



Geekbrains

«Системное администрирование»

Программа: Разработчик-аналитик
Специализация Data Engineer
Сорокин Алексей Альбертович

Лысково
2024



СОДЕРЖАНИЕ

Введение

Глава 1. Основы системного администрирования

1.1. Понятие и задачи системного администрирования

1.2. Роль системного администратора

1.3. Типы и уровни системного администрирования

Глава 2. Менеджмент серверов

2.1. Сборка ПК и подбор компонентов

2.2. Виды серверов и их функции

2.3. Установка, настройка и обновление операционных систем

2.4. Управление доступом к серверам

Глава 3. Сетевое администрирование

3.1. Основы сетевых технологий

3.2. Настройка сетевого оборудования

3.3. Wi-Fi точка доступа.

3.4. Обеспечение безопасности сети

Глава 4. Управление пользователями и группами

4.1. Создание и управление учетными записями пользователей

4.2. Назначение прав и разрешений

4.3. Обеспечение безопасности доступа пользователей

Глава 5. Системный мониторинг и диагностика

5.1. Инструменты системного мониторинга

5.2. Обнаружение и устранение неисправностей

5.3. Резервное копирование и восстановление данных

Глава 6. Безопасность информационных систем

6.1. Угрозы безопасности информационных систем

6.2. Меры по обеспечению безопасности

6.3. Мониторинг безопасности и реагирование на инциденты

Глава 7. Инструменты системного администрирования

7.1. Автоматизация задач

7.2. Системы управления конфигурациями

7.3. Системы мониторинга и оповещения

Глава 8. Практическое применение системного администрирования

8.1. Применение системного администрирования в различных отраслях

8.2. Управление крупномасштабными ИТ-системами

8.3. Карьерный рост в системном администрировании

Заключение

Список литературы

Введение

Системное администрирование — это область, охватывающая организацию, настройку, управление и поддержку компьютерных систем и сетей. Системный администратор отвечает за обеспечение бесперебойной работы IT-инфраструктуры, выполнение задач по установке и обновлению программного обеспечения, настройке сетевых служб и обеспечению безопасности данных.

Актуальность темы:

В современных условиях, когда информационные технологии играют ключевую роль в функционировании организаций, необходимость в квалифицированных специалистах по системному администрированию возрастает. Устранение сбоев, обеспечение безопасности данных и непрерывная работа систем становятся критически важными для бизнеса. Понимание основ системного администрирования позволяет эффективно управлять ресурсами и минимизировать риски, связанные с уязвимостями в технологиях.

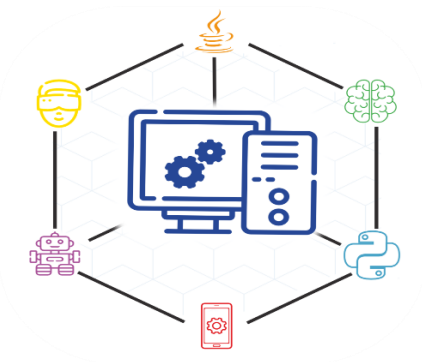
Цели и задачи работы:

Цель данной дипломной работы — рассмотреть основные аспекты системного администрирования и определить его значимость в управлении информационными системами. Основные задачи работы:

1. Изучить роль системного администратора и его обязанности.
2. Проанализировать методы управления пользователями и правами доступа.
3. Исследовать процессы обслуживания серверов и сетевых служб.
4. Рассмотреть инструменты мониторинга и диагностики систем.
5. Определить основные угрозы безопасности и способы их предотвращения.
6. Выявить современные тенденции и нововведения в сфере системного администрирования

Глава 1. Основы системного администрирования

1.1. Понятие и задачи системного администрирования



Системное администрирование - это процесс управления компьютерными системами и сетями, включая планирование, внедрение, эксплуатацию, поддержку и развитие инфраструктуры информационных технологий. Основные задачи системного администратора включают:

- Планирование и развертывание: проектирование и установка новых систем и сетей, а также миграция старых систем на новые платформы.
- Поддержка и обслуживание: обеспечение бесперебойной работы систем, устранение неполадок и решение проблем пользователей.
- Безопасность: защита информации и ресурсов от несанкционированного доступа, предотвращение вирусных атак и других угроз.
- Мониторинг и отчетность: отслеживание состояния систем, сбор статистических данных и подготовка отчетов для руководства.
- Обновления и модернизация: регулярное обновление программного обеспечения и оборудования для поддержания актуальности и эффективности систем.

1.2. Роль системного администратора



Роль системного администратора заключается в обеспечении надежной и безопасной работы информационных систем. Он отвечает за управление всеми аспектами инфраструктуры, начиная от отдельных компьютеров и заканчивая крупными корпоративными сетями. Основные роли системного администратора:

- Технический специалист: занимается установкой, настройкой и поддержкой аппаратных и программных компонентов систем.
- Консультант: предоставляет техническую помощь и консультации пользователям по вопросам работы с системами.
- Архитектор: проектирует и разрабатывает структуру систем, учитывая требования бизнеса и технические ограничения.
- Аналитик: анализирует данные о работе систем и принимает решения по оптимизации их функционирования.

