работающие программы, написанные без учёта многозадачности.

Недостатки: невозможно в неинтерактивных системах, работающих без участия человека. Взаимодействие между программами крайне ограничено.

2. \*\*Совместная(кооперативная) многозадачность:\*\*

Тип многозадачности, при котором следующая задача выполняется только после того, как текущая задача явно объявит себя готовой отдать процессорное время другим задачам.

При простом переключении активная программа получает все процессорное время, а фоновые приложения полностью замораживаются. При кооперативной многозадачности приложение может захватить фактически столько процессорного времени, сколько оно считает нужным. Все приложения делят процессорное время, периодически передавая управление следующей задаче.

Преимущества кооперативной многозадачности: отсутствие необходимости защищать все разделяемые структуры данных объектами типа критических секций и мьютексов, что упрощает программирование, особенно перенос кода из однозадачных сред в многозадачные.

Недостатки: неспособность всех приложений работать в случае ошибки в одном из них, приводящей к отсутствию вызова операции «отдать процессорное время». Крайне затрудненная возможность реализации многозадачной архитектуры ввода-вывода в ядре ОС, позволяющей процессору исполнять одну задачу, в то время как другая задача инициировала операцию ввода-вывода и ждет её завершения.

3. \*\*Вытесняющая (приоритетная) многозадачность:\*\*

Вид многозадачности, в котором операционная система сама передает управление от одной выполняемой программы другой в случае завершения операций ввода-вывода, возникновения событий в аппаратуре компьютера, истечения таймеров и квантов времени, или же поступлений тех или иных сигналов от одной программы к другой. В этом виде многозадачности процессор может быть переключен с исполнения одной программы на исполнение другой без всякого пожелания первой программы и буквально между любыми двумя инструкциями в её коде. Распределение процессорного времени осуществляется планировщиком процессов. К тому же каждой задаче может быть назначен пользователем или самой операционной системой определённый приоритет, что обеспечивает гибкое управление распределением процессорного времени между задачами (например, можно снизить приоритет ресурсоёмкой программе, снизив тем самым скорость её работы, но повысив производительность фоновых процессов). Этот вид многозадачности обеспечивает более быстрый отклик на действия пользователя. Реализована в большинстве современных операционных систем.

Преимущества:

• возможность полной реализации многозадачного ввода-вывода в ядре ОС, когда ожидание завершения ввода-вывода одной программой позволяет процессору тем временем исполнять другую программу;

• сильное повышение надежности системы в целом, в сочетании с использованием защиты памяти — идеал в виде «ни одна программа пользовательского режима не может нарушить работу ОС в целом» становится достижимым хотя бы теоретически, вне вытесняющей многозадачности он не достижим даже в теории.

• возможность полного использования многопроцессорных и многоядерных систем. Недостатки:

• необходимость особой дисциплины при написании кода, особые требования к его реентерабельности, к защите всех разделяемых и глобальных данных объектами типа критических секций и мьютексов.

**Реентерабельность**

Компьютерная программа в целом или её отдельная процедура называется реентерабельной (reentrant — повторно входимый), если она разработана таким образом, что одна и та же копия инструкций программы в памяти может быть совместно использована несколькими пользователями или процессами [3]. При этом второй пользователь может вызвать реентерабельный код до того, как с ним завершит работу первый пользователь и это как минимум не должно привести к ошибке, а при корректной реализации не должно вызвать потери вычислений (то есть не должно появиться необходимости выполнять уже выполненные фрагменты кода). Реентерабельность тесно связана с безопасностью функции в многопоточной среде (thread-safety), тем не менее, это разные понятия. Обеспечение реентерабельности является ключевым моментом при программировании многозадачных систем, в частности, операционных систем.

Для обеспечения реентерабельности необходимо выполнение нескольких условий:

• никакая часть вызываемого кода не должна модифицироваться;

• вызываемая процедура не должна сохранять информацию между вызовами;

• если процедура изменяет какие-либо данные, то они должны быть уникальными для каждого пользователя;

• процедура не должна возвращать указатели на объекты, общие для разных пользователей. В общем случае, для обеспечения реентерабельности необходимо, чтобы вызывающий процесс или функция каждый раз передавал вызываемому процессу все необходимые данные.

Таким образом, функция, которая зависит только от своих параметров, не использует глобальные и статические переменные и вызывает только реентерабельные функции, будет реентерабельной. Если функция использует глобальные или статические переменные, необходимо обеспечить, чтобы каждый пользователь хранил свою локальную копию этих переменных.

# 12. Иерархия, приоритеты и планирование потоков. Динамические уровни приоритетов.

1. \*\*Иерархия и приоритеты потоков:\*\*

- \*\*Иерархия:\*\* Потоки часто группируются по уровням приоритета в зависимости от их важности и роли. Например, системные потоки могут иметь более высокий приоритет по сравнению с прикладными.

- \*\*Приоритеты:\*\* Каждому потоку присваивается приоритет, который определяет его относительную важность и влияет на решение о том, какие потоки будут выполнены в первую очередь.

Потоки планируются на основе их приоритета планирования . Каждому потоку назначается приоритет планирования.

Уровни приоритета варьируются от нуля (самый низкий приоритет) до 31 (наивысший приоритет). Только поток обнуления страниц памяти может иметь нулевой приоритет. (Поток обнуления страниц — это системный поток, отвечающий за обнуление всех свободных страниц, если нет других потоков, которые должны выполняться.)

Система рассматривает все потоки с одинаковым приоритетом как равные. Система назначает кванты времени циклическим перебором всем потокам с наивысшим приоритетом. Если ни один из этих потоков не готов к запуску, система назначает кванты времени циклическим перебором всем потокам со следующим наивысшим приоритетом. Если поток с более высоким приоритетом становится доступным для выполнения, система перестает выполнять поток с более низким приоритетом (не позволяя ей завершить использование кванта времени) и назначает полный квант времени потоку с более высоким приоритетом.

Приоритет каждого потока определяется следующими критериями:

• Класс приоритета процесса

•Уровень приоритета потока в классе приоритета процесса.

Класс и уровень приоритета объединяются для формирования базового приоритета потока.

Каждый **процесс** принадлежит к одному из следующих классов приоритетов:

• IDLE\_PRIORITY\_CLASS

• BELOW\_NORMAL\_PRIORITY\_CLASS

• NORMAL\_PRIORITY\_CLASS

• ABOVE\_NORMAL\_PRIORITY\_CLASS

• HIGH\_PRIORITY\_CLASS

• REALTIME\_PRIORITY\_CLASS

По умолчанию класс приоритета процесса — NORMAL\_PRIORITY\_CLASS. Используйте функцию CreateProcess, чтобы указать класс приоритета дочернего процесса при его создании. Если вызывающий процесс IDLE\_PRIORITY\_CLASS или BELOW\_NORMAL\_PRIORITY\_CLASS, новый процесс наследует этот класс. Используйте функцию **GetPriorityClass** для определения текущего класса приоритета процесса и функцию **SetPriorityClass**, чтобы изменить класс приоритета процесса. Процессы, которые отслеживают систему, такие как экранные заставки или приложения, которые периодически обновляют дисплей, должны использовать IDLE\_PRIORITY\_CLASS. Это не позволяет потокам этого процесса, которые не имеют высокого приоритета, мешать потокам с более высоким приоритетом.

Используйте HIGH\_PRIORITY\_CLASS с осторожностью. Если поток выполняется с наивысшим приоритетом в течение длительных периодов времени, другие потоки в системе не будут получать процессорное время. Если несколько потоков заданы с высоким приоритетом одновременно, потоки теряют свою эффективность.

Почти никогда не следует использовать REALTIME\_PRIORITY\_CLASS, так как это прерывает системные потоки, управляющие вводом с помощью мыши, вводом с клавиатуры и фоновой очисткой диска. Этот класс может подходить для приложений, которые "разговаривают" напрямую с оборудованием или выполняют короткие задачи, которые должны иметь ограниченные перерывы.

Ниже приведены уровни приоритета в каждом классе приоритета.

• THREAD\_PRIORITY\_IDLE

• THREAD\_PRIORITY\_LOWEST

• THREAD\_PRIORITY\_BELOW\_NORMAL

• THREAD\_PRIORITY\_NORMAL

• THREAD\_PRIORITY\_ABOVE\_NORMAL

• THREAD\_PRIORITY\_HIGHEST

• THREAD\_PRIORITY\_TIME\_CRITICAL

Все потоки создаются с уровнем приоритета THREAD\_PRIORITY\_NORMAL. Это означает, что приоритет потока совпадает с классом приоритета процесса. После создания потока используйте функцию **SetThreadPriority**, чтобы настроить его приоритет относительно других потоков в процессе. Типичная стратегия заключается в использовании THREAD\_PRIORITY\_ABOVE\_NORMAL или THREAD\_PRIORITY\_HIGHEST для потока ввода процесса, чтобы обеспечить реагирование приложения на запросы пользователя.

Фоновые потоки, особенно те, которые интенсивно используют процессор, можно задать для THREAD\_PRIORITY\_BELOW\_NORMAL или THREAD\_PRIORITY\_LOWEST, чтобы обеспечить их вытеснять при необходимости. Однако если у вас есть поток, ожидающий другого потока с более низким приоритетом для выполнения какой-то задачи, обязательно заблокируйте выполнение ожидающего потока с высоким приоритетом. Для этого используйте функцию ожидания, критический раздел или функцию **Sleep**, SleepEx или **SwitchToThread**. Это предпочтительнее, чем выполнение цикла потока. В противном случае процесс может оказаться взаимоблокировкой, так как поток с более низким приоритетом никогда не планируется. Чтобы определить текущий уровень приоритета потока, используйте функцию **GetThreadPriority**.

\*\*Динамические уровни приоритетов в Windows:\*\*

В Windows каждый поток обладает динамическим приоритетом, который система может автоматически изменять для обеспечения отзывчивости и предотвращения голодания потоков. Динамический приоритет изначально совпадает с базовым приоритетом, и его система может повышать или понижать в зависимости от различных условий. Повышение приоритета происходит, например, при перемещении процесса на передний план, получении входных данных или выполнении условий ожидания. После повышения динамического приоритета система постепенно его уменьшает с течением времени. Этот механизм направлен на предотвращение инверсии приоритета и гарантирование эффективного использования процессорного времени.

*Инверсия приоритета возникает, когда два или более потоков с разными приоритетами находятся в состязании за планирование. Рассмотрим простой случай с тремя потоками: потоком 1, потоком 2 и потоком 3. Поток 1 имеет высокий приоритет и становится готовым к планированию. Поток 2, поток с низким приоритетом, выполняет код в критическом разделе. Поток 1, поток с высоким приоритетом, начинает ожидать общий ресурс из потока 2. Поток 3 имеет средний приоритет. Поток 3 получает все время процессора, так как поток с высоким приоритетом (поток 1) ожидает общих ресурсов из потока с низким приоритетом (поток 2). Поток 2 не покидает критически важный раздел, так как он не имеет наивысшего приоритета и не будет запланирован. Планировщик решает эту проблему, случайным образом повышая приоритет готовых потоков (в данном случае это держатели блокировки с низким приоритетом). Потоки с низким приоритетом выполняются достаточно долго, чтобы выйти из критического раздела, и поток с высоким приоритетом может войти в критический раздел. Если поток с низким приоритетом не получает достаточно времени ЦП для выхода из критического раздела в первый раз, он получит еще один шанс на следующем этапе планирования.*

# Тема 2.4. Синхронизация и взаимоблокировка ресурсов

# 13. Синхронизация и взаимоблокировка ресурсов. Механизмы синхронизации.

Состязательная ситуация. Понятия критического ресурса и области. Механизмы синхронизации: критические секции, мьютексы, семафоры, события, барьеры, атомарные операции

Ситуации, в которых два (и более) процесса считывают или записывают данные одновременно и конечный результат зависит от того, какой из них был первым, **называются состояниями состязания**

Чтобы избежать состязательной ситуации, нужно найти способ взаимного исключения, то есть некий способ, обеспечивающий правило, при котором если общие данные или файл используются одним процессом, возможность их использования всеми другими процессами исключается.

Та часть программы, в которой используется доступ к общей памяти, называется **критической областью или критической секцией.** Критическая область — часть программы, в которой есть обращение к совместно используемым данным. Соответственно, критический ресурс — тот ресурс, к которому осуществляется одновременный доступ

**Условия для эффективной совместной работы процессов**

1. Два процесса не могут одновременно находиться в своих критических областях.

2. Не должны выстраиваться никакие предположения по поводу скорости или количества центральных процессоров.

3. Никакие процессы, выполняемые за пределами своих критических областей, не могут блокироваться любым другим процессом.

4. Процессы не должны находиться в вечном ожидании входа в свои критические области.

Для достижения режима взаимного исключения (при котором, пока один процесс занят обновлением общей памяти и находится в своей критической области, никакой другой процесс не сможет войти в свою критическую область и создать проблему) можно предложить различные решения.

\*\*Механизмы синхронизации:\*\*

1. \*\*Критические секции:\*\*

- Области кода, где доступ к общим данным ограничивается, чтобы предотвратить конфликты.

- Предоставляют мьютекс для защиты от одновременного доступа нескольких потоков.

2. \*\*Мьютексы:\*\*

- Обеспечивают механизм блокировки, позволяющий потоку получить доступ к ресурсу или критической секции.

- Предотвращают конфликты и обеспечивают монопольный доступ к ресурсу.

3. \*\*Семафоры:\*\*

- Имеют счетчик, контролирующий количество потоков, которым разрешен доступ к ресурсу.

- Подходят для сценариев с ограниченным числом доступных ресурсов.

4. \*\*События:\*\*

- Используются для сигнализации между потоками.

- Могут быть использованы для синхронизации, где один поток ждет наступления события, а другой его сигнализирует.

5. \*\*Барьеры:\*\*

- Используются для синхронизации группы потоков, ожидающих друг друга перед выполнением следующего этапа работы.

6. \*\*Атомарные операции:\*\*

- Гарантируют неделимость выполнения операции, предотвращая переключение контекста между потоками.

- Обеспечивают безопасное выполнение операций над общими данными без необходимости блокировки.

# 14. Взаимоблокировка ресурсов в многозадачных системах. Решение задачи взаимоблокировки ресурсов

Взаимоблокировка в группе процессов возникает в том случае, если каждый процесс из этой группы ожидает события, наступление которого зависит исключительно от другого процесса из этой же группы.

**для возникновения ресурсных взаимоблокировок должны выполняться четыре условия:**

*1. Условие взаимного исключения*. Каждый ресурс либо выделен в данный момент только одному процессу, либо доступен.

*2. Условие удержания и ожидания*. Процессы, удерживающие в данный момент ранее выделенные им ресурсы, могут запрашивать новые ресурсы.

*3. Условие невыгружаемости*. Ранее выделенные ресурсы не могут быть принудительно отобраны у процесса. Они должны быть явным образом высвобождены тем процессом, который их удерживает.

*4. Условие циклического ожидания*. Должна существовать кольцевая последовательность из двух и более процессов, каждый из которых ожидает высвобождения ресурса, удерживаемого следующим членом последовательности.

Для возникновения ресурсной взаимоблокировки должны соблюдаться все четыре условия. Если одно из них не соблюдается, ресурсная взаимоблокировка невозможна.

*Решение задачи взаимоблокировки ресурсов*

Чаще всего для борьбы с взаимными блокировками используются четыре стратегии:

1. Игнорирование проблемы. Может быть, если вы проигнорируете ее, она проигнорирует вас.

2. Обнаружение и восстановление. Дайте взаимоблокировкам проявить себя, обнаружьте их и выполните необходимые действия.

3. Динамическое уклонение от них за счет тщательного распределения ресурсов.

4. Предотвращение за счет структурного подавления одного из четырех условий, необходимых для их возникновения.

**Страусиный алгоритм** Самым простым подходом к решению проблемы является «страусиный алгоритм»: спрячьте голову в песок и сделайте вид, что проблема отсутствует

**Обнаружение взаимоблокировок и восстановление работоспособности** При использовании этой технологии система не пытается предотвращать взаимоблокировки. Она позволяет им произойти, пытается обнаружить момент их возникновения, а затем предпринимает некоторые действия по восстановлению работоспособности. В случае уникального ресурса для системы нужно построить ресурсный граф. Если этот граф содержит один и более циклов, значит, мы имеем дело с взаимоблокировкой. Любой процесс, являющийся частью цикла, заблокирован намертво. Если циклов нет, значит, система не находится в состоянии взаимоблокировки. Известно множество алгоритмов для обнаружения циклов в направленных графах.

**Восстановление за счет приоритетного овладения ресурсом.** Возможность отобрать ресурс у процесса, позволить использовать его другому процессу, а затем вернуть его без извещения процесса во многом зависит от природы этого ресурса.

**Восстановление путем отката.** Если разработчики системы и операторы вычислительной машины знают о том, что есть вероятность возникновения взаимоблокировки, они могут организовать периодическое создание процессами контрольных точек.

**Восстановление путем уничтожения процессов.** Самым грубым, но и самым простым способом прервать взаимоблокировку является уничтожение одного или нескольких процессов.

**Уклонение от взаимоблокировок** Мы предполагали, что, когда процесс запрашивает ресурсы, он просит их все сразу. Но в большинстве систем ресурсы запрашиваются по одному. Система должна уметь принимать решение, представляет выделение ресурса опасность или нет, и выделять его только в том случае, если это безопасно. И при определенных условиях взаимоблокировки можно избежать, но только если заранее будет доступна вполне определенная информация

**Предотвращение взаимоблокировки** Если мы сможем гарантировать, что хотя бы одно из четырех условий возникновения взаимоблокировок никогда не будет выполнено, то взаимоблокировки станут структурно невозможными.

# Тема 2.5. Компьютерное время

# 15. Компьютерное время. Ожидаемые таймеры.

Часовые пояса. Локальное время и UTC. Эпоха UNIX. Функции POSIX для работы с временем. Ожидаемые таймеры. Протокол NTP.

**Unix-время (также POSIX-время)** — система описания моментов во времени, принятая в Unix и других POSIX-совместимых операционных системах. Определяется как количество секунд, прошедших с полуночи (00:00:00 UTC) 1 января 1970 года; этот момент называют эпохой Unix.

Время отсчитывается по часовому поясу Гринвичского меридиана без перехода на летнее время (так называемое «Универсальное координированное время» UTC — Coordinated Universal Time).

В настоящее время в POSIX-системах тип **time\_t** эквивалентен типу long. Диапазона значений типа long (32 бита) достаточно для представления дат, лежащих в отрезке длиной примерно 136 лет.

Поскольку отрицательные числа используются для представления дат до 1970 года, переполнение текущего представления типа time\_t может произойти в 2038 году, если, конечно, до этого момента представление не будет изменено.

Для более удобного представления календарного времени используется тип struct **tm**, в котором каждый компонент даты и времени хранится в отдельном целочисленном поле.

**Функция time** позволяет получить текущее системное календарное время. **Функции localtime, gmtime** преобразовывают дату из секундного представления time\_t в структурное представление struct tm.

**Функция mktime** конвертирует календарное время местного часового пояса в развёрнутом структурном формате в секундное представление. Функции **ctime** и asctime конвертируют календарное время в символьную строку. Функция **strftime** позволяет получать строковое представление времени согласно заданной форматной строке.

**Ядро таймеров POSIX.1b представляет собой набор часов, которые используются как привязка ко времени**.

Linux обеспечивает поддержку следующих часов:

**CLOCK\_REALTIME**: общесистемные часы реального времени, видимые для всех процессов, работающих в системе. Часы измеряют количество времени в секундах и наносекундах с начала эпохи. Разрешение часов равно 1/HZ секунд. Таким образом, если HZ равно 100, то разрешение часов составляет 10 мс. Если HZ равно 1000, то разрешение часов составляет 1 мс. Так как это время базируются на времени настенных часов, оно может быть изменено.

**CLOCK\_MONOTONIC**: время непрерывной работы системы, видимое всем процессам в системе. В Linux оно измеряется как количество времени в секундах и наносекундах после загрузки системы. Его разрешение равно 1/HZ с. Это время не может быть изменено каким-либо процессом.

**CLOCK\_PROCESS\_CPUTIME\_ID**: часы, измеряющие время работы процесса. Время текущего процесса, потраченное на выполнение в системе, измеряется в секундах и наносекундах. Разрешение равно 1/HZ. Это время может быть изменено.