1.3. Типы и уровни системного администрирования



Существует несколько типов системного администрирования, каждый из которых отличается специфическими задачами и областями ответственности:

- Локальное администрирование: управление отдельными компьютерами и локальными сетями.

- Корпоративное администрирование: работа с крупными сетями и инфраструктурами, охватывающими несколько офисов и подразделений компании.

- Хостинговое администрирование: управление виртуальными и физическими серверами, размещенными в дата-центрах.

- Проектное администрирование: координация и выполнение проектов по внедрению новых систем или модернизации существующих.

Системное администрирование может осуществляться на разных уровнях:

- Базовый уровень: выполнение рутинных операций по поддержке и обслуживанию систем.

- Средний уровень: разработка и реализация решений для улучшения работы систем.

- Высокий уровень: стратегическое планирование и управление большими информационными инфраструктурами.

Таким образом, системное администрирование является важным элементом современной информационной среды, требующим глубоких знаний и навыков в области информационных технологий.

Глава 2. Менеджмент серверов

2.1 Сборка ПК и подбор компонентов



Центральный процессор (ЦП; также центральное процессорное устройство — ЦПУ; англ. central processing unit, CPU, дословно — центральное обрабатывающее устройство) — электронный блок либо интегральная схема(микропроцессор), исполняющая машинные инструкции (код программ), главная часть аппаратного обеспечения компьютера или программируемого логического контроллера. Иногда называют микропроцессором или просто процессором.

Процессор занимается обработкой всех задач, выполняемых на компьютере.

Сокеты Intel

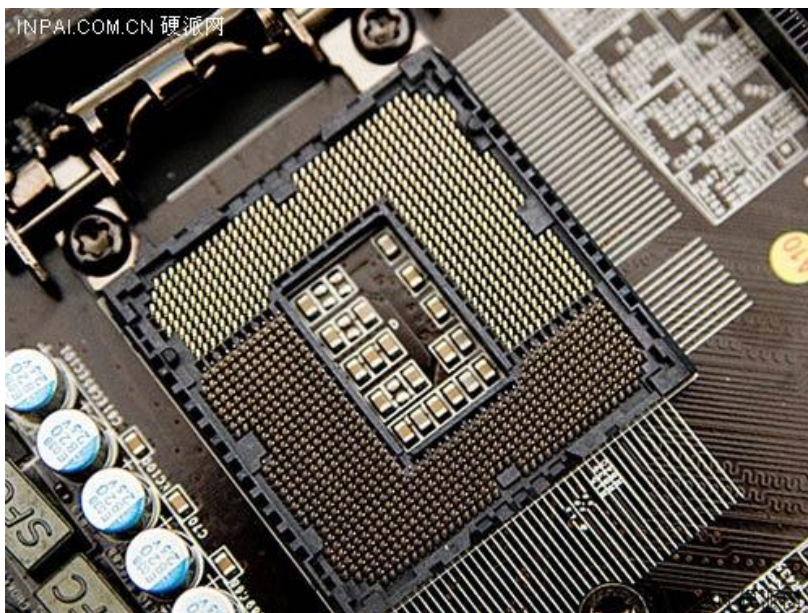
Динамика обновления сокетов для процессоров Intel, на порядок выше, чем у тех же сокетов новых процессоров AMD. В рамках своей предпоследней серии процессоров, появилось целых три сокета, причем они полностью несовместимы.

Socket 478 или mPGA478B — процессорный разъём, предназначенный для установки процессоров Intel Pentium 4 и Celeron, безнадежно устарели, но еще встречаются у клиентов.

Socket (сокеты LGA 775) – эти сокеты уже морально устарели, хотя еще живут во множестве систем, они позиционировались под несколько линеек сразу, таких как Core 2 Duo, Core 2 Quad, Celeron и другие.

Socket (сокеты LGA 1155, 1156, 1366) – данные сокеты можно условно поместить в одну «пачку», но они не совместимы, хоть и позиционируются под одну микроархитектуру Sandy Bridge II, просто для разных версий.

Наиболее ходовым оказался сокет 1155, на нем сейчас и построены большинство систем. Для мощных систем и серверных решений на борту с Core i7 и Xeon, был разработан Socket 1366.



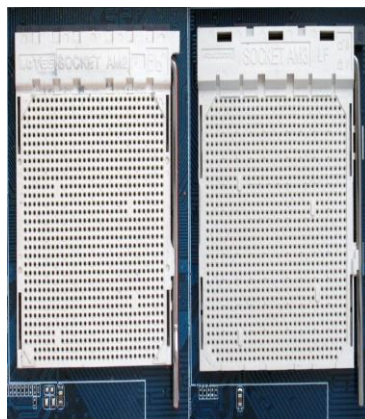
Сокет LGA 1155 на плате MSI. На этой фотографии можно заметить, что "ножки" контактов торчат из сокета на материнской плате.

Socket (LGA 1150 (Socket H3) - процессорный разъем для процессоров Intel Haswell, четвертое поколение процессоров Intel линейки iX и платформы Ivy Bridge.

Socket (сокет LGA 2011) – один из сокетов для некоторых процессоров Ivy Bridge (Core i7, i5, i3 – 3xxx, Xeon)

Сокеты AMD

Политика компании AMD в плане сокетов более консервативна. Несколько сокетов имеют совместимость благодаря сериям с «+». К примеру, Socket AM2 совместим с AM2+, что дает более широкие возможности для апгрейда, но вместе с этим, это немного неприятное топтание на одном месте, что не позволительно для IT- сферы.



Сокет AM2. На этой фотографии, напротив, можно наблюдать углубления под эти контакты, а сами они находятся непосредственно на процессоре.

Socket (сокет AM3 и AM3+) – можно сказать сокет и его модификация, по спецификациям они совместимы между собой, разрабатывались под процессоры FX, Phenom II, Athlon II. Сокет для наиболее мощных Bulldozer (FX) среди лагеря AMD, которые не оправдали надежды, но упав в цене стали более интересным приложением, с точки зрения неплохой производительности за низкую цену.

Socket (сокет AM2 и AM2+) – сокеты для процессоров Phenom, Athlon, Sempron. Также, полностью совместимы. На сегодняшний день можно считать немного устаревшими, хотя еще активно работает масса систем построенных на основе данных сокетов.

Socket (сокет FM1 и FM2) – сокеты FM создавались под процессоры серии AMD Fusion, которые отличаются очень мощной интегрированной графикой. На данный сокет и совместимые с ним процессоры, следует ориентироваться тем, кто не желает тратить на дискретную видеокарту и будет довольствоваться интегрированной графикой.

Сокеты AM3+ и FM2 сейчас являются наиболее ходовыми, на них комплектуется большинство как дешевых, так и более дорогих систем. То есть можем смело констатировать практичность данных соЛинейки процессоров AMD: Sempron, Athlon, Athlon 64, Athlon II, FX-серия, A-серия, Intel: Core iX 1-4 поколение, Core 2 Duo, Pentium D, Pentium 4, Celeron. Для каких целей позиционируются каждая серия? Какие актуальны сегодня. Соотнести процессоры с сокетами.

Линейка процессоров AMD:

Небольшой исторический экскурс (ибо без этого довольно тяжело разобраться во всех хитросплетениях развития и позиционирования процессоров от AMD):

2003 год. Компания AMD выпускает первые 64-битные процессоры, полностью совместимые с процессорами x86, известные под названием Opteron и предназначавшиеся для серверов и рабочих станций. А в сентябре компания AMD выпускает аналогичные процессоры, известные как Athlon 64, и для персональных компьютеров.

2003 г. — AMD K7 Thorton (Athlon XP). Thorton — это скорее очередной Duron, экономичная модель Athlon XP на ядре Barton. Использование слова «Athlon» позволяет позиционировать Thorton как более производительную микросхему по сравнению с предыдущими Duron. Технология производства 0,130 мкм. Тактовая частота 1667—2133 МГц (2000+...2400+), частота шины 266 МГц (dual-pumped).

2004 г. Представление процессора Sempron, которое должно было иметь место в середине августа, перенесено на 28 июля 2004 г. (выпуск 17 августа). Sempron 3100+ для Socket 754 ядро Paris, Sempron 2500+ (1750 МГц), 2600+ (1833 МГц), 2800+ (2000 МГц) для Socket A, ядро Barton. Модели Sempron под Socket A просуществуют до конца 2005 года, но в малобюджетных системах.

Самым последним процессором Sempron под Socket A будет модель 2800+. Эти процессоры позиционировались, как конкуренты Intel Celeron D 2005 г. - Компанией AMD были выпущены двухъядерные процессоры Athlon 64 X2.

2006 г. - Покупка канадской компании ATI компанией AMD.

2007 г. - Появились первые четырёхъядерные процессоры AMD Phenom X4, первые конкуренты ранних Intel Core 2 Quad.

2008 г. - на AMD Technology Analyst Day компания публично анонсировала две реализации процессора Fusion (от [англ. fusion](#) — [рус. слияние](#)) — кодовое наименование [микропроцессорной архитектуры](#). Суть проекта «AMD Fusion» заключается в объединении [центрального многозадачного универсального процессора](#) с [графическим параллельным многоядерным процессором](#) в одном кристалле. Процессоры, создаваемые по такой микроархитектуре, называются [APU](#) — Accelerated Processing Unit (ускоренное обрабатывающее устройство, по аналогии с CPU (Central Processing Unit, центральное обрабатывающее устройство)).