**CLOCK\_THREAD\_CPUTIME\_ID**: То же, что и CLOCK\_PROCESS\_CPUTIME\_ID, но для текущего потока.

Обычно CLOCK\_REALTIME используется для указания абсолютного времени ожидания. CLOCK\_MONOTONIC используется для относительного времени ожидания и периодических задач. Поскольку время этих часов не может быть изменено, периодическим задачам не нужно беспокоиться о преждевременном или задержанном пробуждении, которое могло бы произойти с CLOCK\_REALTIME. Двое других часов могут использоваться для целей учёта.

 Персональные компьютеры для измерения времени использует или системный таймер (меньшая точность) или часы реального времени (большая точность).

**Системный таймер** служит для отслеживания хода времени ядром. Независимо от аппаратной платформы, идея, которая лежит в основе системного таймера, одна и та же - это обеспечение механизма управления прерываниями, которые возникают периодически с постоянной частотой. Для некоторых аппаратных платформ это реализуется с помощью электронных часов, которые генерируют колебания с программируемой частотой. В других аппаратных платформах используется декрементный счетчик (decrementer), куда можно записать некоторое начальное значение, которое будет периодически, с фиксированной частотой, уменьшаться на единицу, пока значение счетчика не станет равным нулю. Когда значение счетчика становится равным нулю, генерируется прерывание. В любом случае эффект получается один и тот же.

**Часы реального времени** (ЧРВ, RTC - Real Time Clock) — электронная схема, предназначенная для учёта хронометрических данных (текущее время, дата, день недели и др.), представляет собой систему из автономного источника питания и учитывающего устройства. Чаще всего часы реального времени встречаются в вычислительных машинах, хотя на самом деле ЧРВ присутствуют практически во всех электронных устройствах, которые должны хранить время.

**HPET** (High Precision Event Timer, таймер событий высокой точности) - тип таймера, используемый в PC-совместимых компьютерах. Совместно разработан Intel и Microsoft, и стал внедряться в чипсеты с 2005 года.

**Счетчик меток времени (TSC)** - это 64-битный регистр, присутствующий во всех процессорах x86, начиная с Pentium. Он подсчитывает количество циклов процессора с момента его сброса. Инструкция RDTSC возвращает TSC в EDX:EAX. В режиме x86-64 RDTSC также очищает старшие 32 бита RAX и RDX.

**Время Windows** - это количество времени в миллисекундах, прошедшее с момента последнего запуска системы. Функция **GetTickCount** или **GetTickCount64** возвращают текущее время Windows.

**Время прерывания** - это время с момента последнего запуска системы в интервалах по 100 наносекунд. Счетчик времени прерываний начинается с нуля при запуске системы и увеличивается при каждом прерывании часов на длину такта часов. Точная длина тактов часов зависит от базового оборудования и может отличаться в разных системах. В отличие от системного времени, количество прерываний не подлежит корректировке пользователями или службой времени Windows, что делает его лучшим выбором для измерения коротких длительностей.

**Объект таймера ожидания** - это объект синхронизации, состояние которого по достижении указанного срока устанавливается в значение Signaled. Существует два типа таймеров ожидания, которые можно создать: **сброс вручную и синхронизация.** Таймер любого типа также может быть периодическим.

**Таймер сброса вручную** - таймер, состояние которого остается сигнальным до вызова **SetWaitableTimer**, чтобы установить новое время выполнения.

**Таймер синхронизации** - таймер, состояние которого остается сигнальным до тех пор, пока поток не завершит операцию ожидания в объекте таймера.

**Периодический таймер** - таймер, который повторно активируется каждый раз, когда истечет указанный период, пока таймер не будет сброшен или отменен.

**Периодический таймер** - это либо периодический таймер сброса вручную, либо периодический таймер синхронизации.

Поток использует функцию CreateWaitableTimer или CreateWaitableTimerEx **для создания объекта таймера.** Поток создания указывает, является ли таймер таймером сброса вручную или таймером синхронизации. Создающий поток может указать имя объекта таймера. Потоки в других процессах могут открывать дескриптор для существующего таймера, указывая его имя в вызове функции **OpenWaitableTimer**. Любой поток с дескриптором объекта таймера может использовать одну из функций ожидания для ожидания, пока состояние таймера будет задано как сигнальное. Поток вызывает функцию **SetWaitableTimer** для активации таймера. Поток может использовать функцию **CancelWaitableTimer** для установки таймера в неактивное состояние. Чтобы сбросить таймер, вызовите SetWaitableTimer. Завершив работу с объектом таймера, вызовите **CloseHandle**, чтобы закрыть дескриптор для объекта таймера.

# Тема 3.1. Управление памятью

# 16. Управление памятью: адресное пространство процесса, организация памяти, основные механизмы управления памятью, концепция рабочего множества.

Часть операционной системы, которая управляет иерархией памяти (или ее частью), **называется менеджером, или диспетчером, памяти**. Он предназначен для действенного управления памятью и должен следить за тем, какие части памяти используются, выделять память процессам, которые в ней нуждаются, и освобождать память, когда процессы завершат свою работу

**Адресное пространство** - это набор адресов, который может быть использован процессом для обращения к памяти. У каждого процесса имеется собственное адресное пространство, независимое от того адресного пространства, которое принадлежит другим процессам (за исключением тех особых обстоятельств, при которых процессам требуется совместное использование их адресных пространств).

Если память распределяется в динамическом режиме, то управлять этим должна операционная система.

Организация памяти в компьютере - это способ, которым операционная система управляет и контролирует физическую и виртуальную память.

Если у компьютера недостаточно памяти для загрузки всех процессов, то требуются другие подходы к организации памяти. Самый простой из них, называемый **свопингом**, заключается в размещении в памяти всего процесса целиком, его запуске на некоторое время, а затем сбросе на диск.

Второй подход называется **виртуальной памятью**, он позволяет программам запускаться даже в том случае, если они находятся в оперативной памяти лишь частично

Другим способом отслеживания памяти является **ведение связанных списков распределенных и свободных сегментов памяти**, где сегмент либо содержит процесс, либо является пустым пространством между двумя процессами. Когда процессы и пустые пространства содержатся в списке отсортированными по адресам, то для выделения памяти создаваемому процессу (или существующему процессу, загружаемому в результате свопинга с диска) могут быть использованы несколько алгоритмов. Предположим, что диспетчер памяти знает, сколько памяти нужно выделить.

Простейший алгоритм **называется «первое подходящее».** Диспетчер памяти сканирует список сегментов до тех пор, пока не найдет пустое пространство подходящего размера. Затем пустое пространство разбивается на две части: одна для процесса и одна для неиспользуемой памяти, за исключением того статистически маловероятного случая, когда процесс в точности помещается в пустое пространство.

Незначительной вариацией алгоритма «первое подходящее» является алгоритм **«следующее подходящее».** Он работает так же, как и «первое подходящее», за исключением того, что отслеживает свое местоположение, как только находит подходящее пустое пространство. При следующем вызове для поиска пустого пространства он начинает поиск в списке с того места, на котором остановился в прошлый раз, а не приступает к поиску с самого начала, как при работе алгоритма «первое подходящее».

Другой хорошо известный и широко используемый алгоритм **— «наиболее подходящее».** При нем поиск ведется по всему списку, от начала до конца, и выбирается наименьшее соответствующее пустое пространство. Вместо того чтобы разбивать большое пустое пространство, которое может пригодиться чуть позже, алгоритм «наиболее подходящее» пытается подыскать пустое пространство, близкое по размеру к необходимому, чтобы наилучшим образом соответствовать запросу и имеющимся пустым пространствам.

При попытке обойти проблему разбиения практически точно подходящих пространств памяти на память, отводимую под процесс, и небольшие пустые пространства можно прийти к идее алгоритма **«наименее подходящее»,** то есть к неизменному выбору самого большого подходящего пустого пространства, чтобы вновь образующееся пустое пространство было достаточно большим для дальнейшего использования.

Еще один алгоритм распределения памяти называется **«быстро искомое подходящее»**. Его использование предусматривает ведение отдельных списков для некоторых наиболее востребованных искомых размеров.

В основе **виртуальной памяти** лежит идея, что у каждой программы имеется собственное адресное пространство, которое разбивается на участки, называемые страницами. Каждая страница представляет собой непрерывный диапазон адресов. Эти страницы отображаются на физическую память, но **для запуска программы одновременное присутствие в памяти всех страниц необязательно.** Когда программа ссылается на часть своего адресного пространства, находящегося в физической памяти, аппаратное обеспечение осуществляет необходимое отображение на лету. Когда программа ссылается на часть своего адресного пространства, которое не находится в физической памяти, операционная система предупреждается о том, что необходимо получить недостающую часть и повторно выполнить потерпевшую неудачу команду.

Виртуальные адреса не выставляются напрямую на шине памяти. Вместо этого они поступают в **диспетчер памяти (Memory Management Unit (MMU))**, который отображает виртуальные адреса на адреса физической памяти

**Блок управления памятью (MMU)** — это аппаратный компонент компьютера, который обрабатывает все операции с памятью и кэшированием, связанные с процессором. Другими словами, MMU отвечает за все аспекты управления памятью. Обычно он интегрирован в процессор, хотя в некоторых системах он занимает отдельную интегральную схему (ИС).

* Распределение памяти. MMU перемещает ресурсы памяти туда, где они могут наилучшим образом удовлетворить системные требования, обычно до и после выполнения системных процессов.
* Мониторинг. Он отслеживает все ресурсы памяти.
* Эффективность. Это сохраняет основную память и другие ресурсы памяти.
* Целостность системы. Это снижает вероятность фрагментации памяти и плохого
* распределения памяти.
* Целостность данных. Это гарантирует сохранение целостности данных.
* Уменьшение рисков с данными. Это сводит к минимуму риск повреждения
* данных.
* Контроль за уровнем издержек. Это снижает затраты, связанные с памятью.
* Управление физической и логической памятью

**основные механизмы управления памятью**

Основные механизмы управления памятью в операционных системах включают:

-Отслеживание свободной и занятой памяти: Операционная система должна знать, какая память в данный момент используется, и какая свободна.

-Выделение памяти процессам: Когда процесс создается, ему нужно выделить определенное количество памяти для его работы.

-Освобождение памяти при завершении процессов: Когда процесс завершается, выделенная ему память должна быть освобождена и возвращена в общий пул.

-Вытеснение процессов из оперативной памяти на диск: Если в оперативной памяти не хватает места для всех процессов, некоторые из них могут быть временно выгружены на диск.

-Возвращение процессов в оперативную память: Когда в оперативной памяти освобождается место, процессы, выгруженные на диск, могут быть возвращены обратно.

-Настройка адресов программы на конкретную область физической памяти: Каждый процесс в системе должен иметь свое собственное адресное пространство, которое отображается на физическую память.

Эти механизмы обеспечивают эффективное использование доступной памяти и поддерживают многозадачность и защиту памяти

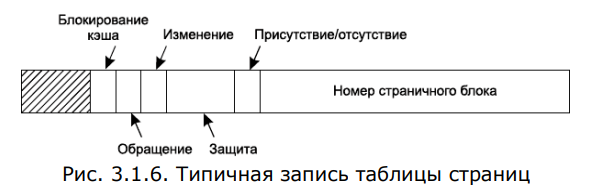
Основные различия между логической и физической памятью заключаются в следующем:

**Логическая память.** Адреса логической памяти, также называемые виртуальным адресным пространством, создаются ЦП и выполняют множество различных функций. Логическую память также называют виртуальной памятью, поскольку ее размер может динамически изменяться в зависимости от требований обработки данных пользователя.

**Физическая память**. Напротив, MMU вычисляет физические адреса. Затем они загружаются в регистр адреса памяти подсистемы памяти, который также называется физической памятью. Когда физические адреса содержат логические адреса, они называются физическим адресным пространством. В отличие от логических адресов, физические **адреса не меняются**.

**Страничная организация памяти**

Виртуальное адресное пространство состоит из блоков фиксированного размера, называемых страницами. Перенос информации между оперативной памятью и диском всегда осуществляется целыми страницами.



**Рабочий набор процесса** — это набор страниц в виртуальном адресном пространстве процесса, которые в настоящее время находятся в физической памяти. Рабочий набор содержит только страничные выделения памяти. В рабочий набор не включаются ресурсы памяти, не допускающие подкачку, такие как расширения адресных окон (AWE) или большие страницы

рабочее множество является динамическим и может меняться со временем в зависимости от поведения процесса.

# 17. Классификация запоминающих устройств. Иерархия памяти. Оперативные и постоянные запоминающие устройства.

**Запоминающее устройство** — носитель информации, предназначенный для записи и хранения данных.

**Классификация запоминающих устройств по устойчивости записи и возможности перезаписи:**

• **Постоянные (ПЗУ),** содержание которых не может быть изменено конечным пользователем (например, BIOS). ПЗУ в рабочем режиме допускает только считывание информации.

• **Записываемые (ППЗУ)**, в которые конечный пользователь может записать информацию только один раз (например, CD-R).

• **Многократно перезаписываемые (ПППЗУ)** (например, CD-RW).

• **Оперативные (ОЗУ**) — обеспечивают режим записи, хранения и считывания информации в процессе её обработки. Быстрые, но дорогие ОЗУ (SRAM) строят на триггерах, более медленные, но более дешёвые разновидности ОЗУ — динамические ЗУ (DRAM) строят на элементах, состоящих из ёмкости (конденсатора) и полевого транзистора, используемого в качестве ключа разрешения записи-чтения. В обоих видах ЗУ информация исчезает после отключения от источника питания (например, тока).

**По типу доступа ЗУ делятся на**:

* **устройства с последовательным доступом** (например, магнитные ленты). Это как кассета, где вы должны пройти через все песни, чтобы добраться до нужной.)
* **устройства с произвольным доступом (RAM)** (например, оперативная память). (Это как книга, где вы можете открыть любую страницу напрямую).
* **устройства с прямым доступом** (например, жесткие магнитные диски). (Это как DVD, где вы можете быстро перейти к определенной главе.)
* **устройства с ассоциативным доступом** (специальные устройства, для повышения производительности БД)

**Классификация запоминающих устройств по геометрическому исполнению:**

* дисковые (магнитные диски, оптические, магнитооптические);
* ленточные (магнитные ленты, перфоленты);
* барабанные (магнитные барабаны);
* карточные (магнитные карты, перфокарты, флэш-карты, и др.)
* печатные платы (карты DRAM).

**Классификация запоминающих устройств по физическому принципу:**

* перфорационные (перфокарта; перфолента);
* с магнитной записью (ферритовые сердечники, магнитные диски, магнитные ленты, магнитные карты);
* оптические (CD, DVD, HD-DVD, Blu-ray Disc);
* использующие эффекты в полупроводниках (флэш-память) и другие.

Иерархия памяти

Современная система памяти образует иерархию от быстрых типов памяти маленького размера до медленных типов памяти большого размера.

На вершине иерархии находятся **регистры процессора**. Доступ к ним занимает 0 тактов, но их всего несколько штук.

Далее идёт несколько килобайт **кэш-памяти** первого уровня, доступ к которой занимает примерно 4 такта. Потом идёт пара сотен килобайт более медленной кэш-памяти второго уровня. Потом несколько мегабайт кэш-памяти третьего уровня. Она гораздо медленней, но всё равно быстрее оперативной памяти.

Далее расположена относительно медленная **оперативная память**. Оперативную память можно рассматривать как кэш для локального диска (локальные диски тоже можно разделить на отдельные категории).

**Локальный диск** сам может рассматриваться как кэш для данных, расположенных на удалённых серверах. Резервные копии данных можно хранить на **магнитных лентах.**

Оперативные и постоянные запоминающие устройства.

В ПЗУ находятся:

* программа управления работой процессора;
* программа запуска и останова компьютера;
* программы тестирования устройств, проверяющие при каждом включении компьютера правильность работы его блоков;
* программы управления дисплеем, клавиатурой, принтером, внешней памятью;
* информация о том, где на диске находится операционная система.

**Оперативная память** (также оперативное запоминающее устройство, ОЗУ) - предназначена для временного хранения данных и команд, необходимых процессору для выполнения им операций. Оперативная память передаёт процессору данные непосредственно, либо через кэш-память. Каждая ячейка оперативной памяти имеет свой индивидуальный адрес.

Устанавливается в виде модулей объемом до 64 ГБ. Наиболее распространенный тип модулей — DIMM, тип памяти — DDR.

# Тема 3.2. Организация виртуальной памяти

# 18. Виртуальная память. Структуризация адресного пространства виртуальной памяти. Задачи управления виртуальной памятью.

**Виртуальная память** - это метод управления памятью компьютера, который позволяет выполнять программы, требующие больше оперативной памяти, чем имеется в компьютере (Это достигается за счет автоматического перемещения данных из оперативной памяти в файл подкачки, расположенный на жестком диске).

**Свопинг (подкачка)** - Механизм обмена (вытеснения и загрузки) содержимым блоков оперативной физической памяти компьютера с устройством хранения данных с целью расширения адресуемого объема оперативной памяти компьютера. Механизм является аппаратно-программным.

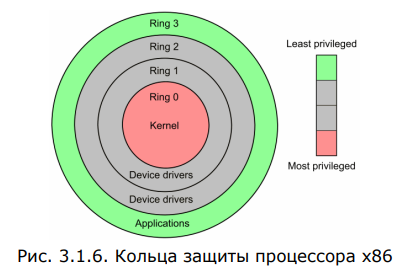
**Страничная память** - Реализации виртуальной памяти, при которой физическая память и адресное пространство разбивается на блоки (страницы), а также осуществляется страничный свопинг. Размеры страниц для X86-64: 4K, 2MB, 1GB.

**Диспетчер памяти** - Memory Management Unit (MMU) - аппаратное (программируемое) устройство, входящее в состав процессора и предназначенное для трансляции виртуальных адресов оперативной памяти в реальные.

**Буфер быстрого преобразования адреса** - Translation Lookaside Buffer (TLB) - ассоциативная память (параллельный поиск), для архитектуры x86\_64 имеет объем 64 строки.

**Уровни привилегий и кольца защиты**

В архитектуре x86 четыре кольца защиты (самый привилегированный 0).



В ARM аналогичный механизм называется уровнями исключений, здесь нулевой **уровень EL0:** область пользователя.

**EL1:** ядро («супервизор» в терминологии ARM).

**EL2:** гипервизоры, например Xen. **Гипервизор для ОС** — то же самое, что ОС для пользовательской среды. Например, Xen позволяет одновременно запускать несколько операционных систем, таких как Linux или Windows, в одной системе и изолирует операционные системы друг от друга для обеспечения безопасности и простоты отладки, точно так же, как Linux делает это для пользовательских программ. Гипервизоры являются ключевой частью современной облачной инфраструктуры: они позволяют нескольким серверам работать на одном оборудовании, сохраняя использование оборудования всегда близким к 100% и экономя много денег.

**EL3**: еще один уровень.

**Кольца защиты с отрицательными номерами**

Условное обозначение более привилегированных уровней на архитектуре X86-64 при использовании тех или иных форм виртуализации. Не имеют физического представления. В архитектуре ARM в них нет необходимости, так как там используется более естественная нумерация уровней исключений (в порядке возрастания).

**Текущий уровень привилегий** Current Privilege Level (CPL) - уровень привилегий, на котором в данный момент исполняется задача. Значение CPL хранится в поле RPL селектора сегмента кода, который помещен в регистр CS. Обычно это значение соответствует уровню привилегий дескриптора исполняемого сегмента кода. Уровень привилегий меняется, когда управление передается сегменту кода с другим значением DPL (за исключением подчиняемых сегментов кода).

**Уровень привилегий дескриптора** Descriptor Privilege Level (DPL) - наименее привилегированный уровень, на котором задача может получить доступ к сегменту или шлюзу, связанному с этим дескриптором. Уровень DPL определяется битами 46 и 45 дескриптора.

**Запрашиваемый уровень привилегий** Requested Privilege Level (RPL) используется для временного понижения своего уровня привилегий при обращении к памяти. RPL заносится в младшие биты селектора.

**//Дескриптор** - это 8-байтная единица описательной информации, распознаваемая устройством управления памятью в защищенном режиме, хранящаяся в дескрипторной таблице. Дескриптор сегмента содержит базовый адрес описываемого сегмента, предел сегмента и права доступа к сегменту. Дескрипторы являются основой защиты и мультизадачности.

**//Селектор** - это 16-битный идентификатор сегмента, помещаемый в сегментный регистр. Он содержит индекс дескриптора в дескрипторной таблице, бит определяющий, к какой дескрипторной таблице производится обращение (LDT или GDT), а также запрашиваемые права доступа к сегменту.

**//Сегментный регистр** – это 80-битный регистр, в котором доступны только младшие 16 бит, которые и содержат селектор. Остальные 64 бита называются Shadow register или «дескрипторным кэшем». Они и содержат базовый адрес, права доступа и лимит. Поэтому, как только мы загружаем в селектор соответствующее значение, процессор сразу же по полю индекс читает базу, лимит и уровень привилегий из дескриптора и заносит их в дескрипторный кэш сегментного регистра.

**Структура**

**Структуризация адресного пространства** виртуальной памяти включает в себя различные методы, такие как **сегментация** и **страничная адресация.**

*Сегментация*: Виртуальное адресное пространство разделено на сегменты, каждый из которых имеет свой уникальный адрес. Сегмент - это условно выделенная область адресного пространства определенного размера.

//Процессоры архитектуры x86-64 поддерживают два основных режима работы: Long mode («длинный» режим) и Legacy mode («унаследованный», режим совместимости с 32-битным x86)1. Эти режимы влияют на структуризацию адресного пространства виртуальной памяти.

Long mode («длинный» режим): Это «родной» режим для процессоров x86-64, который позволяет использовать все преимущества 64-битной архитектуры. В этом режиме можно выполнять 64-битные программы, а также поддерживается выполнение 32-битного кода для обратной совместимости.

Legacy mode («унаследованный» режим): Этот режим позволяет процессору работать как 32-битный процессор x86, обеспечивая полную совместимость с 32-битным кодом и операционными системами. В этом режиме 64-битные //программы и операционные системы работать не будут

**Страничная память** — способ организации виртуальной памяти, при котором виртуальные адреса отображаются на физические постранично.

Виртуальная память делится на страницы. Размер размера страницы задается процессором и обычно на x86-64 составляет 4 KiB. Это означает, что управление памятью в ядре выполняется с точностью до страницы. Когда вам понадобится новая память, ядро предоставит вам одну или несколько страниц. При освобождении памяти вы вернёте одну или несколько страниц

Ставится задача транслировать 48-битный виртуальный адрес в физический. Она решается аппаратным обеспечением — блоком управления памятью (**memory management unit, MMU**). Этот блок является частью процессора. Чтобы транслировать адреса, он использует структуры данных в оперативной памяти, называемые таблицами страниц. Вместо двухуровневой системы таблиц страниц, используемой системами с 32-битной архитектурой x86, системы, работающие в длинном режиме, используют четыре уровня таблицы страниц.

Возможные размеры страниц:

• 4 КБ (212 байт) — наиболее часто используется (как и в x86)

• 2 МБ (221 байт)

• 1 ГБ (230 байт)

**Кеширование**. Таблицы страниц хранятся в оперативной памяти. Если при каждом обращении по виртуальному адресу выполнять полностью трансляцию адресов, это будет работать очень медленно. Поэтому в процессоре реализуется специальный кеш под названием **«буфер ассоциативной трансляции»**

В ранних ОС управление памятью сводилось просто к загрузке программы и ее данных из некоторого внешнего накопителя (перфоленты, магнитной ленты или магнитного диска) в память. С появлением мультипрограммирования перед ОС были поставлены новые задачи, связанные с распределением имеющейся памяти между несколькими одновременно выполняющимися программами

**Функциями ОС по управлению памятью** в мультипрограммной системе являются:

* отслеживание свободной и занятой памяти;
* выделение памяти процессам и освобождение памяти по завершении процессов;
* вытеснение кодов и данных процессов из оперативной памяти на диск (полное или частичное), когда размеры основной памяти не достаточны для размещения в ней всех процессов, и возвращение их в оперативную память, когда в ней освобождается место;
* настройка адресов программы на конкретную область физической памяти.

**Задачи управления виртуальной памятью: задача размещения, задача перемещения, задача преобразования адресов, задача замещения**

Виртуальная память решает следующие задачи:

• размещает данные в запоминающих устройствах разного типа, например, часть программы в оперативной памяти, а часть на диске;

• перемещает по мере необходимости данные между запоминающими устройствами разного типа, например, подгружает нужную часть программы с диска в оперативную память;

• преобразует виртуальные адреса в физические.

• Операционные системы используют различные алгоритмы для определения, какие страницы данных должны быть выгружены из оперативной памяти, чтобы освободить место для других данных (LRU)

# 19. Подкачка. Алгоритмы замещения страниц. Куча (heap). Стек.

**Подкачка**

Файл подкачки или виртуальная память — это способ системы виртуальной памяти увеличить оперативную память, когда ее не хватает для совершения операций. Система автоматически задействует файл подкачки, когда приложениям не хватит системной памяти ОЗУ

*Подкачка в Linux:*

В Linux подкачка реализуется через механизм swap-раздела (или файла).

Если система обнаруживает, что в оперативной памяти недостаточно места для хранения всех активных процессов, она начинает перемещать части неиспользуемых данных на swap-раздел.

Swap-раздел может быть создан на жестком диске, и он предоставляет дополнительное пространство для хранения страниц памяти, которые временно не нужны.

Когда данные необходимы, они могут быть восстановлены из swap-раздела обратно в оперативную память.

***-Управление подкачкой:***

В Linux, управление подкачкой осуществляется ядром и специальным процессом, называемым демоном страниц. Демон страниц - это специальный процесс в Linux, который периодически проверяет, необходимо ли освободить некоторую память. Если доступной памяти становится недостаточно, демон страниц начинает освобождать страницы В Windows, управление подкачкой также осуществляется операционной системой, но подходы к управлению могут отличаться.

*Подкачка в Windows:*

В Windows есть три основных файла подкачки: hiberfile.sys, pagefile.sys и swapfile.sys

hiberfile.sys - это файл для сохранения памяти в режиме «сон» (гибернация);

pagefile.sys - основной файл подкачки;

swapfile.sys - файл подкачки отдельных

Аналогично Linux, если оперативной памяти недостаточно, Windows перемещает неиспользуемые данные на файл подкачки.

Файл подкачки обычно создается при установке системы и представляет собой зарезервированное место на жестком диске.

Windows использует алгоритмы замещения страниц для определения, какие данные следует перемещать на файл подкачки и какие - обратно в оперативную память.

**Алгоритмы замещения страниц**

Алгоритмы замещения страниц — это алгоритмы, используемые операционной системой для принятия решения о том, какие страницы памяти следует выгрузить на долгосрочное хранилище (например, в файл подкачки) при нехватке оперативной памяти

***Использование битов состояния в алгоритмах исключения страниц:***

Многие алгоритмы используют биты состояния (например, бит "**обращения**" или "**модификации**") для принятия решения о том, какие страницы следует замещать. Например, бит "использования" может помочь определить, насколько часто страница была доступна.

**алгоритм FIFO (first in first out),** который заключается в том, что первой выталкивается на диск первая из загруженных в реальную память виртуальных страниц;

**алгоритм LRU (least recently used)**, который заключается в том, что первой из памяти выталкивается на диск виртуальная страница, которая дольше всего не использовалась;

**алгоритм LFU (least frequently used),** который заключается в том, что на диск выталкивается виртуальная страница, которая наименее часто используется;

**алгоритм NUR (not used recently**), который похож на алгоритм LRU, но при выталкивании на диск выбираются те страницы, на которые дольше всего не было записи (в последнее время были и обращения, и модификации). Оптимального алгоритма подкачки виртуальных страниц не существует, т. к. поведение приложений непредсказуемо.

*Оптимальный алгоритм замещения страниц:*

Это идеальный алгоритм, который всегда выбирает страницу для замещения, которая не будет использована в течение самого долгого времени. Однако он трудно реализуем из-за невозможности предвидения будущего использования страниц.

***Алгоритм «второй шанс»:***

Модификация алгоритма FIFO. Имеет очередь страниц, и если страница получает "второй шанс" (то есть она снова используется), она не выгружается. В противном случае, она может быть выбрана для замещения.

***Алгоритм «часы»:***

Это улучшенная версия алгоритма «второй шанс», который использует круговой список страниц, аналогичный циферблату часов. Стрелка указывает на самую старую страницу. Страницы, получившие "второй шанс", не выгружаются, а их бит "второго шанса" сбрасывается.

*Алгоритм старения (Aging):*

Этот метод представляет собой модификацию алгоритма «второй шанс», где каждая страница имеет свой счетчик старения. При каждом тике счетчик уменьшается, и страницы с более низкими значениями заменяются.

*Алгоритм «рабочий набор»:*

Основан на идее, что программы обычно используют ограниченное количество страниц в определенный момент времени. Система следит за "рабочим набором" страниц для каждого процесса и пытается поддерживать их в оперативной памяти.

Если страница активно используется, она остается в рабочем наборе. Если страница не используется в течение определенного периода времени, она может быть вытеснена из рабочего набора[2](https://www.prorobot.ru/referats/r04/prorobot.ru-04-0018.pdf)

*Алгоритм WSClock (Working Set Clock):*

Это улучшение алгоритма «второй шанс», которое также учитывает временные интервалы, в течение которых страница не использовалась, и её "возраст". Использует понятие рабочего множества, подобного алгоритму «рабочий набор».

**Куча (heap)** — это сегмент памяти, для которого не устанавливается постоянный размер перед компиляцией и который может динамически управляться программистом. То есть, это «свободный пул» памяти, который можно использовать при запуске приложения.

Размер кучи приложения определяется физическими ограничениями оперативной памяти (оперативной памяти) и обычно намного больше размера стека.

Память из кучи выделяется с помощью функции **malloc**(). malloc возвращает указатель void, который затем нужно привести к правильному типу. После использования блока памяти его нужно освободить помощью функции **free**().

**Управление кучей в Windows**

Каждый процесс имеет кучу по умолчанию, предоставляемую системой. Приложения, которые часто выделяют ресурсы из кучи, могут повысить производительность с помощью частных куч**.**

**Частная куча** — это блок одной или нескольких страниц в адресном пространстве вызывающего процесса. После создания частной кучи процесс использует такие функции, как **HeapAlloc** и **HeapFree**, для управления памятью в этой куче.

Функции кучи также можно использовать для управления памятью в куче процесса по умолчанию с помощью дескриптора, возвращаемого функцией **GetProcessHeap**. Для этой цели новые приложения должны использовать функции кучи вместо глобальных и локальных функций.

Нет различий между памятью, выделенной из частной кучи, и памятью, выделенной с помощью других функций выделения памяти.

Функция **HeapCreate** создает частный объект кучи, из которого вызывающий процесс может выделять блоки памяти с помощью функции HeapAlloc. После фиксации страницы не удаляются до завершения процесса или до тех пор, пока куча не будет уничтожена путем вызова функции **HeapDestroy**. Функция HeapAlloc выделяет указанное количество байтов из частной кучи и возвращает указатель на выделенный блок. Этот указатель можно использовать в функциях HeapFree, **HeapReAlloc**, **HeapSize** и **HeapValidate**.

**Стек** — это сегмент памяти, в котором данные, такие как локальные переменные и вызовы функций, добавляются и/или удаляются по принципу «последним пришел — первым вышел» (LIFO).

Вообще говоря, стек — это структура данных, которая хранит значения данных в памяти последовательно. Однако, в отличие от массива, вы получаете доступ (чтение или запись) к данным только на «верхней части» стека. Чтение из стека называется «извлечение» (**pop**), а запись в стек — «вталкивание» (**push**).

Все архитектуры x86 используют стек в качестве временной области хранения в оперативной памяти, которая позволяет процессору быстро сохранять и извлекать данные из памяти. На текущую вершину стека указывает регистр esp.

# Тема 3.3. Управление вводом-выводом и файлами

# 20. Типы устройств ввода/вывода. Обработка внешних прерываний. Синхронный и асинхронный ввод/вывод.

**Типы устройств ввода/вывода**

Устройства ввода-вывода можно условно разделить на две категории: **блочные** устройства и **символьные** устройства.

К **блочным** относятся такие устройства, которые хранят информацию в блоках фиксированной длины, у каждого из которых есть собственный адрес. Вся передача данных ведется пакетами из одного или нескольких целых (последовательных) блоков. Важным свойством блочного устройства является то, что оно способно читать или записывать каждый блок независимо от всех других блоков. Среди наиболее распространенных блочных устройств жесткие диски, приводы оптических дисков и флеш-накопители USB.

Другой тип устройств ввода-вывода — **символьные** устройства. Они выдают или воспринимают поток символов, не относящийся ни к какой блочной структуре. Они не являются адресуемыми и не имеют никакой операции позиционирования. В качестве символьных устройств могут рассматриваться терминалы, принтеры, сетевые интерфейсы, мыши (в качестве устройства-указателя) и множество других устройств, не похожих на дисковые устройства.

Устройства ввода-вывода зачастую состоят из **механической** и **электронной** составляющих. Электронный компонент называется контроллером устройства, или адаптером. Механический компонент представлен самим устройством.

**Задача контроллера** состоит в преобразовании последовательного потока битов в блок байтов и коррекции ошибок в случае необходимости.

У каждого контроллера для связи с центральным процессором имеется несколько регистров. Путем записи в эти регистры операционная система может давать устройству команды на предоставление данных, принятие данных, включение, выключение или выполнение каких-нибудь других действий. Считывая данные из этих регистров, операционная система может узнать о текущем состоянии устройства, о том, готово ли оно принять новую команду, и т. д.

**Прямой доступ к памяти (Direct Memory Access, DMA)** - это схема, при которой центральный процессор обращается к контроллерам устройств для обмена данными, что позволяет ему не запрашивать данные у контроллера ввода-вывода побайтно, экономя рабочее время процессора.

**Режимы работы DMA:**

* Пакетный режим: Весь блок данных передается в одной непрерывной последовательности.
* Режим похищения цикла: Транзакции DMA и ЦП чередуются.
* Прозрачный режим: Контроллер DMA передает данные только тогда, когда ЦП выполняет операции, не использующие системные шины.

**Удалённый прямой доступ к памяти (remote direct memory access, RDMA)** - аппаратное решение для обеспечения прямого доступа к оперативной памяти другого компьютера при помощи высокоскоростной сети без привлечения средств операционных систем обоих компьютеров.

**Обработка внешних прерываний**

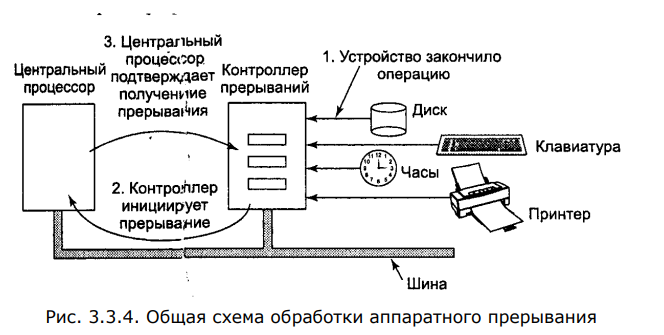
1. \*\*Прерывания на аппаратном уровне\*\*: Когда устройство ввода-вывода заканчивает работу, оно инициирует прерывание. Этот сигнал распознается микросхемой контроллера прерываний, расположенной на материнской плате.

2. \*\*Обработка прерываний\*\*: Если прерывание уже обрабатывается, и в это время приходит запрос от другого устройства по линии с более низким приоритетом, то новый запрос просто игнорируется. В этом случае устройство продолжает удерживать сигнал прерывания на шине до тех пор, пока оно не будет обслужено центральным процессором.

3. \*\***Вектор прерываний**\*\*: Номер, выставленный на адресную шину, используется в качестве индекса в таблице, называемой вектором прерываний, из которой извлекается новое значение счетчика команд.

4. \*\*Подтверждение прерывания\*\*: Вскоре после начала своей работы процедура обработки прерываний подтверждает получение прерывания, записывая определенное значение в порт контроллера прерываний.

5. \*\*Сохранение информации\*\*: Аппаратура всегда, прежде чем начать процедуру обработки прерывания, сохраняет определенную информацию. Сохраняемая информация и место ее хранения широко варьируются в зависимости от центрального процессора. Как минимум сохраняется счетчик команд, что позволяет продолжить выполнение прерванного процесса.



//Более подробно

Когда устройство ввода-вывода заканчивает свою работу, оно **инициирует прерывание** (при условии, что прерывания разрешены операционной системой). Для этого устройство выставляет сигнал на выделенную устройству специальную линию шины. Этот **сигнал распознается микросхемой контроллера** прерываний, расположенной на материнской плате. Контроллер прерываний принимает решение о дальнейших действиях.

Если прерывание уже обрабатывается, и в это время приходит запрос от другого устройства по линии с более низким приоритетом, то новый запрос просто игнорируется.

Для обработки прерывания контроллер выставляет на адресную шину номер устройства, требующего к себе внимания, и устанавливает сигнал прерывания на соответствующий контакт процессора. Этот сигнал заставляет процессор приостановить текущую работу и начать выполнять **обработку прерывания**. Номер, выставленный на адресную шину, используется в качестве индекса в таблице, называемой **вектором прерываний**

Вскоре после начала своей работы **процедура обработки прерываний подтверждает получение прерывания**, записывая определенное значение в порт контроллера прерываний. Это подтверждение разрешает контроллеру издавать новые прерывания. Благодаря тому, что центральный процессор откладывает выдачу подтверждения до момента, когда он уже готов к обработке нового прерывания, удается избежать ситуации состязаний при появлении почти одновременных прерываний от нескольких устройств

Аппаратура всегда, **прежде чем начать процедуру обработки прерывания, со­храняет определенную информацию**. Сохраняемая информация и место ее хра­нения широко варьируются в зависимости от центрального процессора. Как минимум сохраняется счетчик команд, **что позволяет продолжить выполнение прерванного процесса.** Другая крайность представляет собой сохранение всех программно доступных регистров и большого количества внутренних регистров центрального процессора.

**Обслуживание прерывания состоит из двух, а иногда и трех этапов.**1. Быстрое сохранение непостоянной информации: Когда происходит прерывание, процессор быстро сохраняет непостоянную информацию, такую как содержимое регистра, в процедуре прерывания. Это происходит на уровне запроса прерывания (IRQL) DIRQL.( , процессор быстро сохраняет важную информацию, которую он в данный момент обрабатывает, чтобы вернуться к ней позже.)

2. Обработка сохраненных переменных данных: Затем процессор обрабатывает сохраненные переменные данных в отложенном вызове процедуры (DPC), который выполняется на уровне запроса прерывания DISPATCH\_LEVEL(затем процессор начинает обрабатывать прерывание. Это может включать в себя чтение данных, которые были отправлены устройством, или выполнение каких-то действий в ответ на прерывание.).

3. Выполнение дополнительных работ: Если это необходимо, процессор выполняет дополнительные работы на уровне запроса прерывания PASSIVE\_LEVEL.( если после обработки прерывания требуется выполнить еще какую-то работу, процессор может сделать это на третьем этапе.)

**Синхронный и асинхронный ввод/вывод**

При асинхронном вводе-выводе приложение инициирует операцию ввода-вывода, а затем может продолжить свою работу (во время выполнения этого запроса). При синхронном вводе-выводе приложение блокируется до завершения выполнения операции ввода-вывода. С точки зрения вызывающего потока асинхронный ввод-вывод более эффективен, поскольку позволяет продолжать выполнение, в то время как операция ввода-вывода ставится диспетчером ввода-вывода в очередь и впоследствии выполняется. Однако приложение, использующее асинхронный ввод-вывод, требует механизма определения завершенности этой операции.

**Буферизация** — метод организации обмена, в частности, ввода и вывода данных в компьютерах и других вычислительных устройствах, который подразумевает использование буфера для временного хранения данных. **При вводе данных одни устройства или процессы производят запись данных в буфер, а другие — чтение из него, при выводе — наоборот**. Процесс, выполнивший запись в буфер, может немедленно продолжать работу, не ожидая, пока данные будут обработаны другим процессом, которому они предназначены. В свою очередь, процесс, обработавший некоторую порцию данных, может немедленно прочитать из буфера следующую порцию. Таким образом, буферизация позволяет процессам, производящим ввод, вывод и обработку данных, выполняться параллельно, не ожидая, пока другой процесс выполнит свою часть работы. Поэтому буферизация данных широко применяется в многозадачных ОС.