2009 г. - с переходом на новый Socket AM3 процессоры AMD обзавелись поддержкой памяти DDR3, что позволило установить на материнскую плату до 16 Гб ОЗУ.

2010 г. - AMD выпускает первые шестиядерные процессоры для настольных ПК Phenom II X6, совместимые с платформами Socket AM2+ и Socket AM3.

2011 г. - AMD выпускает процессоры на микроархитектуре Bulldozer.

2012 г. – AMD анонсировала линейку новых APU Trinity

ОЗУ

ОЗУ (оперативное запоминающее устройство), оно же RAM (“Random Access Memory” – память с произвольным доступом), представляет собой область временного хранения данных, при помощи которой обеспечивается функционирование программного обеспечения. Физически, оперативная память в системе представляет собой набор микросхем или модулей (содержащих микросхемы), которые обычно подключаются к системной плате.

В процессе работы память выступает в качестве временного буфера (в ней хранятся данные и запущенные программы) между дисковыми накопителями и процессором, благодаря значительно большей скорости чтения и записи данных.

Примечание.

Совсем новички часто путают оперативную память с памятью жесткого диска (ПЗУ – постоянное запоминающее устройство), чего делать не нужно, т.к. это совершенно разные виды памяти.

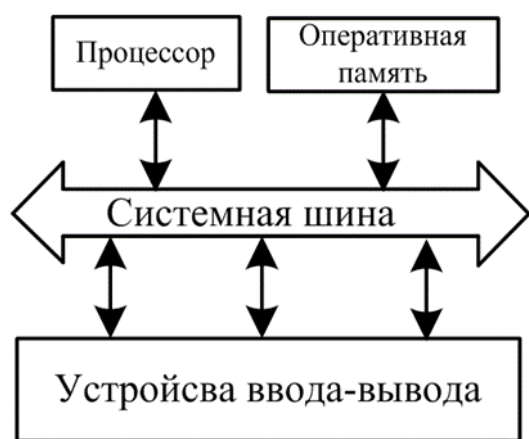
Оперативная память (по типу является динамической – Dynamic RAM), в отличие от постоянной – энергозависима, т.е.

для хранения данных ей необходима электроэнергия, и при ее отключении (выключение компьютера) данные удаляются. Пример энергонезависимой памяти ПЗУ - флэш-память, в которой электричество используется лишь для записи и чтения, в то время как для самого хранения данных источник питания не нужен.

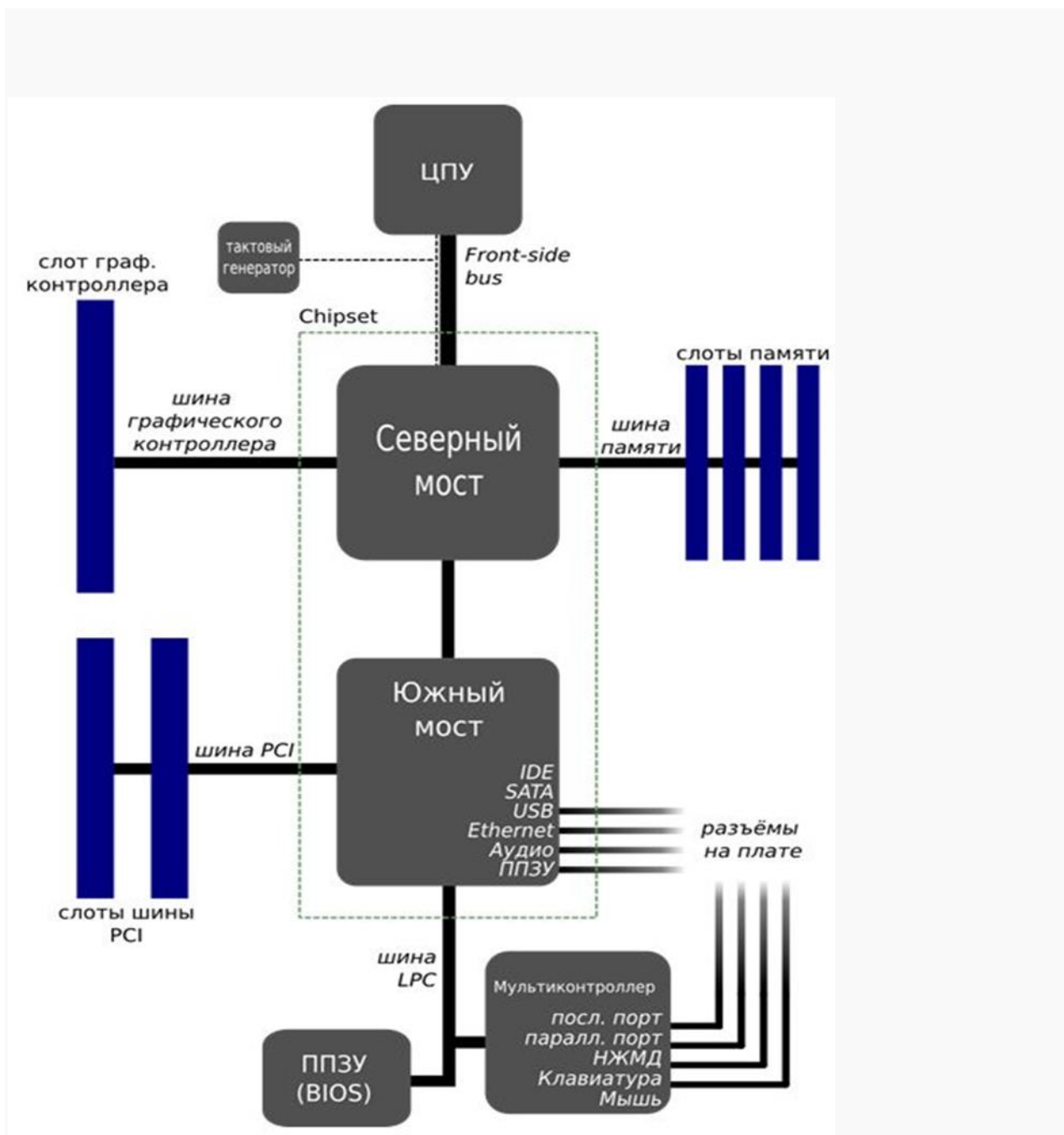
По своей структуре память напоминает пчелиные соты, т.е. состоит из ячеек, каждая из которых предназначена для хранения мёда определенного объема данных, как правило, одного или четырех бит. Каждая ячейка оной имеет свой уникальный «домашний» адрес, который делится на два компонента – адрес горизонтальной строки (Row) и вертикального столбца (Column).

Ячейки представляют собой конденсаторы, способные накапливать электрический заряд. С помощью специальных усилителей аналоговые сигналы переводятся в цифровые, которые в свою очередь образуют данные. Для передачи на микросхему памяти адреса строки служит некий сигнал, который зовется RAS (Row Address Strobe), а для адреса столбца — сигнал CAS (Column Address Strobe).

Работа оперативной памяти непосредственно связана с работой процессора и внешних устройств компьютера, так как именно ей последние «доверяют» свою информацию. Таким образом, данные сперва попадают с жесткого диска (или другого носителя) в саму ОЗУ и уже затем обрабатываются центральным процессором (смотрите изображение).



Оперативной памятью управляет контроллер, который находится в чипсете материнской платы, а точнее в той его части, которая называется North Bridge (северный мост) – он обеспечивает подключение CPU(процессора) к узлам, использующим высокопроизводительные шины: ОЗУ, графический контроллер (смотрите изображение). В современных процессорах контроллер уже встроен в процессор. Материнская плата освобождена от этой роли.



Примечание.

Важно понимать, что если в процессе работы оперативной памяти производится запись данных в какую-либо ячейку, то её содержимое, которое было до поступления новой информации, будет безвозвратно утеряно. Т.е. по команде процессора данные записываются в указанную ячейку, одновременно стирая при этом то, что там было записано ранее.

Рассмотрим еще один важный аспект работы оперативки – это ее деление на несколько разделов с помощью специального программного обеспечения (ПО), которое поддерживается операционными системами.

Дело в том, что современные устройства оперативной памяти являются достаточно объемными (привет двухтысячным, когда хватало и 32 Мб), чтобы

в ней можно было размещать данные от нескольких одновременно работающих задач. Процессор также может одновременно обрабатывать несколько задач. Это обстоятельство способствовало развитию так называемой системы динамического распределения памяти, когда под каждую обрабатываемую процессором задачу отводятся динамические (переменные по своей величине и местоположению) разделы оперативной памяти.

Динамический характер работы позволяет распоряжаться имеющейся памятью более экономно, своевременно «изымая» лишние участки памяти у одних задач и «добавляя» дополнительные участки – другим (в зависимости от их важности, объема обрабатываемой информации, срочности выполнения и т.п.). За «правильное» динамическое распределение памяти в ПК отвечает операционная система, тогда как за «правильное» использование памяти, отвечает прикладное программное обеспечение.

Совершенно очевидно, что прикладные программы должны иметь способность работать под управлением операционной системы, в противном случае последняя не сможет выделить такой программе оперативную память или она не сможет «правильно» работать в пределах отведенной памяти. Именно поэтому не всегда удастся запустить под современной операционной системой ранее написанные программы, которые работали под управлением устаревших систем, например, под ранними версиями Windows (Windows 98).