**Дисковое планирование**

Способ оптимизации обращения к данным, находящимся на разных участках жесткого диска (обычно магнитного). Известны следующие алгоритмы: случайное планирование, «Первым вошел — первым вышел» (FIFO), с использованием приоритета (PRI), «Последним вошел — первым вышел» (LIFO), стратегия выбора наименьшего времени обслуживания (SSTF), стратегия SCAN, стратегия C-SCAN, стратегия N-step-SCAN, стратегия FSCAN

# 21. Файловые системы. Файлы и директории. Управление внешней памятью.

**Файловая система** - порядок, определяющий способ организации, хранения и именования данных на носителях информации в компьютерах, а также в другом электронном оборудовании.

Файловая система определяет формат содержимого и способ физического хранения информации, которую принято группировать в виде файлов. Конкретная файловая система определяет размер имен файлов (и каталогов), максимальный возможный размер файла и раздела, набор атрибутов файла.

**Логическая организация** данных определяет, как файлы и директории представлены и организованы для пользователей и приложений.

**Физическая организация** данных отвечает за способ хранения данных на физическом носителе информации, таком как жесткий диск.

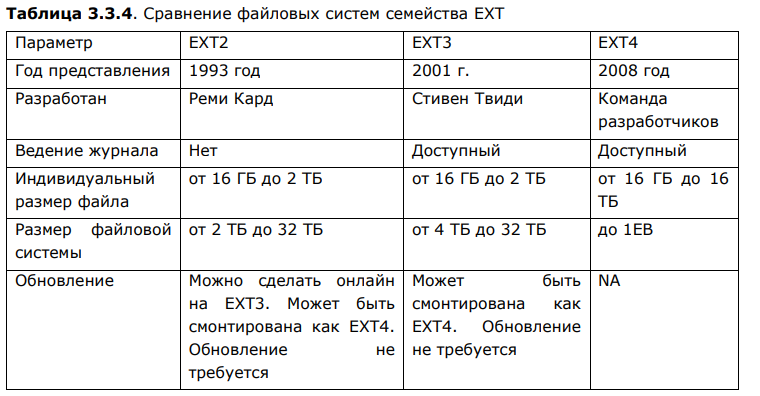
Каждому файлу на диске соответствует один и только один индексный дескриптор файла, который идентифицируется своим порядковым номером - индексом файла (**inode**)

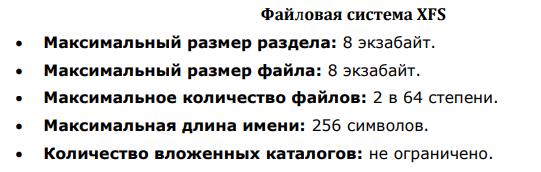
**Дескриптор файла** - это управляющий блок, содержащий информацию, необходимую ОС для различных операций с файлом. Конкретный вид дескриптора файла определяется используемой ОС. Другие названия дескриптора - блок управления файлом, элемент каталога файлов.

Типичный дескриптор файла содержит следующие данные: символическое имя файла; тип файла; атрибуты файла; данные о размещении файла во внешней памяти и др.

Список файловых систем, которые поддерживаются ядром, находится в файле /proc/filesystems.

**Виды файловых систем, предлагаемых при установке ОС на базе Linux:** Ext, Ext2, Ext3, Ext4, JFS, XFS, Btrfs, Swap.





**Типы файловых систем Windows включают**: таблица размещения файлов (FAT), FAT32 и расширенная таблица размещения файлов (exFAT); файловая система NT (NTFS); устойчивая файловая система (ReFS).



**VFS** определяет набор основных абстракций файловой системы и разрешенные с этими абстракциями операции. Системные вызовы обращаются к структурам данных VFS, определяют тип файловой системы (к которой принадлежит нужный файл) и при помощи хранящихся в структурах данных VFS указателей на функции запускают соответствующую операцию в указанной файловой системе.

**Файл** - поименованная совокупность данных, обычно размещаемая на внешних запоминающих устройствах.

Файл в системе Linux — это последовательность байтов произвольной длины (от 0 до некоторого максимума), содержащая произвольную информацию.

Для удобства файлы могут группироваться в каталоги. Каталоги хранятся на диске в виде файлов, и с ними можно работать практически так же, как с файлами. Каталоги могут содержать подкаталоги, что приводит к иерархической файловой системе.

Существует два способа задания имени файла в системе Linux (как в оболочке, так и при открытии файла из программы). Первый способ заключается в использовании **абсолютного пути. или относительные пути**, которые указываются относительно текущего рабочего каталога.(прописываем папка относитьльно какой-то программы )/source/img(unity)  
***Ссылка*** - это способ указания на другой файл или директорию в файловой системе. Она представляет собой запись, которая идентифицирует другой файл или директорию. Ссылки позволяют размещать один и тот же файл в нескольких директориях. ( это записи каталога, указывающие на существующие файлы. Они могут быть жесткими или символьными.) (**Символическая** ссылка - это отдельный файл, который указывает на другой файл или директорию. Жесткая ссылка - это прямая ссылка на физическое местоположение файла на диске.)

Каждому файлу на диске соответствует один и только один **индексный дескриптор файла**, который идентифицируется своим порядковым номером - индексом файла (inode). Это означает, что число файлов, которые могут быть созданы в файловой системе, ограничено числом индексных дескрипторов, которое либо явно задается при создании файловой системы, либо вычисляется исходя из физического объема дискового раздела.

Управление внешней памятью

1. **Файловая система NFS** позволяет произвольному набору клиентов и серверов пользоваться общей файловой системой. Она может работать как в локальной сети, так и через Глобальную сеть.
2. **Экспорт каталогов**: Каждый сервер NFS экспортирует один или несколько своих каталогов, предоставляя доступ к ним удаленным клиентам. Список экспортируемых сервером каталогов хранится в файле (обычно это файл /etc/exports).
3. **Монтирование каталогов**: Клиенты получают доступ к экспортируемым каталогам, монтируя эти каталоги. Если клиент монтирует (удаленный) каталог, то этот каталог становится частью иерархии каталогов клиента.
4. **Системные вызовы**: Файловой системой NFS поддерживается большинство системных вызовов операционной системы Linux, за исключением системных вызовов open и close.
5. **Сообщение lookup**: Вместо открытия файла, чтобы прочитать его, клиент посылает на сервер сообщение lookup (содержащее имя файла) с запросом найти этот файл и вернуть описатель файла.
6. **Серверы без состояния (stateless)**: Преимущество этой схемы заключается в том, что серверу не нужно помнить (между обращениями к нему) что-либо об открытых соединениях. Поэтому если на сервере произойдет сбой с последующей перезагрузкой, то не будет потеряно никакой информации об открытых файлах, так как ее просто нет.

**//Управление памятью** – это процесс управления и координации памяти компьютера, назначение частей, известных как блоки, различным запущенным программам для оптимизации общей производительности системы.

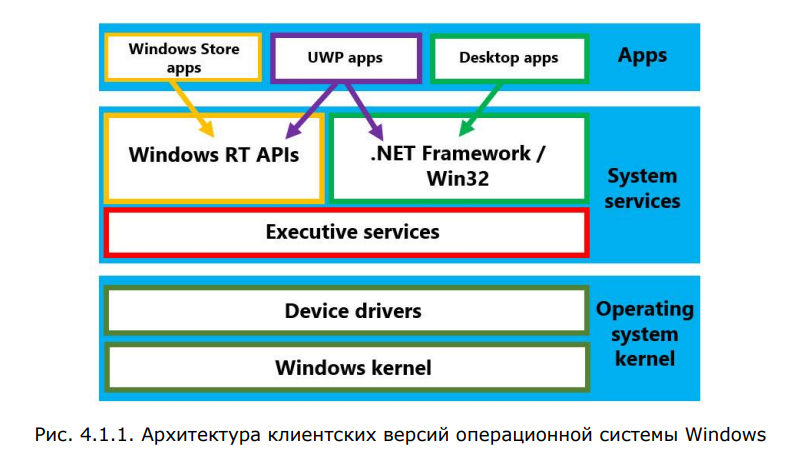
Это самая важная функция операционной системы, которая управляет основной памятью. Это помогает процессам перемещаться вперед и назад между основной памятью и исполнительным диском. Это помогает ОС отслеживать каждую область памяти, независимо от того, выделена она для какого-либо процесса или //остается свободной.

**Кеширование** в операционной системе служит для минимизации количества операций передачи данных. Для достижения данной цели в Linux-системах между дисковыми драйверами и файловой системой имеется кэш. Кэш представляет собой таблицу в ядре, в которой хранятся тысячи недавно использованных блоков. Когда файловой системе требуется блок диска (например, блок i-узла, каталога или данных), то сначала проверяется кэш. Если нужный блок есть в кэше, он берется оттуда, при этом обращения к диску удается избежать (что значительно улучшает производительность системы). Если же блока в кэше страниц нет, то он считывается с диска в кэш, а оттуда копируется туда, куда нужно. Поскольку в кэше страниц есть место только для фиксированного количества блоков, то используется один из описанных ранее алгоритмов замещения страниц.

# Тема 4.1. Введение в операционную систему Windows

# 22. Принципы организации и структура ОС Windows. Обзор версий Windows. Методы инсталляции ОС Windows.

**Принципы организации и структура ОС Windows**

****

Архитектура операционной системы Windows включает **ядро операционной системы, системные службы и приложения**

На самом низком уровне операционной системы **ядро операционной системы** состоит из самого ядра Windows и драйверов устройств низкого уровня.

Ядро отвечает за прием запросов операционной системы от системных служб. Затем ядро преобразует эти запросы в инструкции для аппаратного обеспечения компьютера, включая центральный процессор (ЦП), память и аппаратные устройства. При запуске операционной системы сначала инициализируются ядро и связанные с ним низкоуровневые драйверы устройств, а затем службы операционной системы.

**Службы операционной системы** являются частью операционной системы, а не компонентами, которые вы устанавливаете после развертывания операционной системы. Кроме того, службы операционной системы функционируют без каких-либо действий со стороны пользователя. Фактически они начинаются до того, как пользователь войдет в систему. И службы операционной системы, и драйверы устройств являются программным обеспечением. Однако разница между ними заключается в том, что драйверы устройств напрямую взаимодействуют с аппаратными устройствами или компонентами. Как правило, системная служба взаимодействует с другими программными компонентами операционной системы.

На верхнем уровне операционной системы **приложения** работают путем взаимодействия с пользователем компьютера, а на нижнем уровне — путем интеграции со службами операционной системы. Вы устанавливаете приложения после установки операционной системы, и для их использования вам необходимо запускать приложения вручную.

**Отличия службы от приложения**.

Служба – процесс, работающий, даже когда никто не зарегистрирован в системе. Служба использует несколько потоков: один поток принимает команды от операционной системы (Start, Stop, Pause, Resume и т.п.), второй поток является основным рабочим потоком (обычно он создает еще множество потоков для выполнения отдельных задач). Завершение этого потока завершает работу всей службы. Управляется диспетчером управления службами (**Service Control Manager, SCM**). Физически может находиться в .EXE или .DLL-файле, в одном файле может находиться множество служб. Если служба находится в .DLL-файле, ее запускает svchost.exe.

**Реестр** — это база данных, в которой Windows хранит параметры конфигурации пользователя и компьютера. Всякий раз, когда вы вносите изменения в конфигурацию Windows, это изменение фиксируется в реестре.

Реестр Windows организован иерархически. На верхнем уровне имеется пять кустов реестра, которые представляют собой отдельный набор связанных параметров, структурированных как серия ключей, подразделов и значений.

Операционная система Windows имеет **модульную структуру,** что обеспечивает ее работу на самых разных аппаратных платформах, с самыми разными приложениями. Кроме того, этим достигается относительно эффективная возможность модернизации ОС (либо путем замены каких-либо отдельных структурных блоков, либо путем включения новых блоков)

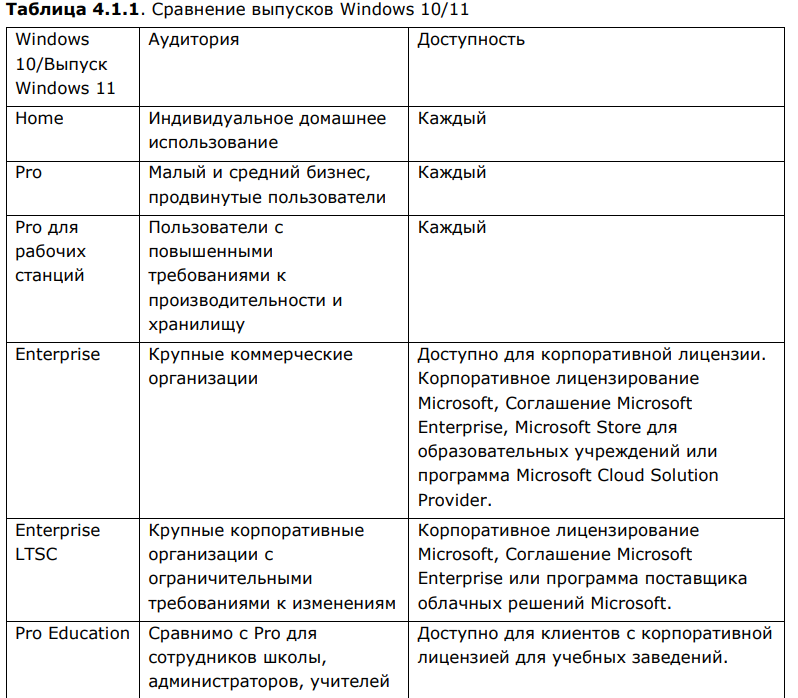
Принцип модульной структуры состоит в том, что за реализацию каждой из функций ОС отвечает отдельный модуль. Все остальные части системы и приложения обращаются к этой функции через стандартный интерфейс. А доступ к основным системным данным можно получить только через определенные функции.

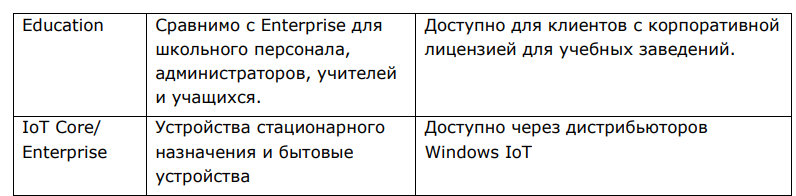
Самый удивительный аспект состоит в том, что ядро Windows практически не меняется в зависимости от всех этих архитектур и SKU. Ядро динамически масштабируется в зависимости от архитектуры и процессора, на котором оно работает, так, чтобы пользоваться всеми возможностями оборудования. Конечно, в ядре присутствует определённое количество кода, связанного с конкретной архитектурой, однако его там минимальное количество, что позволяет Windows запускаться на разнообразных архитектурах.

**Клиентские версии Windows**

Различные выпуски Windows удовлетворяют потребности потребителей, от частных лиц до крупных предприятий.

* **Home** - Индивидуальное домашнее использование.
* **Pro** - Малый и средний бизнес, продвинутые пользователи.
* **Pro для рабочих станций** - Пользователи с повышенными требованиями к производительности и хранилищу.
* **Enterprise** - Крупные коммерческие организации.
* **Enterprise LTSC** - Крупные корпоративные организации с ограничительными требованиями к изменениям.
* **Pro Education** - Сравнимо с Pro для сотрудников школы, администраторов, учителей и учащихся.
* **Education** - Сравнимо с Enterprise для школьного персонала, администраторов, учителей и учащихся.
* **IoT Core/ Enterprise** - Устройства стационарного назначения и бытовые устройства.





Enterprise LTSC получает только обновления безопасности и другие важные обновления. Эти среды обычно представляют собой закрытые системы, разработанные с учетом определенной спецификации, на которую могут повлиять традиционные обновления.

**Серверные версии Windows Server**

*Серверные версии Windows:* Последняя LTSC-версия: **Windows Server 2022**, также поддерживается Windows Server 2019.

*Безопасность:* Windows Server 2022 обеспечивает многоуровневую безопасность и гибридные возможности с Azure.

Встроенные возможности защищенного ядра снижают риск от угроз безопасности.

*Защищенное Соединение:* Улучшенное защищенное соединение с использованием быстрых и защищенных зашифрованных соединений HTTPS и стандартного шифрования SMB AES 256.

***Редакции Windows Server 2022:***

* Standard: Основная функциональность, исключая Hotpatching и SDN. Storage Replica ограничен до 2TB и 2 автоматически лицензируемых машин.
* Datacenter: Поддерживает все функции, кроме Hotpatching и SMB over QUIC.
* Datacenter: Azure Edition: Премиальная редакция, поддерживается в Azure, предлагает дополнительные функции, такие как горячее обновление и SMB через QUIC.

Методы инсталляции ОС Windows

Существует несколько разных вариантов развертывания сервера Windows и настольных операционных систем бизнес-класса. Это могут быть **ручная установка**, **полностью автономные** (не обслуживаемые) установки, **автономные готовые** или дополнительно настроенные установки, а **также развертывания заготовленных** и, возможно, специально настроенных образов операционной системы.

кратко

**Методы инсталляции ОС Windows(процесс установки ОС на компьютер)**

*Ручная установка с использованием установочного носителя(на флешке есть ос ):*

Установка системы вручную с использованием установочного носителя.

Применяется, когда нет подходящего образа для конкретной аппаратной платформы или при небольшом количестве установок.

*Автономная (необслуживаемая) установка(когда все необходимые файлы для установки уже находятся на установочном носителе):*

Используется файл ответов, предоставляющий ответы на вопросы, задаваемые во время ручной установки.

Позволяет автоматизировать установку с заданными параметрами.

*Установка, сопровождаемая производителем:*

Некоторые производители поставляют носители автономной установки, упрощающие процесс для конечного пользователя.

*Создание копий или образов систем:*

Полезно при развертывании нескольких идентичных компьютеров или серверов.

Создание образов системы с помощью инструментов Microsoft, таких как WDS, Sysprep, или сторонних разработчиков.

*-Служба развертывания Windows (WDS)(развернуть образ)*

Позволяет развертывать установочные образы и специально настроенные образы на серверах и настольных компьютерах.

*-Диспетчер настроек системного центра (SCCM)(управлем настраиваем)*

Средство развертывания и управления образами систем с возможностью централизованного управления.

*-Инструментальный набор развертывания Microsoft (MDT)(делаем образ)*

Обеспечивает средства для создания образов, управления драйверами и приложениями, а также автоматизации процесса развертывания.

**1. Ручная установка с использованием установочного носителя**

**Устанавливать систему вручную** не очень сложно. Нужно воспользоваться установочным носителем и пройти все этапы установки, документируя по мере продвижения все настройки. Этот способ иногда необходим, когда у администратора нет образа, подходящего для определенной аппаратной платформы, или когда регулярно развертывается только небольшое количество систем, а время, необходимое на создание автоматических установок или установок с использованием образов, не ограничено и не является ключевым фактором для организации.

**Автономные установк**и могут быть полезными при развертывании большого количества настольных компьютеров и серверов, на которых установлено одинаковое оборудование. Файл автономной установки представляет собой текстовый XML-файл, содержащий ответы на все вопросы, задаваемые во время ручной установки.

Конфигурационные файлы автономной установки обычно называют **файлами ответов.** Опции в некоторых файлах ответов автономной установки могут включать принятие лицензионного соглашения конечным пользователем, ввод лицензионного ключа, вариант форматирования жесткого диска, определение раздела или размера тома для операционной системы и многое другое. Теперь это называется файлом необслуживаемой установки (unattended installation file). Чтобы выбрать файл ответов во время установки, нужно загрузить среду предустановки Windows и выполнить команду setup.exe с параметром /unattend:filename. При отсутствии параметра /unattend программа установки будет искать файл с именем Autounattend.xml в корневых папках всех доступных дисков. Поэтому проще всего записать файл ответа на USB-устройство флэш-памяти, вставить его в компьютер, а затем загрузить этот компьютер с установочного диска Windows.

**Создание копий или образов систем** может быть полезно при развертывании нескольких идентичных настольных компьютеров и серверов. Вы создаете настольный компьютер или сервер, подготавливаете систему для клонирования или создания образа и копируете или захватываете образ системы с помощью средств сторонних разработчиков или средств развертывания от Microsoft, таких как WDS.

**WDS** — это серверная роль в Windows Server, которая спроектирована для оказания помощи организациям, использующим доменную службу Active Directory, при развертывании систем Windows. Система WDS обычно настраивается для обеспечения служб хранения и извлечения образов, необходимых для их развертывания, клиентских компонентов, таких как образы загрузки РХЕ, и управляющих компонентов, используемых для конфигурирования параметров WDS, в том числе добавление образов на сервер WDS и создание мультивещательных передач.