Ещё (для общего развития) следует знать, что самая популярная на сегодня, из ныне обитающих на компьютерах пользователей, операционная система Windows 7, разрядностью 64 бита, поддерживает объем памяти до 192 Гбайт (младший 32-битный собрат “видит” не больше 4 Гбайт). Рассмотрим ограничения по объему ОП в зависимости от типа ОС.

32-разрядные версии Windows 2000/2003/XP и Vista теоретически поддерживают до 4 Гб памяти, но реально доступно для приложений не более 2 Гб.

ОС начального уровня Windows XP Starter Edition и Windows Vista Starter способны работать не более чем с 256 Мб и 1 Гб памяти соответственно.

Максимальный поддерживаемый объем 64-разрядной Windows Vista зависит от ее версии и составляет:

Home Basic — 8 Гб;
Home Premium — 16 Гб;
Ultimate — Более 128 Гб;
Business — Более 128 Гб;
Enterprise — Более 128 Гб.

Ограничения оперативной памяти в Windows 7:

В 32-разрядной версии Начальная — 2 Гб;
В 32-разрядной версии Home Basic — 4 Гб;

В 32-разрядной версии Home Premium — 4 Гб;
В 32-разрядной версии Professional — 4 Гб;
В 32-разрядной версии Корпоративная — 4 Гб;
В 32-разрядной версии Ultimate — 4 Гб;

В 64-разрядной версии Начальная — 2 Гб;
В 64-разрядной версии Home Basic — 8 Гб;
В 64-разрядной версии Home Premium — 16 Гб;
В 64-разрядной версии Professional — 192 Гб;
В 64-разрядной версии Корпоративная — 192 Гб;
В 64-разрядной версии Ultimate — 192 Гб;

Ограничения оперативной памяти в Windows 8:

В 32-разрядной версии Windows 8 Enterprise — 2 Гб;
В 32-разрядной версии Windows 8 Professional — 4 Гб;
В 32-разрядной версии Windows 8 — 4 Гб;

В 64-разрядной версии Windows 8 Enterprise — 512 Гб;
В 64-разрядной версии Windows 8 Professional — 512 Гб;
В 64-разрядной версии Windows 8 — 128 Гб;

Обмен данными между процессором и памятью может происходить напрямую, но чаще все же бывает с участием кэш-памяти.

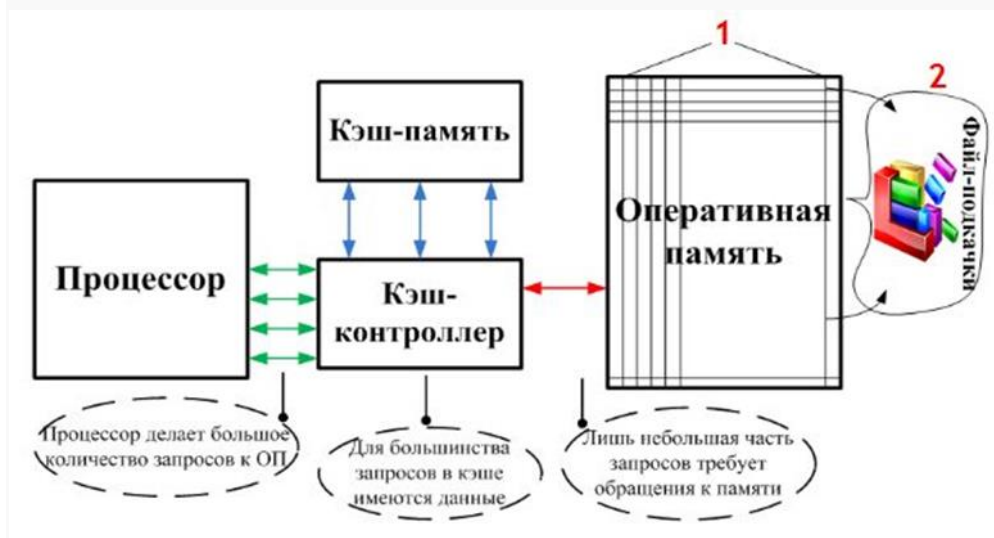
Кэш-память является местом временного хранения наиболее часто запрашиваемой информации и представляет собой относительно небольшие участки быстрой локальной памяти. Её использование позволяет значительно уменьшить время доставки информации в регистры процессора, так как быстроедействие внешних носителей (оперативки и дисковой подсистемы) намного хуже процессорного. Как следствие, уменьшаются, а часто и полностью устраняются, вынужденные простои процессора, что повышает общую производительность системы.

В свою очередь, кэш-памятью управляет специальный контроллер, который, анализируя выполняемую программу, пытается предвидеть, какие данные и команды вероятнее всего понадобятся в ближайшее время процессору, и подкачивает их, т.е. кэш-контроллер загружает в кэш-память нужные данные из оперативной памяти, и возвращает, когда нужно, модифицированные процессором данные в оперативку.

После процессора, оперативную память можно считать самым быстроедействующим устройством. Поэтому основной обмен данными и происходит между этими двумя девайсами. Вся информация в персональном компьютере хранится на жестком диске. При включении компа в ОЗУ с винта записываются драйверы, специальные программы и элементы операционной

системы. Затем туда записываются те программы – приложения, которые мы будем запускать, при закрытии последних они будут стерты из оной.

Данные, записанные в оперативной памяти, передаются в CPU (он же не раз упомянутый процессор, он же Central Processing Unit), там обрабатываются и записываются обратно. И так постоянно (смотрите изображение).



Все это хорошо до тех пор, пока ячеек памяти (1) хватает. А если нет?

Тогда в работу вступает файл подкачки (2). Этот файл расположен на жестком диске и туда записывается все, что не влезает в ячейки оперативной памяти. Поскольку быстродействие жесткого диска значительно ниже, чем у ОЗУ, то работа файла подкачки сильно замедляет работу системы. Кроме этого, это снижает долговечность самого жесткого диска. Но это уже совсем другая история.

Примечание.

Во всех современных процессорах имеется кэш (cache) – массив сверхскоростной оперативной памяти, являющейся буфером между контроллером сравнительно медленной системной памяти и процессором.

В этом буфере хранятся блоки данных, с которыми CPU работает в текущий момент, благодаря чему существенно уменьшается количество обращений процессора к чрезвычайно медленной (по сравнению со скоростью работы процессора) системной памяти. Однако, кэш-память малоэффективна при работе с большими массивами данных (видео, звук, графика, архивы), ибо такие файлы просто туда не помещаются, поэтому все время приходится обращаться к оперативной памяти, или к HDD (у которого также имеется свой кэш).

Типы оперативной памяти для рабочих станций: DDR, DDR2, DDR3.

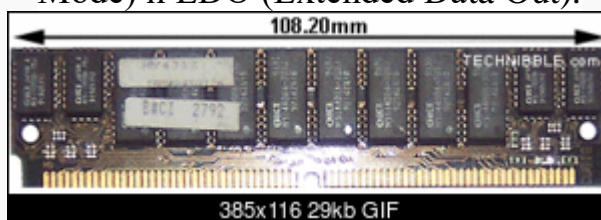
Самые распространённые типы оперативной памяти которые применялись и применяются в персональных компьютерах в обиходе называются SIMM, DIMM, DDR, DDR2, DDR3.

SIMM

SIMM на 30 контактов. Применялись в персональных компьютерах с процессорами от 286 до 486. Сейчас уже является раритетом.



SIMM на 72 контакта. Память такого типа была двух видов FPM (Fast Page Mode) и EDO (Extended Data Out).



Тип FPM использовался на компьютерах с процессорами 486 и в первых Pentium до 1995 года. Потом появился EDO. В отличие от своих предшественников, EDO начинает выборку следующего блока памяти в то же время, когда отправляет предыдущий блок центральному процессору.

Конструктивно они одинаковы, отличить можно только по маркировке. Персоналки, поддерживавшие EDO, могли работать и с FPM, а вот наоборот – далеко не всегда.

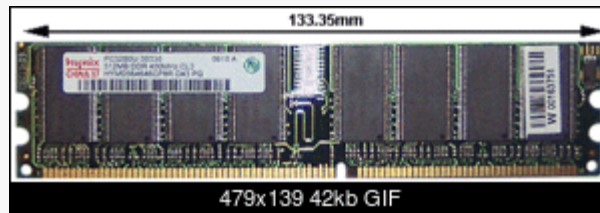
DIMM



Так называли тип памяти SDRAM (Synchronous DRAM). Начиная с 1996 года большинство чипсетов Intel стали поддерживать этот вид модулей памяти, сделав его очень популярным вплоть до 2001 года. Большинство компьютеров с процессорами Pentium и Celeron использовали именно этот вид памяти.

Дальше пошла эра DDR, и память почти перестали называть симы или димы. Теперь в ходу название DDR (DDR2, DDR3) модуль или планка.

DDR



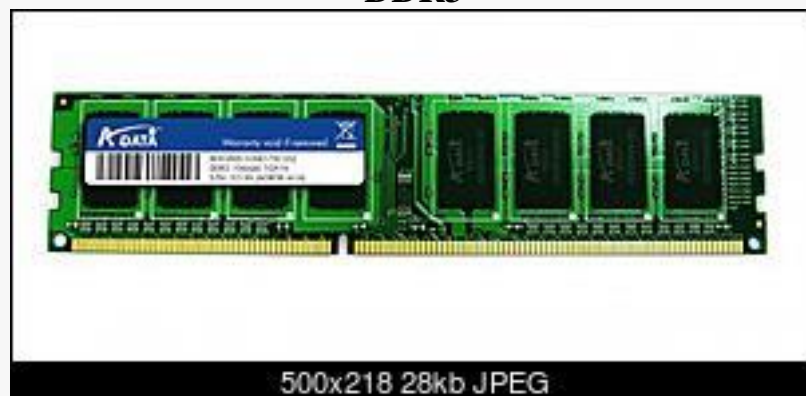
DDR (Double Data Rate) стал развитием SDRAM. Этот вид модулей памяти впервые появился на рынке в 2001 году. Основное отличие между DDR и SDRAM заключается в том, что вместо удвоения тактовой частоты для ускорения работы, эти модули передают данные дважды за один такт.