**WIM** — это формат образа диска на основе файлов, который впервые был представлен в Windows Vista. Файлы WIM представляют собой сжатые пакеты, содержащие несколько связанных файлов. Формат WIM-файла оптимизирован для максимального сжатия с использованием LZX или для быстрого сжатия с использованием XPRESS. Структура файла WIM содержит до шести типов ресурсов: заголовок, файловый ресурс, ресурс метаданных, таблицу поиска, данные XML и таблицу целостности. Для работы с WIM-файлами используют программы ImageX и DISM из состава WADK. DISM также входит в состав Windows.

Загрузочные образы и установочные образы являются разными типами образов операционной системы и выполняют разные функции. Вот их основные отличия:

1. **Загрузочные образы (Boot Images):**
   * **Функция:** Загрузочные образы предназначены для инициализации загрузки операционной системы. Они содержат минимальный набор файлов и компонентов, необходимых для запуска процесса загрузки.
   * **Состав:** Обычно включают в себя ядро операционной системы, необходимые системные файлы и компоненты загрузки. Эти образы загружаются в оперативную память при старте компьютера и запускают процесс загрузки операционной системы.
2. **Установочные образы (Install Images):**
   * **Функция:** Установочные образы предназначены для развертывания операционной системы на жесткий диск или другие устройства хранения данных. Они включают в себя полный набор файлов и компонентов операционной системы, необходимых для ее установки и функционирования после завершения процесса установки.
   * **Состав:** В установочные образы входят операционная система, драйверы, системные файлы, приложения (в зависимости от конфигурации), а также информация о настройках и параметрах установки.

# 23. ОС Windows: организация рабочей среды пользователя, работа с учетными записями пользователей и групп, работа с профилями пользователей.

Рабочая среда пользователя состоит из настроек рабочего стола, например, цвета экрана, настроек мыши, размера и расположения окон, из настроек процесса обмена информацией по сети и с устройством печати, переменных среды, параметров реестра и набора доступных приложений

Для управления средой пользователя предназначены следующие средства Windows:

**Сценарий входа в сеть** **(сценарий регистрации)** представляет собой командный файл, имеющий расширение .bat, или исполняемый файл с расширением .ехе, который выполняется при каждой регистрации пользователя в сети. Сценарий может содержать команды операционной системы, предназначенные, например, для создания соединения с сетью или для запуска приложения. Кроме того, с помощью сценария можно устанавливать значения переменных среды, указывающих пути поиска, каталоги для временных файлов и другую подобную информацию.

**Профили пользователей**. В профиле пользователя хранятся все настройки рабочей среды компьютера, на котором работает Windows 2000, определенные самим пользователем. Это могут быть, например, настройки экрана и соединения с сетью.

**Сервер сценариев Windows** (Windows Scripting Host, WSH). Сервер сценариев независим от языка и предназначен для работы на 32-разрядных платформах Windows. Он включает в себя как ядро сценариев Visual Basic Scripting Edition (VBScript), так и JScript. Сервер сценариев Windows предназначен для выполнения сценариев прямо на рабочем столе Windows или на консоли команд. При этом сценарии не надо встраивать в документ НТМL.

Большинство настроек рабочей среды пользователя можно настроить с помощью **групповых политик**.

**Работа с учетными записями пользователей и групп**

**Локальные учетные записи** пользователей определяются локально на устройстве и могут назначаться только на этом устройстве. **Локальные учетные записи пользователей** — это субъекты безопасности, которые используются для защиты и управления доступом к ресурсам на устройстве для служб или пользователей.

**Учетные записи локальных пользователей по умолчанию** — это встроенные учетные записи, которые создаются автоматически при установке операционной системы. Учетные записи локальных пользователей по умолчанию не могут быть удалены или удалены и не предоставляют доступ к сетевым ресурсам. Учетные записи локальных пользователей по умолчанию используются для управления доступом к ресурсам локального устройства на основе прав и разрешений, назначенных учетной записи.

Учетные записи локальных пользователей по умолчанию и создаваемые локальные учетные записи пользователей находятся в папке Пользователи. Папка Пользователи находится в папке Локальные пользователи и группы в локальной консоли управления Майкрософт (MMC).

**//Управление компьютером** — это набор средств администрирования, которые можно использовать для управления локальным или удаленным устройством. Вы также можете управлять локальными пользователями с помощью NET.EXE USER и управлять локальными группами с помощью NET.EXE LOCALGROUP или с //помощью различных командлетов PowerShell и других технологий сценариев.

**Учетная запись локального администратора по умолчанию** — это учетная запись пользователя для системного администрирования. У каждого компьютера есть учетная запись администратора (SID S-1-5-домен-500, отображаемое имя — Администратор). Учетная запись администратора — это первая учетная запись, которая создается при установке Windows.

Учетная запись администратора имеет полный контроль над файлами, каталогами, службами и другими ресурсами на локальном устройстве. Учетная запись администратора может создавать других локальных пользователей, назначать права пользователей и назначать разрешения. Учетная запись администратора может в любое время управлять локальными ресурсами, изменив права и разрешения пользователя. Учетную запись администратора по умолчанию нельзя удалить или заблокировать, но ее можно переименовать или отключить.

**Гостевая учетная запись** позволяет случайным или разовым пользователям, у которых нет учетной записи на компьютере, временно войти на локальный сервер или клиентский компьютер с ограниченными правами пользователя. По умолчанию учетная запись гостя отключена и имеет пустой пароль. Так как учетная запись гостя может предоставлять анонимный доступ, она считается угрозой безопасности. По этой причине рекомендуется оставить учетную запись гостя отключенной, если только ее использование не требуется. По умолчанию учетная запись "Гость" является единственным членом группы SID S-1-5-32-546 "Гости" по умолчанию, которая позволяет пользователю войти на устройство.

**Управление учетной записью локального пользователя**

**Применение ограничений локальной учетной записи**

**Контроль учетных записей (UAC)** — это функция безопасности, которая информирует вас о том, что программа вносит изменения, требующие административных разрешений. UAC работает путем настройки уровня разрешений учетной записи пользователя. По умолчанию контроль учетных записей настраивается для уведомления при попытке приложений внести изменения в компьютер, но вы можете изменить это, когда управление учетными записями уведомляет вас.

Контроль учетных записей позволяет рассматривать учетную запись с правами администратора как учетную запись обычного пользователя, не являющегося администратором, до тех пор, пока не будут запрошены и утверждены полные права, также называемые повышением прав.

**Работа с профилями пользователей**

Система создает профиль пользователя при первом входе пользователя на компьютер. При последующих входах система загружает профиль пользователя, а затем другие системные компоненты настраивают среду пользователя в соответствии с информацией в профиле.

Типы профилей пользователей: локальные, перемещаемые, обязательные, временные.

Профиль пользователя состоит из следующих элементов: куста реестра HKEY\_CURRENT\_USER и набора папок, хранящегося в файловой системе.

**Локальный профиль пользователя** создается при первом входе пользователя на компьютер. Профиль хранится на локальном жестком диске компьютера. Изменения, внесенные в профиль локального пользователя, относятся к пользователю и компьютеру, на котором внесены изменения.

Профиль пользователя не загружается автоматически при входе пользователя с помощью функции LogonUser. Чтобы загрузить профиль пользователя программным способом, используйте функцию LoadUserProfile. Чтобы выгрузить профиль пользователя, загруженный LoadUserProfile, вызовите функцию UnloadUserProfile.

**Перемещаемый профиль пользователя** — это копия локального профиля, которая копируется в общую папку сервера и хранится в ней. Этот профиль загружается на любой компьютер, на который пользователь входит в сеть. Изменения, внесенные в перемещаемый профиль пользователя, синхронизируются с серверной копией профиля при выходе пользователя из системы. Преимущество перемещаемых профилей пользователей заключается в том, что пользователям не нужно создавать профиль на каждом компьютере, который они используют в сети.

**Обязательный профиль пользователя** — это тип профиля, который администраторы могут использовать для указания параметров для пользователей. Только системные администраторы могут вносить изменения в обязательные профили пользователей. Изменения, внесенные пользователями в параметры рабочего стола, теряются при выходе пользователя из системы.

**Временный профиль** выдается каждый раз, когда ошибка препятствует загрузке профиля пользователя. Временные профили удаляются в конце каждого сеанса, а изменения, внесенные пользователем в параметры рабочего стола и файлы, теряются при выходе пользователя из системы. Временные профили доступны только на компьютерах под управлением Windows 2000 и более поздних версий.

# Тема 4.2. Администрирование в ОС Windows

# 24. Системный реестр ОС Windows, его назначение и использование.

**Реестр** — это база данных, в которой Windows хранит параметры конфигурации пользователя и компьютера. Всякий раз, когда вы вносите изменения в конфигурацию Windows, это изменение фиксируется в реестре

Реестр Windows организован иерархически. На верхнем уровне имеется пять кустов реестра, которые представляют собой отдельный набор связанных параметров, структурированных как серия ключей, подразделов и значений:

**HKEY\_CLASSES\_ROOT (Ассоциации файлов и приложений для открытия файлов)** Этот куст содержит информацию о ассоциации файлов и определяет, какое приложение открывается, когда пользователь дважды щелкает определенный тип файла в файловой системе. Например, он определяет, что приложением для файлов .xlsx является Microsoft Excel. Этот куст заполняется на основе настроек, связанных с компьютером и пользователем, которые хранятся в разделах HKEY\_LOCAL\_MACHINE\Software\Classes и HKEY\_CURRENT\_USER\Software\Classes. Обычно вы не будете вносить изменения в этот куст.

**HKEY\_CURRENT\_USER** Этот куст содержит информацию о конфигурации для текущего пользователя, вошедшего в систему. Такие элементы, как цветовая схема Windows пользователя и настройки шрифта, хранятся в соответствующих значениях под этим кустом. При ссылке на этот куст при редактировании реестра этот куст иногда называют HKCU. Этот куст представляет собой ярлык ключа, хранящегося в HKEY\_USERS.

**HKEY\_LOCAL\_MACHINE** Вероятно, это самый важный куст, в который вы, вероятно, будете вносить больше всего изменений. Этот куст, иногда называемый сокращенно HKLM, хранит все параметры конфигурации, связанные с компьютером. Здесь хранятся параметры, относящиеся к общесистемным настройкам, установленным программам и аппаратному обеспечению.

**HKEY\_USERS** В этом кусте содержатся профили всех пользователей, зарегистрированных на компьютере. Каждый пользователь имеет свою ветку с индивидуальными настройками.

**HKEY\_CURRENT\_CONFIG** Этот куст содержит информацию о текущем профиле оборудования, который локальный компьютер использовал во время запуска системы. Обычно вы не вносите изменения в этот куст. (параметры видеокарты, монитора и других устройств.)

Для поддержания структуры базы данных аналогичные настройки хранятся в папках и подпапках, известных как **ключи и подразделы**. Это упрощает ссылку на определенное значение реестра. Значения определяют поведение операционной системы и хранятся в разделах и подразделах. Существует много типов значений, в зависимости от типа данных, которые каждое из них хранит.

Значения определяют поведение операционной системы и хранятся в разделах и подразделах. Ниже перечислены наиболее распространенные типы значений реестра:

**REG\_BINARY**. Необработанные двоичные данные. Эти значения обычно отображаются в шестнадцатеричном формате. Информация об оборудовании часто хранится в значениях REG\_BINARY.

**REG\_DWORD**. 4-байтовые числа (32-битное целое число). Многие значения, связанные с драйверами устройств и службами, хранятся в значениях REG\_DWORD.

**REG\_SZ.** Текстовая строка фиксированной длины.

**REG\_EXPAND\_SZ.** Текстовая строка переменной длины.

**REG\_MULTI\_SZ**. Несколько строковых значений.

# 25. ОС Windows: планирование и назначение разрешений NTFS, списки управления доступом.

*1. Введение:*

NTFS (New Technology File System) - файловая система, используемая в операционных системах Windows.

Разрешения NTFS определяют доступ к файлам и папкам на уровне файловой системы.

*2. Понимание Разрешений:*

Разрешения определяют, кто может что делать с файлами и папками (чтение, запись, исполнение).

Каждый объект (файл или папка) имеет ACL (Access Control List), содержащий список разрешений.

*3. Пользователи и Группы:*

Разрешения могут быть назначены пользователям или группам пользователей.

Группы упрощают управление, так как разрешения могут быть назначены целой группе.

*4. Права и Роли:*

Права: Определяют общие действия, такие как изменение системного времени.

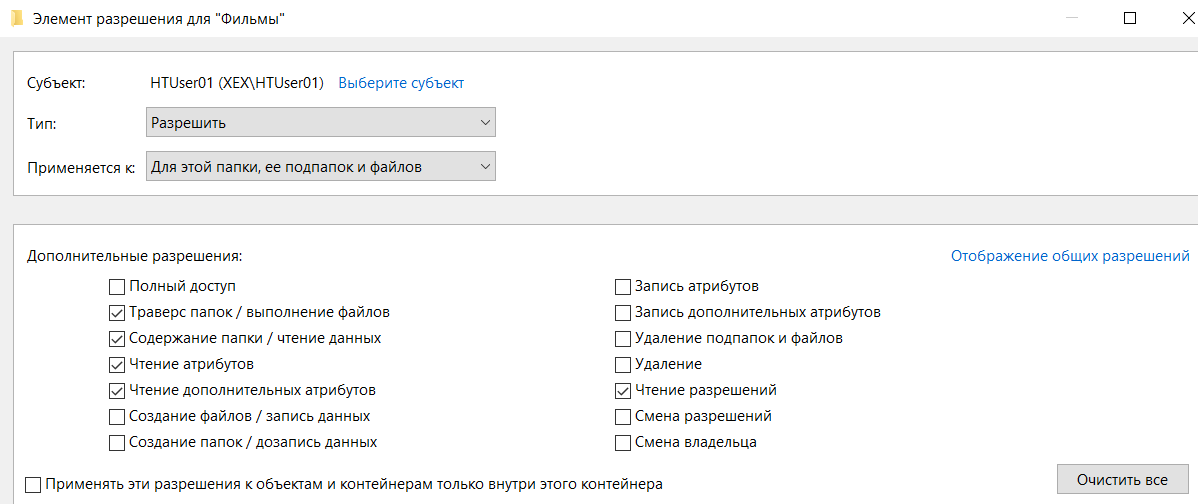
Роли: Задают специфические задачи, такие как администратор или пользователь.

*5. Процесс Назначения Разрешений:*

Выбор Объекта: Выберите файл или папку, для которой вы хотите настроить разрешения.

Свойства и Закладка "Безопасность": Правый клик по объекту, выберите "Свойства" и перейдите на закладку "Безопасность".

Выбор Пользователя или Группы: Нажмите "Изменить" и выберите нужного пользователя или группу.



*6. Работа с Разрешениями:*

Разрешения по Умолчанию: Определяют доступ к новым объектам до изменения разрешений.

Наследование Разрешений: Разрешения могут быть унаследованы от родительских объектов.

*7. Основные Разрешения:*

Полный доступ (Full Control): Полные права на чтение, запись, изменение, удаление и выполнение.

Чтение и Исполнение (Read & Execute): Позволяет просматривать и выполнять файлы, но не изменять.

Запись (Write): Позволяет создавать и изменять файлы, но не удалять или исполнять.

*8. Пример Назначения Разрешений:*

Задача: Назначить группе "Редакторы" разрешение на изменение файлов в папке "Проекты".

Действия:

Выберите папку "Проекты".

Перейдите на закладку "Безопасность".

Нажмите "Изменить" и добавьте группу "Редакторы" с разрешением "Изменение".

*9. Проверка Разрешений:*

Проверяйте разрешения, удостоверьтесь, что необходимые группы и пользователи имеют доступ.

*10. Завершение:*

Разрешения NTFS важны для безопасности и управления файлами в Windows.

Регулярно аудитите разрешения для поддержания актуальности и безопасности.

# 26. Средства автоматической настройки в ОС Windows.

BAT-файлы. Powershell. WMI. ETW. Групповые политики. Административные шаблоны.

**В Windows есть две оболочки командной строки: командная оболочка cmd и PowerShell**. Каждая оболочка — это программа, которая обеспечивает прямую связь между оператором и операционной системой или приложением, предоставляя среду для автоматизации ИТ-операций.

Командная оболочка cmd была первой оболочкой, встроенной в Windows, для автоматизации повседневных задач, с пакетными (.bat или .cmd) файлами. С помощью Windows Script Host можно запускать более сложные скрипты в командной оболочке (команды cscript и vscript).

PowerShell был разработан для расширения возможностей командной оболочки для выполнения команд PowerShell, называемых командлетами. Командлеты похожи на команды Windows, но предоставляют более расширяемый язык сценариев. Команды Windows и командлеты PowerShell можно запускать в PowerShell, но командная оболочка может выполнять только команды Windows, а не командлеты PowerShell. Встраивание - это механизм, который позволяет использовать функциональность PowerShell в других приложениях, включая графический интерфейс.

**BAT-файлы** – Текстовые файлы с расширением .cmd или .bat (от слова batch).

**Инструментарий управления Windows (WMI)** — это инфраструктура для управления данными и операциями в операционных системах Windows. Это расширенная и адаптированная под Windows реализация стандарта WBEM, принятого многими компаниями, в основе которого лежит идея создания универсального интерфейса мониторинга и управления различными системами и компонентами распределённой информационной среды предприятия с использованием объектно-ориентированных идеологий и протоколов HTML и XML. В основе структуры данных в WBEM лежит Common Information Model (CIM), реализующая ООП-подход к представлению компонентов системы. CIM является расширяемой моделью, что позволяет программам, системам и драйверам добавлять в неё свои классы, объекты, методы и свойства. WMI, основанный на CIM, также является открытой унифицированной системой интерфейсов доступа к любым параметрам операционной системы, устройствам и приложениям.

Из бота

Инструментарий управления Windows (Windows Management Instrumentation, **WMI**) представляет собой набор инструментов и служб в операционных системах Microsoft Windows, предназначенных для управления и мониторинга компьютерных систем. WMI предоставляет стандартный интерфейс для взаимодействия с системными ресурсами и компонентами, а также для сбора информации о системе и её конфигурации.

Основные черты и функциональность WMI включают:

1. **Стандартизированный интерфейс:** WMI предоставляет стандартный интерфейс для управления компьютером и его компонентами. Это позволяет разработчикам и администраторам использовать унифицированный подход к управлению ресурсами.
2. **Управление конфигурацией и ресурсами:** WMI позволяет получать информацию о конфигурации компьютера, устанавливать параметры и управлять различными системными ресурсами, такими как процессор, память, жесткий диск, сетевые настройки и многое другое.
3. **Мониторинг и события:** WMI предоставляет механизм для мониторинга событий и изменений в системе. Это может быть использовано для отслеживания производительности, слежения за состоянием служб и других системных событий.
4. **Управление службами и программами:** С помощью WMI можно управлять службами Windows, устанавливать параметры их запуска, останавливать и запускать службы, а также управлять установленным программным обеспечением.

**Event Tracing for Windows (ETW)** — это служба, которая позволяет получать события от одного или нескольких поставщиков событий в режиме реального времени или из файла \*.etl за некоторый временной период (механизм трассировки и регистрации событий, которые генерируются приложениями в пользовательском режиме и драйверами в ядре)

Архитектура ETW включает в себя 4 элемента (рис. 4.2.1):

• поставщики событий (providers)

• потребители событий (consumers)

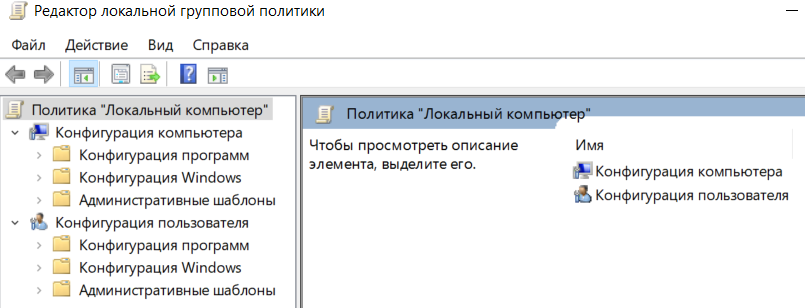
• контроллеры ETW (controllers)

• сессии ETW (event tracing sessions)

Проще говоря, ETW позволяет операционной системе и приложениям фиксировать различные события, происходящие внутри компьютера, чтобы администраторы или разработчики могли анализировать эти события для улучшения производительности, отладки или мониторинга

**Групповая политика** — важный элемент любой среды Microsoft Active Directory (AD). Её основная **цель** — дать ИТ-администраторам возможность централизованно управлять пользователями и компьютерами в домене.

//Active Directory - это сервис, который управляет информацией о пользователях, компьютерах и других ресурсах в сети. Active Directory обеспечивает централизованное управление ресурсами и безопасностью в корпоративной сети, упрощая администрирование и обеспечивая более удобный опыт использования сетевых ресурсов для конечных пользователей.



Групповая политика **состоит из** набора политик, называемых **объектами групповой политики (GPO)**.

При создании домена AD автоматически создаются два объекта групповой политики:

• **политика домена** по умолчанию устанавливает базовые параметры для всех пользователей и компьютеров в домене в трех плоскостях: политика паролей, политика блокировки учетных записей и политика Kerberos; (все пользователи и компьютеры в домене будут следовать этим параметрам если не указано иное )

• **политика контроллеров домена** по умолчанию устанавливает базовые параметры безопасности и аудита для всех контроллеров домена в рамках домена.

Объект групповой политики не действует, пока не будет связан с контейнером Active Directory, например, сайтом, доменом или подразделением.(МЫ ДОЛЖНЫ СВЯЗАТЬ С КОНТЕЙНЕРОМ ЧТОБЫ ПОЛИТИКА РАБОТАЛА) (что все контроллеры домена будут следовать этим параметрам безопасности и аудита)

**Административные** шаблоны (файлы) в формате XML, написанные на различных языках, которые задают параметры групповых политик, основанные на значениях реестра. Административные шаблоны позволяют администраторам устанавливать и изменять настройки безопасности, поведения и другие параметры на компьютере или сети через групповые политики.

**Два вида административных шаблонов:**

* **ADMX** — не зависящий от языка файл установки, который указывает количество и тип параметров политики, расположение по категориям согласно отображению файла в редакторе локальных групповых политик.(не зависят от языка \содержат все настройки которые вы можете опрпделить \определяют количество и тип политик)
* **ADML** — файл установки на определенном языке, который предоставляет

связанные с языком сведения для ADMX-файла. позволяет параметру политики отображаться в редакторе локальных групповых политик на нужном языке. Вы можете добавлять новые языки, добавляя новые ADML-файлы на нужных языках.(содержит сведения для ADMX файла \позволяют параметру политики локальных грцпповых политик отображаться в редакторе на нужном языке )  
Таким образом, основное различие между ADMX и ADML заключается в том, что ADMX определяет, какие политики доступны для настройки, а ADML определяет, как эти политики отображаются и описываются на разных языках

# Тема 4.3. UNIX-подобные и другие POSIX-совместимые операционные системы

# 27. Основные понятия системы UNIX. Пользователи системы, атрибуты пользователя. Файловая структура ОС.

Операционная система UNIX всегда была интерактивной системой, разработанной для одновременной поддержки множества процессов и множества пользователей. Она была разработана программистами и для программистов. От системы требовалось быть простой, элегантной и совместимой. В системе должно быть небольшое количество базовых элементов, которые можно комбинировать, чтобы приспособить их для конкретного приложения. **Другие характерные особенности**: использование простых текстовых файлов для настройки и управления системой; широкое применение утилит, запускаемых из командной строки; взаимодействие с пользователем посредством виртуального устройства — терминала; представление физических и виртуальных устройств и некоторых средств межпроцессного взаимодействия в виде файлов; использование конвейеров из нескольких программ, каждая из которых выполняет одну задачу.

**обобщил философию следующим образом: «Философия UNIX гласит:** пишите программы, которые делают что-то одно и делают это хорошо; пишите программы, которые бы работали вместе; пишите программы, которые бы поддерживали текстовые потоки, поскольку это универсальный интерфейс».

девять основных принципов:

1. Простые решения красивы (Small is Beautiful).

2. Пусть каждая программа делает что-то одно, но хорошо.

3. Стройте прототип программы как можно раньше.

4. Предпочитайте переносимость эффективности.

5. Храните данные в простых текстовых файлах.

6. Извлекайте пользу из уже существующих программных решений.

7. Используйте скриптовые языки для уменьшения трудозатрат и улучшения переносимости.

8. Избегайте пользовательских интерфейсов, ограничивающих возможности пользователя по взаимодействию с системой.

9. Делайте каждую программу «фильтром».

**Комитет POSIX разработал стандарт 1003.1**, который определяет набор библиотечных процедур, которые должна обеспечивать каждая соответствующая данному стандарту система UNIX. Большая часть этих процедур делает системный вызов, но некоторые из них могут быть реализованы вне ядра. **Идея стандарта POSIX** заключается в том, что производитель программного обеспечения, который при написании программы использует только описанные в стандарте 1003.1 процедуры, может быть уверен, что его программа будет работать на любой системе UNIX, соответствующей данному стандарту. Также был принят ряд сопутствующих документов, которые стандартизируют потоки, утилиты, сетевое программное обеспечение и многие другие функции системы UNIX. Кроме того, язык C также был стандартизирован Национальным институтом стандартизации //США (ANSI) и Международной организацией по стандартизации ISO.

**Unix** - это семейство операционных систем (ОС), обладающих сходной архитектурой и интерфесом с пользователем. Unix как явление зародилось в начале 70-х годов и развивается до сих пор. **Основные современные варианты UNIX:** Linux, BSD (FreeBSD, NetBSD, OpenBSD), AIX, HPUX, Solaris, SCO.

Важнейшие стандарты, обеспечивающие целостность семейства UNIX: POSIX - Portable Operating System Interface, ANSI C (c89 и с99).

**Классическая архитектура UNIX двухуровневая**: **Пользовательское пространство (User space ) и ядро** - управляет ресурсами компьютера и предлагает программам базовый набор услуг (системные вызовы), **системные программы** (управление сетью, терминалами, печатью), прикладные программы (редакторы, утилиты, компиляторы и т.д.).

Операционная система UNIX обладает классическим монолитным ядром, в котором можно выделить следующие основные части: файловая подсистема, управление процессами и драйверы устройств. 

**Существует два основных объекта операционной системы** UNIX, с которыми приходится работать пользователю – **файлы и процессы**. Эти объекты сильно связаны друг с другом, и в целом организация работы с ними как раз и определяет архитектуру операционной системы.

Все данные пользователя хранятся в файлах; доступ к периферийным устройствам осуществляется посредством чтения и записи специальных файлов; во время выполнения программы, операционная система считывает исполняемый код из файла в память и передает ему управление. С другой стороны, вся функциональность операционная определяется выполнением соответствующих процессов. В частности, обращение к файлам на диске невозможно, если файловая подсистема операционной системы (совокупность процессов, осуществляющих доступ к файлам) не имеет необходимого для этого кода в памяти.

В операционной системе содержится большое количество стандартных программ, некоторые из них указаны в стандарте POSIX 1003.2, тогда как другие могут различаться от версии к версии. К этим программам относятся командный процессор (оболочка), компиляторы, редакторы, программы обработки текста и утилиты для работы с файлами. Именно эти программы и запускает пользователь с клавиатуры. Графические интерфейсы пользователя поддерживает оконная система X Windowing System, которую обычно называют Х11 (или просто Х). Она определяет обмен и протоколы отображения для управления окнами на растровых дисплеях UNIX-подобных систем.

Пользователи системы, атрибуты пользователя

Прежде чем клиент сможет начать работу с ОС UNIX, он должен стать пользователем системы, т.е. получить имя, пароль и ряд других атрибутов. С точки зрения системы пользователь не обязательно человек.

**Пользователем** является объект, который обладает определенными правами и может запускать на выполнение программы и владеть файлами. Пользователями могут быть отдельные клиенты, удаленные компьютеры или группы пользователей с одинаковыми правами и функциями.

**В системе существует один пользователь, обладающий неограниченными правами это суперпользователь или администратор системы** (обычно с именем root).

Каждый пользователь имеет уникальное или регистрационное имя, но система различает пользователей по идентификатору пользователя UID. Идентификаторы также должны быть уникальны. Пользователи являются членами одной или нескольких групп. Информация о пользователях обычно хранится в специальном файле: /etc/passwd. Этот файл доступен только для чтения. Писать в него может только администратор.

**Группа** — список пользователей, имеющих сходные задачи. Принадлежность к группе определяется дополнительными правами, которыми обладают все пользователи группы. Каждая группа имеет уникальное имя, а система различает группы по групповому идентификатору (GID). Информация о группах хранится в специальном файле: /etc/group.

Атрибуты пользователя

Как правило, все **атрибуты** пользователя хранятся в файле /etc/passwd.

Каждая строка файла является записью конкретного пользователя и имеет следующий формат:

name:passwd-encod:UID:GID:comments:home-dir:shell

— всего семь полей (атрибутов), разделенных двоеточиями.

**name** - регистрационное имя пользователя.

**passwd-encod** - пароль пользователя в закодированном виде. Пароль часто хранят в отдельном файле, а в поле passwd-encod ставится символ х.

**UID** - числовой идентификатор пользователя, является внутренним представлением пользователя в системе**.**

**GID** - определяет идентификатор первичной группы пользователя.

**comments** - обычно это полное "реальное" имя пользователя.

**home-dir** - домашний каталог пользователя.

**shell** - имя программы, которую UNIX использует в качестве командного интерпретатора.

**Файловая структура ОС**

**Файловая структура ОС.** почему-то в данном разделе рассматривается всё на примере LINUX

Файл в системе Linux — это последовательность байтов произвольной длины (от 0 до

некоторого максимума), содержащая произвольную информацию. Не делается различия

между текстовыми (ASCII) файлами, двоичными файлами и любыми другими типами

файлов. Значение битов в файле целиком определяется владельцем файла. Системе это

безразлично. Имена файлов ограничены 255 символами. Всё зависит от системы.   
**1ой была система MINIX1** имена файлов были ограничены в ней 14 символами максимальный размер файла составлял 64 Мбайт  
**2ой была ext,** которая позволяла использовать имена файлов длиной 255 символов и размер файлов 2 Гбайт (однако она была медленнее, чем файловая система MINIX 1)

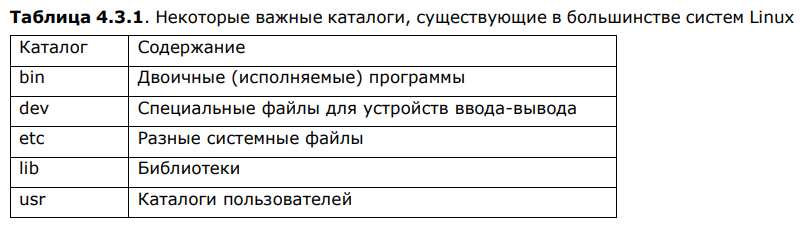
**3ей была ext2** (с длинными именами файлов, большими файлами и более высокой производительностью),  которая и стала основной файловой системой.  
но линукс поддерживает большое множество файловых систем.

По соглашению многие программы ожидают, что имена файлов будут состоять из

основного имени и расширения, разделенных точкой (которая также считается

символом). Так, prog.c — это обычно программа на языке C

Система содержит каталоги, подкаталоги и фалы в них. Символ / разделяет их в пути



Существует два способа задания имени файла в системе Linux (как в оболочке, так и при открытии файла из программы). Первый способ заключается в использовании **абсолютного** пути (absolute path), указывающего, как найти файл от корневого каталога. Также имена путей могут указываться относительно рабочего каталога. Путь, заданный относительно рабочего каталога, называется **относительным** путем (relative path).

//мб с этого начать

Файлы ядра можно обнаружить в каталоге /boot. В заархивированном виде ядро системы Линукс располагается в vmlinuz, где z - символ, прямо указывающий на то, ядро сжато до минимального размера с целью экономии свободного пространства **Файл initrd.img – это первичная файловая система**, монтирующая в первую очередь, прежде чем будет осуществлено подключение реальных физических накопители к виртуальной файловой системе VFS. В этом же месте можно обнаружить все другие дополняющие модули ядра, следовательно, данный файл в плане размерности может быть ощутимо больше самого ядра Линукс.

**В файле system.map** не составит труда обнаружить различные функций. Программы устанавливаются в различные директории в файловой системе. Одна из наиболее распространенных директорий для установки программ — это **/usr/bin.** Здесь обычно размещаются исполняемые файлы программ, доступные для всех пользователей системы. Эта директория имеет преимущество перед другими в пути поиска исполняемых файлов, что позволяет пользователю запускать программы из любой директории.

Другая важная директория для установки программ — это **/opt.** Она служит для установки приложений, которые не являются частью основной операционной системы. Здесь можно разместить программы, которые вы загрузили из Интернета или с которыми не связаны зависимости от других программ. Установка программ в эту директорию обеспечивает лучшую изоляцию и восстановление системы после обновления или удаления программ.

Наконец, важно упомянуть о **/usr/local** — директории, в которой обычно размещаются локально установленные программы. Здесь могут находиться программы, установленные самим пользователем или администратором системы и которые не входят в стандартный пакет установки Linux. Размещение программ в этой директории позволяет отделить их от программ, поставляемых с операционной системой, и облегчает их управление и обновление.

# 28. ОС UNIX: особенности процессов, сигналы, обработка сигналов.

**Основными активными сущностями в системе Linux являются процессы.** Каждый процесс выполняет одну программу и изначально получает один поток управления. Иначе говоря, у процесса есть один счетчик команд, который отслеживает следующую исполняемую команду.

Linux позволяет процессу создавать дополнительные потоки (после того, как он начинает выполнение). Несколько независимых процессов могут работать одновременно. Более того, у каждого пользователя может быть одновременно несколько активных процессов, так что в большой системе могут одновременно работать сотни и даже тысячи процессов.

Фактически на большинстве однопользовательских рабочих станций работают десятки **фоновых процессов, называемых демонами (daemons).** Они запускаются при загрузке системы из сценария оболочки.

Процессы создаются в операционной системе Linux с помощью системного **вызова fork,** который создает точную копию исходного процесса, называемого **родительским процессом (parent process).** Новый процесс **называется дочерним процессом (child process**). У родительского и у дочернего процессов есть собственные (приватные) образы памяти. Открытые файлы используются родительским и дочерним процессами совместно.

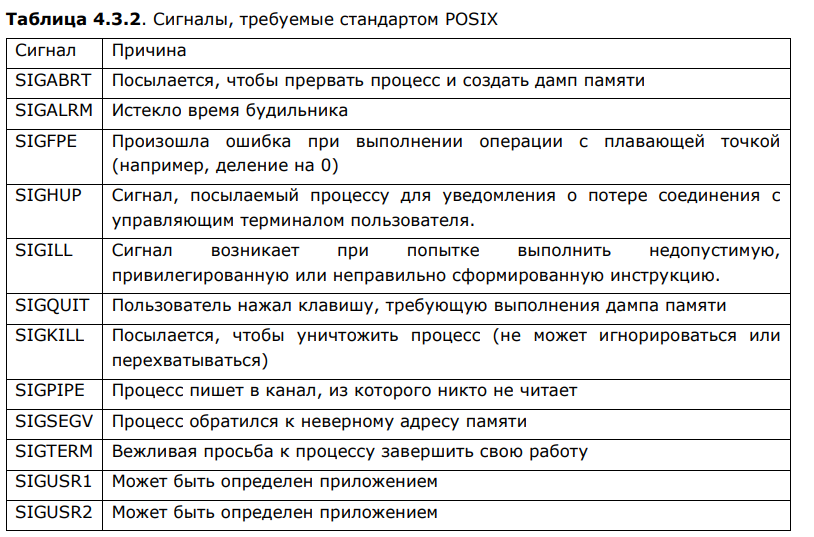
Процессы именуются своими PID-идентификаторами. При создании процесса его PID выдается родителю нового процесса. Если дочерний процесс желает узнать свой PID, то он может воспользоваться системным вызовом **getpid.**

**Типы процессов**

* **Системные процессы** являются частью ядра и всегда расположены в оперативной памяти.
* **Демоны** — это неинтерактивные процессы, которые запускаются обычным образом — путем загрузки в память соответствующих им программ (исполняемых файлов), и выполняются в фоновом режиме.
* К **прикладным процессам** относятся все остальные процессы, выполняющиеся в системе. Как правило, это процессы, порожденные в рамках пользовательского сеанса работы.

**Сигналы** — это способ информирования процесса со стороны ядра о происшествии некоторого события. По сути, сигналы являются программными прерываниями. Смысл термина «сигнал» состоит в том, что сколько бы однотипных событий в системе не произошло, по поводу каждой такой группы событий процессу будет подан ровно один сигнал. То есть, сигнал означает, что определяемое им событие произошло, но не несет информации о том, сколько именно произошло однотипных событий.

Сигналы могут инициироваться одними процессами по отношению к другим процессам с помощью специального системного вызова kill. Процессы могут сообщить системе, какие действия следует предпринимать, когда придет входящий сигнал.



обработка сигналов.

**Варианты такие**: проигнорировать сигнал, перехватить его, позволить сигналу убить процесс (действие по умолчанию для большинства сигналов).

Если процесс выбрал перехват посылаемых ему сигналов, он должен указать процедуру обработки сигналов. Когда сигнал прибывает, управление сразу же передается обработчику. Когда процедура обработки сигнала завершает свою работу, управление снова передается в то место, в котором оно находилось, когда пришел сигнал (это аналогично обработке аппаратных прерываний ввода-вывода).

**Обработка сигналов** в Linux осуществляется через установку обработчиков сигналов. Когда процесс получает сигнал, ядро отправляет управление к обработчику, который был предварительно установлен для этого сигнала. Процесс может выбрать различные действия при получении сигнала:

**Игнорирование (SIG\_IGN):** Процесс может проигнорировать сигнал, если установлен обработчик SIG\_IGN (ignore).

**По умолчанию (SIG\_DFL)**: Если не установлен пользовательский обработчик, применяется действие по умолчанию (default). Например завершение процесса.

**Пользовательский обработчик (функция):** Процесс может установить свою собственную функцию-обработчик. Когда сигнал поступает, управление передается этой функции.

//Не надо

В системе Linux процессы могут общаться друг с другом с помощью некой формы передачи сообщений. Можно создать **канал** между двумя процессами, в который один процесс сможет писать поток байтов, а другой процесс сможет его читать. Синхронизация процессов достигается путем блокирования процесса при попытке прочитать данные из пустого канала. Когда данные появляются в канале, процесс разблокируется. При помощи каналов организуются конвейеры оболочки. **Неименованный канал** (или программный канал) представляется в виде области памяти на внешнем запоминающем устройстве, управляемой операционной системой, которая осуществляет выделение взаимодействующим процессам частей из этой области памяти для совместной работы, т.е. это область памяти является разделяемым ресурсом.

Файловая система ОС Unix поддерживает специальные файлы, которые называются FIFO-файлами (или **именованными каналами**). Файлы этого типа очень схожи с обыкновенными файлами (в них можно писать и из них можно читать информацию), за исключением того факта, что они организованы по стратегии FIFO (т.е. невозможны операции, связанные с перемещением файлового указателя). Таким образом, файлы FIFO могут использоваться для организации взаимодействия процессов, при этом в отличие от неименованных каналов эти файлы могут существовать независимо от процессов, взаимодействующих через них. Эти файлы хранятся на внешних запоминающих устройствах, поэтому возможно открыть этот файл, записать в него информацию, а через любой промежуток времени (в течение которого допустимы перезагрузки системы) прочитать записанную информацию.

# Тема 4.4. Операционная система ОС Linux

# 29. Основные принципы функционирования Linux. Основные компоненты Linux. Дистрибутивы Linux. Файловая система Linux.

Все UNIX-совместимые системы организованы по принципу клиент-сервер. Все компьютеры в сети работают как один большой компьютер..

Каждый пользователь работает с системой через виртуальный терминал, которых может быть до 12-ти в зависимости от версии Linux (на экране обозначается как tty1..tty12**).**

**В ОС Linux все файлы организованы в непрерывный поток байтов**. Данные, вводимые с клавиатуры, представляют собой входной поток данных, а отображаемые данные – выходной поток. Поскольку процедуры ввода и вывода организованы также, как и файлы, то они могут свободно взаимодействовать с файлами. Чтобы передать данные из одной команды в другую, можно использовать конвейеры.

**Файл может быть каталогом или исполняемой программой (командой).** Команда file помогает определить, для чего используется данный файл (например, текстовый файл или каталог). Файловая система в ОС Linux как и в большинстве других систем имеет иерархическую (древовидную) структуру. Вверху дерева всегда находится корневой каталог ROOT. В этой операционной системе также справедливо понятие текущего каталога. Каждый файл имеет относительное имя пути, которое определяет его принадлежность к какому-либо каталогу, и абсолютное имя пути, которое показывает весь путь файла, начиная от корневого каталога.

**Название Linux в первую очередь относится к ядру операционной системы**. Вообще говоря, в операционных системах этого семейства можно выделить следующие компоненты: **ядро, модули, планировщик, файл подкачки, файловые системы, механизмы защиты, инструменты администрирования, серверные возможности, графический интерфейс пользователя, система управления пакетами** и т. д.

**В ядре** собрана основная функциональность для работы с памятью, управления процессами и т.д. Когда ядру требуется дополнительные функции, он обращается к модулям. В модулях, например, может содержаться код для работы с оборудованием. Файлы ядра Linux находятся в /boot.

Так как ядро Linux обеспечивает одновременную работу нескольких процессов от нескольких пользователей (с поддержкой нескольких процессоров), операционная система нуждается в средствах управления многопоточностью**. Планировщик Linux** назначает процессам приоритеты и определяет, какой процесс выполняется на конкретном процессоре (если в системе установлено несколько процессоров). Планировщик можно настроить для работы в системах различного типа. При правильной настройке более важные процессы получают более быструю реакцию процессора. Например, планировщик Linux на настольном компьютере предоставляет больший приоритет задаче перемещения окна и меньший — задаче фонового копирования файлов.

Ядро Linux старается держать работающие в данный момент процессы в оперативной памяти. Простаивающие процессы перемещаются **в файл подкачки**, представляющий собой выделенную область на жестком диске, которая используется для хранения не перемещающихся в оперативную память данных и процессов. При переполнении оперативной памяти процессы выносятся в файл подкачки. При переполнении файла подкачки (но этого допускать нельзя) новые процессы не запускаются.

Ядро Linux поддерживает тысячи аппаратных устройств. При этом за счет включения в работающее ядро только актуальных драйверов размер ядра удается сохранять на приемлемом уровне. Использование загружаемых модулей позволяет добавить в ядро поддержку дополнительных устройств**. Модули** можно загружать и выгружать по запросу в результате подключения или отключения устройства.

**Файловые системы/ Механизмы защиты.** Как и UNIX, операционная система Linux изначально создавалась для обеспечения, одновременного многопользовательского доступа. Для защиты пользовательских ресурсов каждому файлу назначаются наборы разрешений на чтение, запись и выполнение, которые определяют права доступа.

В стандартной системе Linux пользователь root имеет доступ ко всей системе без ограничений, специальные регистрационные записи могут управлять определенными службами (например, службами Web-сервера Apache), а пользователям могут присваиваться разрешения по отдельности или в составе групп. Последние нововведения, например, Security-Enhanced Linux (SELinux), поддерживают более тонкую настройку и защиту безопасных сред обработки информации.

**Инструменты администрировани**я включают в себя сотни (а возможно и тысячи) команд и графических утилит, которые позволяют добавлять пользователей, управлять дисками, следить за состоянием сети, устанавливать программное обеспечение, а также гарантировать безопасность и управлять ресурсами компьютера.

**Серверные возможности** позволяют компьютеру под управлением Linux предоставлять службы для клиентов в сети. Иными словами, кроме установки Web-обозревателей для просмотра Web-страниц, компьютер можно превратить в сервер, который предоставляет Web-страницы другим компьютерам. При этом среди популярных серверных функций можно назвать Web-серверы, серверы электронной почты, баз данных, печати, файловые серверы, серверы DNS и DHCP.

**Графический интерфейс** пользователя состоит из графической инфраструктуры (обычно это X WindowSystem), оконных менеджеров, панелей, пиктограмм и меню. Графический интерфейс пользователя позволяет применять комбинацию мыши и клавиатуры вместо простого ввода команд с клавиатуры.

**Дистрибутивы** состоят из отдельных пакетов, каждый из которых содержит какое-то приложение, утилиту или сервис. Отдельный пакет может содержать, например, веб-браузер, библиотеку для работы с графическими файлами в формате PNG, набор шрифтов и так далее. Программное обеспечение, содержащееся в пакете, поставляется в одном из двух основных видов: в виде бинарных файлов, которые предназначены для непосредственной установки в вашу систему, без какой-либо дополнительной обработки (например, компиляции); в виде исходных текстов, которые обычно содержат текст на каком-то языке программирования, заархивированный в формате tar и упакованный программой gzip, а также вспомогательные файлы, необходимые для компиляции приложения из файлов пакета.

Мы можем распределить дистрибутивы Linux на три группы:

• Enterprise Grade Linux Distributions

* Red Hat Enterprise Linux
* CentOS
* SUSE Linux Enterprise Server
* Debian GNU/Linux
* Ubuntu LTS

• Consumer Grade Linux Distributions

* Fedora
* Ubuntu non-LTS
* openSUSE

• Experimental and Hacker Linux Distributions

* Arch
* Gentoo

**Дистрибутивы Enterprise Grade Linux** предназначены для развертывания в крупных организациях с использованием оборудования предприятия. Они обычно включают более старые выпуски ядра и другое программное обеспечение, которое, как известно, работает надежно. Часто дистрибутивы портируют важные обновления, такие как исправления безопасности, на эти стабильные версии**.**

**Дистрибутивы Consumer Grade Linux** больше ориентированы на малый бизнес или домашних пользователей и любителей. Они подготовлены для использования новейшего оборудования, установленного в системах потребительского уровня. Этим системам потребуются новейшие драйверы, чтобы максимально использовать новое оборудование.

**Дистрибутивы Experimental and Hacker Linux** используют самые современные технологии. Они содержат самые последние версии программного обеспечения, даже если эти версии все еще содержат ошибки и непроверенные **функции.**

**Файловая система Linux**

В операционной системе GNU/Linux все объекты являются файлами, в том числе и директории, которые служат для организации доступа к файлам.

Существуют следующие **типы файлов**: обычные файлы, каталоги, символьные ссылки, блочные устройства, символьные устройства, сокеты, каналы. (подробнее в 33 вопросе)

В любой файловой системе Linux всегда есть только один корневой каталог, который называется /. Пользователь Linux всегда работает с единым деревом каталогов, даже если данные расположены на разных носителях: жёстких или съёмных дисках, CD-ROM, сетевых дисках и т. д.

Положение любого каталога в дереве каталогов точно и однозначно описывается при помощи полного пути. **Полный путь** всегда начинается от корневого каталога и состоит из перечисления всех вершин, встретившихся при движении по рёбрам дерева до искомого каталога включительно. Названия соседних вершин разделяются символом наклонной черты / (слэш). Для каждого процесса Linux определена текущая директория, с которого система начинает **относительный путь** при выполнении файловых операций. Между полным путём и относительным есть только одно существенное различие: относительный путь начинается от текущей директории, в то время как полный путь всегда начинается от корневой директории. То есть, первый символ полного пути всегда будет /. Точка . в начале имени файла делает его скрытым, то есть, он не показывается в выводе команды ls.

**Домашний каталог** (домашняя папка, домашняя директория) – предназначен для хранения собственных данных пользователя Linux и личных настроек для программ. Как правило, становится текущим непосредственно после регистрации пользователя в системе. Полный путь к домашнему каталогу хранится в переменной окружения HOME, в полном пути к файлу можно заменять на знак тильды ~. Для обычных пользователей домашний каталог находится в директории /home.

**FHS (Filesystem Hierarchy Standard)** – стандарт файловой системы, специфичной для GNU/Linux, создан в 1994-1996 гг. Текущая версия стандарта FHS 3.0 выпущена 03.06.2015 г. Некоторые Linux-системы отвергают FHS и следуют своему собственному стандарту.В FHS все файлы и каталоги находятся внутри корневого каталога, даже если они расположены на различных физических носителях. В корневой директории должны быть следующие директории: bin, boot, dev, etc, lib, media, mnt, opt, run, sbin, srv, tmp, usr, var. При наличии соответствующих подсистем добавляются папки home, root и lib64.

# 30. ОС Linux: управление процессами, выполнение задач в фоновом режиме, изменение приоритетов выполняющихся программ.

Процессы существуют в иерархии: после загрузки ядра в память запускается первый процесс (init или systemd), который, в свою очередь, запускает другие процессы, которые, опять же, могут запускать другие процессы. Каждый раз, когда пользователь вводит команду, запускается программа и генерируется один или несколько процессов. **Каждый процесс имеет уникальный идентификатор (PID) и идентификатор родительского процесса (PPID)**. Это положительные целые числа, которые назначаются в последовательном порядке.

**Команда top** динамически отображает все запущенные процессы

Альтернативные команды – htop и atop. **Команда ps** выводит статическую информацию о процессах. Без опций выводит только процессы, относящиеся к текущей оболочке. Команда поддерживает три стиля параметров, причем они не совпадают. Например, ps aux не эквивалентна ps –aux, но ps -e эквивалентна ps ax. Иерархию процессов можно увидеть с **помощью команды pstree**. Завершить процесс можно с помощью **команды kill.**

**Для выполнения команды в фоновом режиме достаточно добавить в конце символ амперсанда &.** В выводе терминала будут отображены порядковый номер задачи (в квадратных скобках) и идентификатор процесса. Работая в фоновом режиме, команда все равно продолжает выводить сообщения в терминал, из которого была запущена. Для этого она использует потоки stdout и stderr, которые можно закрыть при помощи следующего синтаксиса: $ command > /dev/null 2>&1 &

Узнать состояние всех остановленных и выполняемых в фоновом режиме задач в рамках текущей сессии терминала можно при помощи **утилиты jobs** c использованием опции -l. Вывод содержит порядковый номер задачи, идентификатор фонового процесса, состояние задачи и название команды, которая запустила задание. В любое время можно вернуть процесс из фонового режима на передний план. Для этого **служит команда fg.** Если в фоновом режиме выполняется несколько программ, следует также указывать номер.

Для завершения фонового процесса применяют команду kill с номером программы. Если изначально процесс был запущен обычным способом, его можно перевести в фоновый режим, выполнив следующие действия:

• Остановить выполнение команды, нажав комбинацию клавиш Ctrl+Z.

• Перевести процесс в фоновый режим при помощи команды bg.

**Утилита nice** — программа, предназначенная для запуска процессов с изменённым приоритетом nice. Приоритет nice (целое число) процесса используется планировщиком процессов ядра ОС при распределении процессорного времени между процессами. **Приоритет nice** — число, указывающее планировщику процессов ядра ОС приоритет, который пользователь хотел бы назначить процессу.

Утилита nice, запущенная без аргументов, выводит приоритет nice, унаследованный от родительского процесса. nice принимает аргумент «смещение» в диапазоне от -20 (наивысший приоритет) до +19 (низший приоритет). Если указать смещение и путь к исполняемому файлу, утилита nice получит приоритет своего процесса, изменит его на указанное смещение и использует системный вызов семейства exec() для замещения кода своего процесса кодом из указанного исполняемого файла. Команда nice сделает то же, но сначала выполнит системный вызов семейства fork() для запуска дочернего процесса (sub-shell). Если смещение не указано, будет использовано смещение +10. Привилегированный пользователь (root) может указать отрицательное смещение.

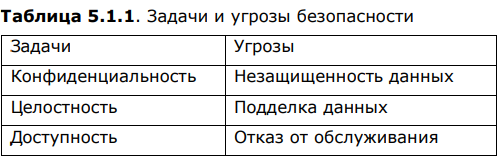
Для того, чтобы изменить приоритет у существующего процесса (т.е. такого процесса, который ранее был уже запущен), необходимо воспользоваться **командой renice** [значение приоритета] -p [id процесса]. У запущенной программы с помощью команды renice можно изменить назначенный приоритет. Согласно правилам, обычный пользователь может только увеличивать значение nice (уменьшать приоритет) любого процесса.

# Тема 5.1. Безопасность и контроль доступа

# 31. Понятие безопасности ОС. Основные угрозы безопасности ОС. Методы и защитные механизмы операционных систем.

Классификация угроз. Zero trust. Авторизация и аутентификация пользователей. Криптографическая защита данных. Права доступа

**Безопасность** в контексте операционных систем охватывает механизмы и стратегии, направленные на защиту информации и обеспечение нормальной работы системы.



Во многих работах, посвященных безопасности, безопасность информационных систем разбита на три компонента: конфиденциальность, целостность и доступность. Вместе все три компонента часто называют CIA (Confidentiality, Integrity, Availability).

Первое свойство — **конфиденциальность** (confidentiality) — направлено на сохранение секретности данных

Второе свойство — **целостность** (integrity) — означает, что пользователи, не обладающие необходимыми правами, не должны иметь возможности изменять какие-либо данные без разрешения их владельцев.

Третье свойство — **доступность** (availability) — означает, что никто не может нарушить работу системы и вывести ее из строя

Позже было решено, что трех основных свойств для всех возможных сценариев недостаточно, и были добавлены дополнительные свойства, такие как **аутентичность** (authenticity), **идентифицируемость** (accountability), **неотвергаемость** (nonrepudiability)- после совершила какое-либо действие, она не может отказаться от своей ответственности или утверждать, что этого не произошло, **закрытость** (privacy) и др

Классификация угроз **по цели** атаки:

• несанкционированное чтение информации;

• изменение информации;

• уничтожение информации;

• полное или частичное разрушение операционной системы.

Классификация угроз **по принципу воздействия** на операционную систему:

• использование известных (легальных) каналов получения информации

• использование скрытых каналов получения информации

• создание новых каналов получения информации с помощью программных закладок.

**Классификация угроз по типу используемой злоумышленником уязвимости защиты**

* Неадекватная политика безопасности, в том числе и ошибки администратора системы;
* ошибки и недокументированные возможности программного обеспечения операционной системы, в том числе и так называемые люки – случайно или преднамеренно встроенные в систему «служебные входы», позволяющие обходить систему защиты;
* ранее внедренная программная закладка.

Классификация угроз **по характеру** воздействия на ОС:

• активное воздействие – несанкционированные действия злоумышленника в системе;

• пассивное воздействие – несанкционированное наблюдение злоумышленника за процессами, происходящими в системе

Угрозы безопасности ОС можно также классифицировать по таким признакам, как способ действий злоумышленника, используемые средства атаки, объект атаки, способ воздействия на объект атаки, состояние атакуемого объекта ОС на момент атаки.

Операционная система **может подвергнуться следующим типичным атакам**:

• *сканирование файловой системы.* Злоумышленник просматривает файловую систему компьютера и пытается прочесть (или скопировать) все файлы подряд.

• *подбор пароля.* несколько методов подбора паролей:

* тотальный перебор;
* тотальный перебор, оптимизированный по статистике встречаемости символов или с помощью словарей;
* подбор пароля с использованием знаний о пользователе (его имени, фамилии, даты рождения, номера телефона и т. д.);

• *кража ключевой информации*. Носитель с ключевой информацией (смарткарта, Touch Memory и т. д.) может быть просто украден;

• *сборка мусора*. Во многих операционных системах удаленная пользователем информация не физически уничтожается, а лишь помечается как удаленная, что предоставляет возможность злоумышленникам восстановить и просмотреть данные.

• *превышение полномочий*. Злоумышленник, используя ошибки в программном обеспечении ОС получает полномочия, превышающие те, которые ему предоставлены в соответствии с политикой безопасности.

• *программные закладки.*

• *жадные программы* – это программы, преднамеренно захватывающие значительную часть ресурсов компьютера, в результате чего другие программы не могут выполняться или выполняются крайне медленно. Запуск жадной программы может привести к краху операционной системы.

**Операционную систему называют защищенной, если она предусматривает средства защиты от основных классов угроз.** Защищенная операционная система обязательно должна содержать средства разграничения доступа пользователей к своим ресурсам, а также средства проверки подлинности пользователя, начинающего работу с операционной системой.

Существуют ***два основных подхода*** *к созданию защищенных операционных систем*: **фрагментарный**, где защитные функции добавляются отдельно после создания основной системы, и **комплексный**, где защитные функции внедряются в архитектуру системы на этапе проектирования, обеспечивая их тесное взаимодействие и интеграцию.

**При применении фрагментарного** подхода подсистема защиты операционной системы представляет собой набор разрозненных программных продуктов, как правило, от разных производителей. Эти программные средства работают независимо друг от друга, при этом практически невозможно организовать их тесное взаимодействие. Кроме того, отдельные элементы такой подсистемы защиты могут некорректно работать в присутствии друг друга, что приводит к резкому снижению надежности системы.

Основные административные меры защит.

• Постоянный контроль корректности функционирования ОС, особенно ее подсистемы защиты

• Организация и поддержание адекватной политики безопасности.

•Осведомление пользователей о необходимости соблюдения мер безопасности при работе с ОС и контроль за соблюдением этих мер.

• Регулярное создание и обновление резервных копий программ и данных ОС.

• Постоянный контроль изменений в конфигурационных данных и политике безопасности ОС.

**Архитектура подсистемы защиты операционной системы**

Подсистема защиты ОС выполняет следующие основные функции:

• *Идентификация и аутентификация*. Ни один пользователь не может начать работу с операционной системой, не идентифицировав себя и не предоставив системе аутентифицирующую информацию, подтверждающую, что пользователь действительно является тем, кем он себя заявляет.

• *Разграничение доступа.* Каждый пользователь системы имеет доступ только к тем объектам ОС, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности.

• *Аудит.* Операционная система регистрирует в специальном журнале события, потенциально опасные для поддержания безопасности системы.

*• Управление политикой безопасности*. Политика безопасности должна постоянно поддерживаться в адекватном состоянии, то есть должна гибко реагировать на изменения условий функционирования ОС.

• *Криптографические функции*. Защита информации немыслима без использования криптографических средств защиты. Шифрование используется в ОС при хранении и передаче по каналам связи паролей пользователей и некоторых других данных, критичных для безопасности системы.

*• Сетевые функции*. Современные ОС, как правило, работают не изолированно, а в составе локальных и/или глобальных компьютерных сетей. ОС компьютеров, входящих в одну сеть, взаимодействуют между собой для решения различных задач, в том числе имеющих прямое отношение к защите информации.

**Криптография** – это метод защиты информации путем использования закодированных алгоритмов, хэшей и подписей

# Тема 5.2. Механизмы безопасности в операционных системах семейства Windows

# 32. Механизмы безопасности в операционных системах семейства Windows.

Идентификаторы безопасности (SID). Маркеры защиты. Списки управления доступом (ACL). Доменные службы Active Directory. Виды групп пользователей.

**Идентификатор безопасности (SID)** — это уникальное значение переменной длины, используемое для идентификации доверенного лица.

Идентификатор безопасности используется для уникальной идентификации субъекта безопасности или группы безопасности. Субъекты безопасности могут представлять любую сущность, которая может быть проверена операционной системой, например учетной записью пользователя, учетной записью компьютера или потоком или процессом, выполняющимся в контексте безопасности учетной записи пользователя или компьютера. Каждая учетная запись или группа или каждый процесс, выполняемый в контексте безопасности учетной записи, имеет уникальный идентификатор безопасности, выданный центром, например контроллером домена Windows.

Идентификатор безопасности хранится в базе данных безопасности. Система создает идентификатор безопасности, определяющий определенную учетную запись или группу во время создания учетной записи или группы.

Если идентификатор безопасности используется в качестве уникального идентификатора для пользователя или группы, он никогда не может использоваться повторно для идентификации другого пользователя или группы.

**Маркер доступа** — это объект, описывающий контекст безопасности процесса или потока. При каждом входе пользователя система создает маркер доступа для этого пользователя. Маркер доступа содержит идентификатор безопасности пользователя, права пользователя и идентификаторы SID для всех групп, к которому принадлежит пользователь. Этот маркер предоставляет контекст безопасности для любых действий, выполняемых пользователем на этом компьютере.

Маркеры доступа содержат следующие сведения:

• Идентификатор безопасности (SID) для учетной записи пользователя

• Идентификаторы безопасности для групп, членом которых является пользователь

• Идентификатор безопасности входа, который идентифицирует текущий сеанс входа в систему.

• Список привилегий, которыми пользовались пользователи или группы пользователей.

• Идентификатор безопасности владельца

• Идентификатор безопасности для основной группы

• DACL по умолчанию, используемый системой, когда пользователь создает защищаемый объект без указания дескриптора безопасности.

• Источник маркера доступа

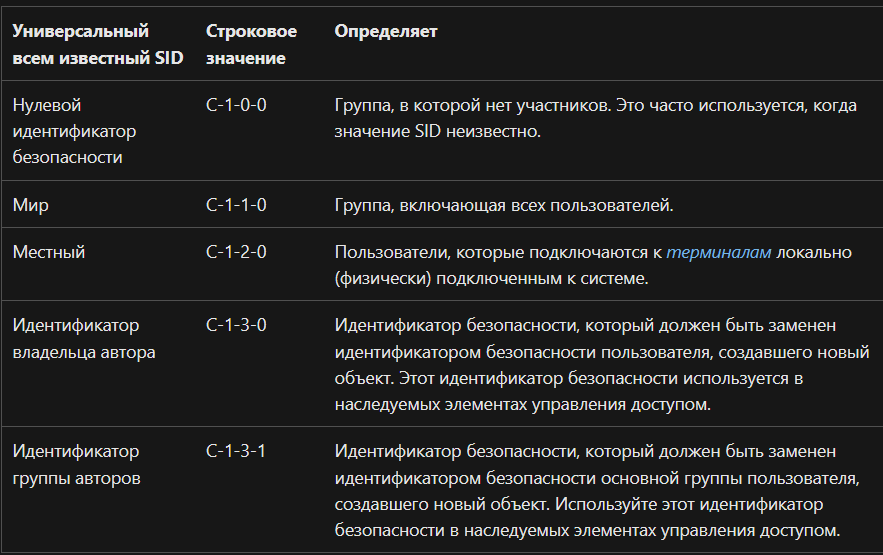
• Является ли маркер основным или маркером олицетворения

• Необязательный список ограничений идентификаторов безопасности

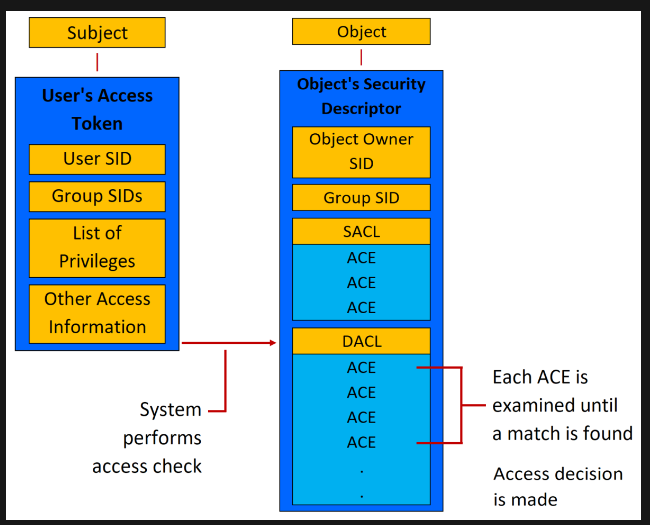
• Текущие уровни олицетворения

• Другая статистика.

Используйте функцию **OpenProcessToken**, чтобы получить дескриптор основного маркера процесса. Используйте функцию **OpenThreadToken** для получения дескриптора маркера олицетворения потока.



**Дескриптор безопасности** содержит сведения о безопасности, связанные с защищаемым объектом. Дескриптор безопасности состоит из структуры SECURITY\_DESCRIPTOR и связанных с ней сведений о безопасности.



Дескриптор безопасности может содержать следующие сведения о безопасности:

• Идентификаторы безопасности для владельца и основной группы объекта.

• DACL, указывающий права доступа, разрешенные или запрещенные определенным пользователям или группам.

• SACL, указывающий типы попыток доступа, которые создают записи аудита для объекта.

• Набор битов элементов управления, которые определяют значение дескриптора безопасности или его отдельных членов.

**Списки управления доступом (ACL)** состоят из записей управления доступом (ACE). Каждый ACE в ACL идентифицирует доверенного лица и указывает права доступа, разрешенные, запрещенные или регистрируемые для этого доверенного лица. Дескриптор безопасности для защищаемого объекта может содержать два типа списков управления доступом: **DACL и SACL**

**Список управления доступом на уровне пользователей (DACL)** определяет доверенных лиц, которым разрешен или запрещен доступ к защищаемому объекту. Когда процесс пытается получить доступ к защищаемому объекту, система проверяет ACE в DACL объекта, чтобы определить, следует ли предоставить доступ к нему. Если у объекта нет DACL, система предоставляет полный доступ всем пользователям. Если DACL объекта не имеет ACE, система отклоняет все попытки доступа к объекту, так как DACL не разрешает какие-либо права доступа. Система проверяет ACE в последовательности, пока не найдет один или несколько ACE, которые разрешают все запрошенные права доступа, или пока не будет отказано в любом из запрошенных прав доступа.

**Системный список управления доступом (SACL)** позволяет администраторам регистрировать попытки доступа к защищенному объекту. Каждый ACE указывает типы попыток доступа со стороны указанного доверенного лица, которые приводят к созданию системой записи в журнале событий безопасности. ACE в SACL может создавать записи аудита при сбое попытки доступа и/или при успешном выполнении.

**Каталог** — это иерархическая структура, в которой хранятся сведения об объектах в сети. Служба каталогов, например, службы домен Active Directory (AD DS), предоставляет методы хранения данных каталога и предоставления этих данных сетевым пользователям и администраторам.

**Логическая структура Active Directory** представляет собой иерархическую структуру доменов Active Directory и подразделений в лесу. Взаимосвязь компонентов логической структуры контролирует доступ к хранимым данным, а также то, как информация реплицируется между различными контроллерами домена в лесу

Active Directory также включает следующие компоненты:

• Схема — набор правил, который определяет классы объектов и атрибутов, содержащихся в каталоге, ограничения и ограничения экземпляров этих объектов, а также формат их имен.

• Глобальный каталог, содержащий сведения о каждом объекте в каталоге. Это позволяет пользователям и администраторам находить сведения о каталоге независимо от того, какой домен в каталоге фактически содержит данные.

• Механизм запроса и индекса, чтобы объекты и их свойства могли быть опубликованы и найдены сетевыми пользователями или приложениями.

• Служба репликации, которая синхронизирует данные каталога по сети. Все контроллеры домена в домене участвуют в репликации и содержат полную копию всех сведений о каталоге для своего домена. Любые изменения данных каталога реплицируются в домене на все контроллеры домена.

**Структура и архитектура хранения Active Directory состоят из четырех частей**:

• Домены и леса Active Directory. Леса, домены и организационные единицы (OU) составляют основные элементы логической структуры Active Directory. Лес определяет один каталог и представляет собой границу безопасности. Леса содержат домены.

• Поддержка системы доменных имен (DNS) для Active Directory. DNS предоставляет службу разрешения имен для определения местоположения контроллера домена и иерархическую структуру, которую Active Directory может использовать для обеспечения соглашения об именах, которое может отражать организационную структуру.

• Схема. Схема предоставляет определения объектов, которые используются для создания объектов, хранящихся в каталоге.

• Хранилище данных. Хранилище данных — это часть каталога, которая управляет хранением и получением данных на каждом контроллере домена.

**Active Directory имеет два типа групп**:

• Группы безопасности. Используйте для назначения разрешений общим ресурсам.

• Группы рассылки: создание списков рассылки электронной почты

Группы безопасности могут обеспечить эффективный способ назначения доступа к ресурсам в сети.

Группы рассылки можно использовать только для отправки электронной почты в коллекции пользователей с помощью почтового приложения, например, Exchange Server. Группы рассылки не включены в систему безопасности, поэтому их нельзя включить в списки управления доступом.

# Тема 5.3. Механизмы безопасности в операционных системах семейства Linux

# 33. Механизмы безопасности в операционных системах семейства Linux.

Типы файлов в ОС Linux. Владельцы файлов. Управление правами доступа в файловой системе. Атрибуты файлов. Управление свойствами файлов.

**Типы файлов в ОС Linux**

В GNU/Linux как и других Unix-подобных операционных системах понятие типа файла не связано с расширением файла (несколькими буквами после точки в конце имени), как это обстоит в Windows. Поэтому тип файла в Linux – это скорее тип объекта, но не тип данных как в Windows. В операционной системе GNU/Linux существуют следующие типы файлов:

• обычные файлы

• каталог

• символьные ссылки

• блочные устройства

• символьные устройства

• сокеты

• каналы

Каждый тип имеет собственное обозначение одним символом.

**Обычные файлы(-)** Сюда относятся все файлы с данными, играющими роль ценной информации сами по себе. Linux не различает текстовые файлы, исполняемые или картинки. В любом случае это будет обычный (regular) файл. Все они обозначаются знаком "-". Остальные типы файлов считаются специальными (special).

**Каталоги**(d) В Linux каталог представляет собой такой тип файла, данными которого является список имен других файлов и каталогов, вложенных в данный каталог. Напрямую, то есть через какой-либо редактор, пользователь не может редактировать данные файла-каталога. Редактированием занимается ядро операционной системы, получая, в том числе от пользователя, команды создания файла, удаления и др. В файле каталога осуществляется связь между именами файлов (словесного обозначения для людей) и их индексными дескрипторами (истинным именем-числом, которым оперирует ОС). В Unix-подобных системах один и тот же файл может существовать под разными именами и/или в разных каталогах: все имена будут связаны с одним и тем же индексным дескриптором (механизм жестких ссылок). Также следует, что файлы всегда должны содержаться в каталогах, иначе станут недоступны, так как нигде не будет содержаться записи о них.

**Символьные ссылки(l**) Символьная ссылка – это файл, в данных которого содержится адрес другого файла по его имени (а не индексному дескриптору). Выполнение символьной ссылки приводит к открытию файла, на который она указывает. Это аналог ярлыков в операционной системе Windows. Если удалить исходный файл, то символьная ссылка продолжит существовать. Она по-прежнему будет указывать на файл, которого уже нет. Символьные ссылки не содержат атрибутов файлов, на которые они указывают. У них есть собственные атрибуты (свое время создания, размер, права доступа).

В системе Linux есть два типа ссылок: **Символьные ссылки (**symbolic links, или soft links) указывают путь к другому файлу. Если удалить файл, на который указывает ссылка (называемая target), ссылка все равно будет существовать, но перестанет «работать», поскольку теперь она указывает на несуществующий файл. Может указывать на файл в другой файловой системе.

**Жесткие ссылки (hard links)** указывают на то же место (inode) на диске, где находится исходный файл. После создания жесткой ссылки она становится неотличимой от оригинального имени файла, то есть как бы становится дополнительным именем файла. После удаления исходного файла жесткая ссылка продолжает существовать. Файл удаляется, когда количество жестких ссылок на него становится равным нулю. Должны указывать на файл в этой же файловой системе.

**Символьные (c) и блочные устройства (b)** Файлы устройств предназначены для обращения к аппаратному обеспечению компьютера (дискам, принтерам, терминалам и др.). Когда происходит обращение к файлу устройства, то ядро операционной системы передает запрос драйверу этого устройства. К символьным устройствам обращение происходит последовательно (символ за символом). Примером символьного устройства может служить терминал. Считывать и записывать информацию на блочные устройства можно в произвольном порядке, причем блоками определенного размера. Пример: жесткий диск.

**Сокеты (s) и каналы (p)** Чтобы понять, что такое канал и сокет, необходимо понимание процессов в операционной системе. И каналы, и сокеты организуют их взаимодействие. Пользователь с данными типами файлов почти не сталкивается. Ключевым отличием канала от сокета является то, что канал однонаправлен. Через канал один процесс всегда передает данные второму, но не наоборот. Сокеты позволяют передавать данные в разных направлениях, т. е. осуществляют связь. Также следует отметить, что канал представлен в структуре каталогов файлом, только если он именован. Когда возникают безымянные каналы, то они существуют только внутри ядра Linux.

**Временные файлы** — это файлы, используемые программами для хранения данных, которые нужны только в течение короткого времени. Это могут быть данные о запущенных процессах, журналы ошибок, промежуточные файлы, используемые при преобразовании данных, файлы кэша и т.д.

**В Linux у каждого файла и каждого каталога есть два владельца: пользователь и группа.** Эти владельцы устанавливаются при создании файла или каталога. Пользователь, который создаёт файл становится владельцем этого файла, а первичная группа, в которую входит этот же пользователь, так же становится владельцем этого файла. Чтобы определить, есть ли у вас как у пользователя права доступа к файлу или каталогу, оболочка проверяет владение ими

Это происходит в следующем порядке:

1. Оболочка проверяет, являетесь ли вы владельцем файла, к которому вы хотите получить доступ. Если вы являетесь этим владельцем, вы получаете разрешения и оболочка прекращает проверку.

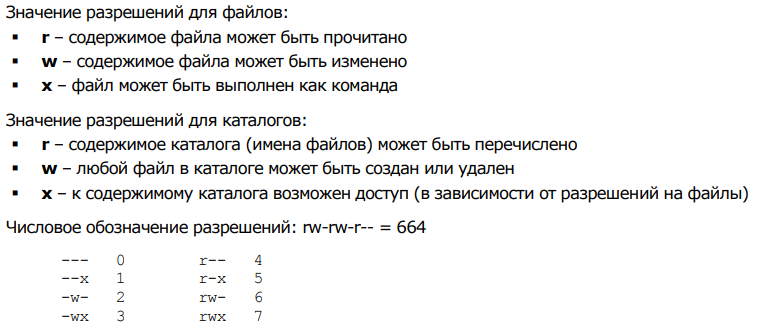
2. Если вы не являетесь владельцем файла, оболочка проверит, являетесь ли вы участником группы, у которой есть разрешения на этот файл. Если вы являетесь участником этой группы, вы получаете доступ к файлу с разрешениями, которые для группы установлены, и оболочка прекратит проверку.

3. Если вы не являетесь ни пользователем, ни владельцем группы, вы получаете права других пользователей (Other).

//Команда **chown** позволяет сменить владельца (команда chgrp – только группу-владельца). Имя пользователя-владельца и группы владельца разделяется двоеточием; Если текущий пользователь linda хочет изменить эффективную первичную группу, он будет использовать **команду newgrp**, за которой следует имя группы, которую он хочет установить в качестве новой эффективной первичной группы. После изменения действующей основной группы все новые файлы, созданные пользователем, получат эту группу в качестве группы-владельца. Чтобы вернуться к исходной настройке первичной группы, //используйте **exit**

**Разрешения на доступ к файлу**

Три крайних правых цифры в числовом представлении относятся к следующим категориям пользователей: первая относится к пользователю-владельцу, вторая – к группе-владельцу, третья – ко всем остальным пользователям

****

Команда **chmod** позволяет изменять разрешения двумя способами:

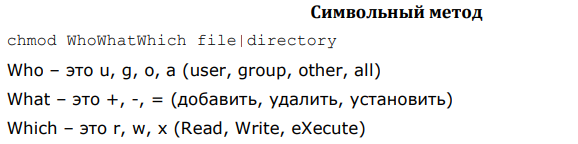
**символьным** chmod a+x cat.txt

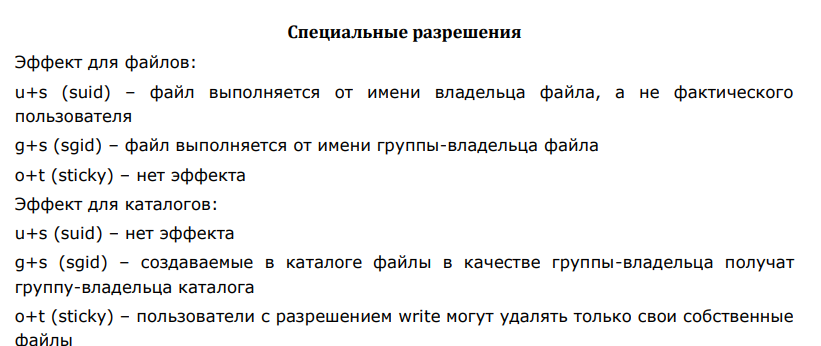
**числовым** chmod 750 animals

Некоторые опции:

-R, --recursive изменять файлы и директории рекурсивно

-v, --verbose выводить диагностику о каждом обрабатываемом файле

-c, --changes выводить диагностику только для изменяемых файлов 



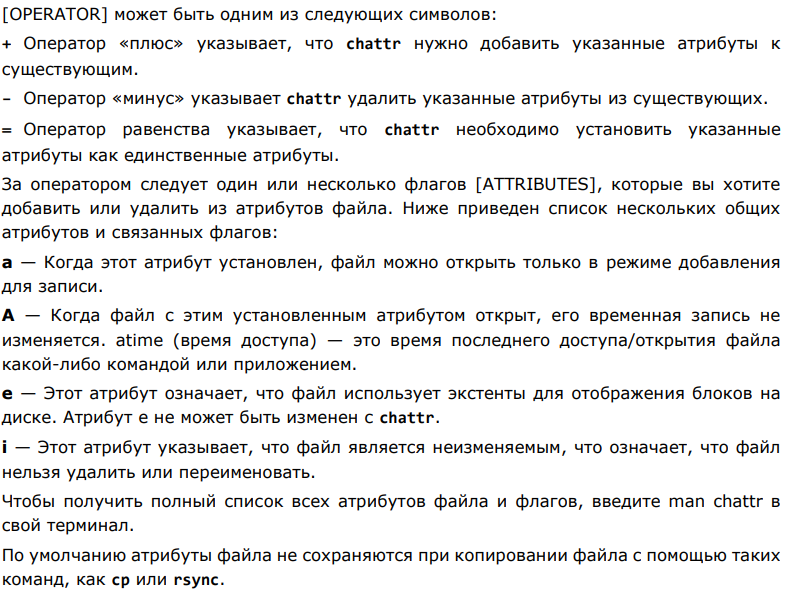
При создании файла или директории, среда операционной системы присваивает им определенные права доступа по умолчанию**. umask - пользовательская маска** (user mask), которая используется для определения конечных прав доступа. После процедуры начальной инсталляции Linux по умолчанию она равна 0022 (022) или 0002 (002).

В операционной системе Linux базовые права для директории равны 0777 (rwxrwxrwx), а для файла 0666 (rw-rw-rw) По умолчанию umask 0002 используется для обычного пользователя. С этой маской права по умолчанию для директории равны 775, а для файла - 664 Для суперпользователя (root) umask по умолчанию равна 0022. С этой маской права по умолчанию для директории равны 755, а для файла – 644.

**Специальное разрешение «sticky bit»**, которое применяется только к каталогам, запрещает пользователям удалять или переименовывать файл в таком каталоге, если они не владеют файлом В выводе команды ls -l каталоги с установленным sticky bit обозначаются буквой t вместо x в последней группе разрешений.

**В Linux атрибуты файла** — это свойства метаданных, которые описывают поведение файла. Например, атрибут может указывать, сжат ли файл, или указывать, можно ли удалить файл. Некоторые атрибуты, такие как неизменяемость, могут быть установлены или очищены, в то время как другие, такие как шифрование, доступны только для чтения и могут быть только просмотрены. Поддержка определенных атрибутов зависит от используемой файловой системы





**Метки времени (timestamps)**

Доступ (Access - last access) — время, когда файл был прочитан последний раз.

У каждого файла доступны следующие метки времени:

• Доступ

• Модифицирован

• Изменён

• Создан

Временные метки файла являются частью функциональности файловой системы. Следовательно, на различных файловых системах некоторые временные метки могут быть недоступны.

**Доступ (Access - last access)** — время, когда файл был прочитан последний раз. Это время меняется при доступе таких системных вызовов как mknod(2), utimes(2) и read(2). Если это текстовый файл, то дата последнего доступа обновляется при каждом его открытии. Если это исполнимый файл, то дата доступа обновится при его запуске. При некоторых опциях монтирования диска (noatime или relatime) это значение может быть неточным**. Модифицирован** (Modify - last modified) — время последнего изменения содержимого файла. То есть если это текстовый файл, то время модификации поменяется когда вы его откроете и удалите какое-то слово или что-то допишите. Меняется системными вызовами mknod(2), utimes(2) и write(2). **Изменён** (Change - last changed) — Время последнего изменения метаданных файлов в файловой системе. То есть если в файле изображения вы измените EXIF метаданные — это будет модификация (поскольку по сути поменяется содержимое файла). Примером Изменения файла является смена разрешений доступа к нему (чтение, запись, выполнение), смена владельца, группы и т. д. Меняется с chmod(2), chown(2), link(2), mknod