DDR2

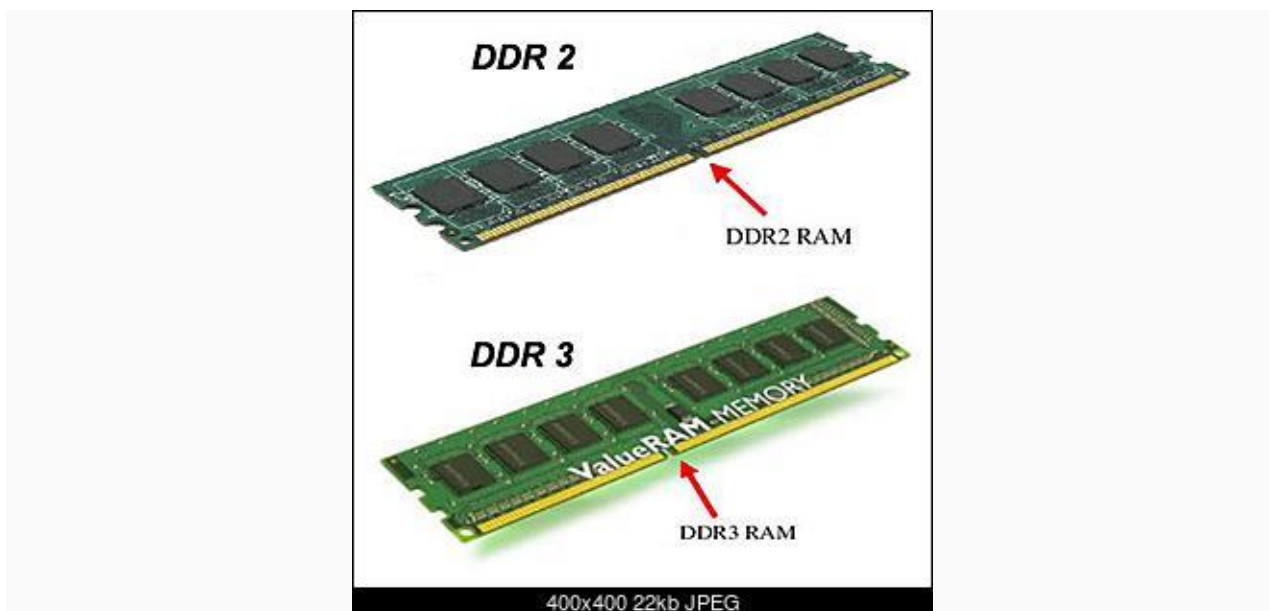


DDR2 (Double Data Rate 2) – более новый вариант DDR, который теоретически должен быть в два раза более быстрым. Впервые память DDR2 появилась в 2003 году, а чипсеты, поддерживающие ее – в середине 2004. Основное отличие DDR2 от DDR – способность работать на значительно большей тактовой частоте, благодаря усовершенствованиям в конструкции. По внешнему виду отличается от DDR числом контактов: оно увеличилось со 184 (у DDR) до 240 (у DDR2).

DDR3



Как и модули памяти DDR2, они выпускаются в виде 240-контактной печатной платы (по 120 контактов с каждой стороны модуля), однако не являются электрически совместимыми с последними, и по этой причине имеют иное расположение «ключа».



Итак, подытожим выше сказанное и четко решим как на практике отличить платы DDR.

Так как ключ смещен всего на пару контактов, и хоть контактов и увеличилось у DDR2 по сравнению с DDR, на глаз отличить их сложно. Поэтому мы тупо считаем контакты и, помня что у DDR2 их 240 на обе стороны, а у DDR 184, успешно дифференцируем тип ОП.

Различить планки DDR2 и DDR3 еще проще. У DDR3 ключ достаточно уведен от центра. (Показано на рисунке выше). Но еще проще посмотреть в программах диагностики (Everest, Siv и тд.), если ПК можно включить.

ПЗУ

Накопитель на жёстких магнитных дисках или **НЖМД** (англ. *hard (magnetic) disk drive*, *HDD*, *HMDD*), *жёсткий диск*, в компьютерном сленге «*винчестер*» — запоминающее устройство (устройство хранения информации) произвольного доступа, основанное на принципе магнитной записи. Является основным накопителем данных в большинстве компьютеров.

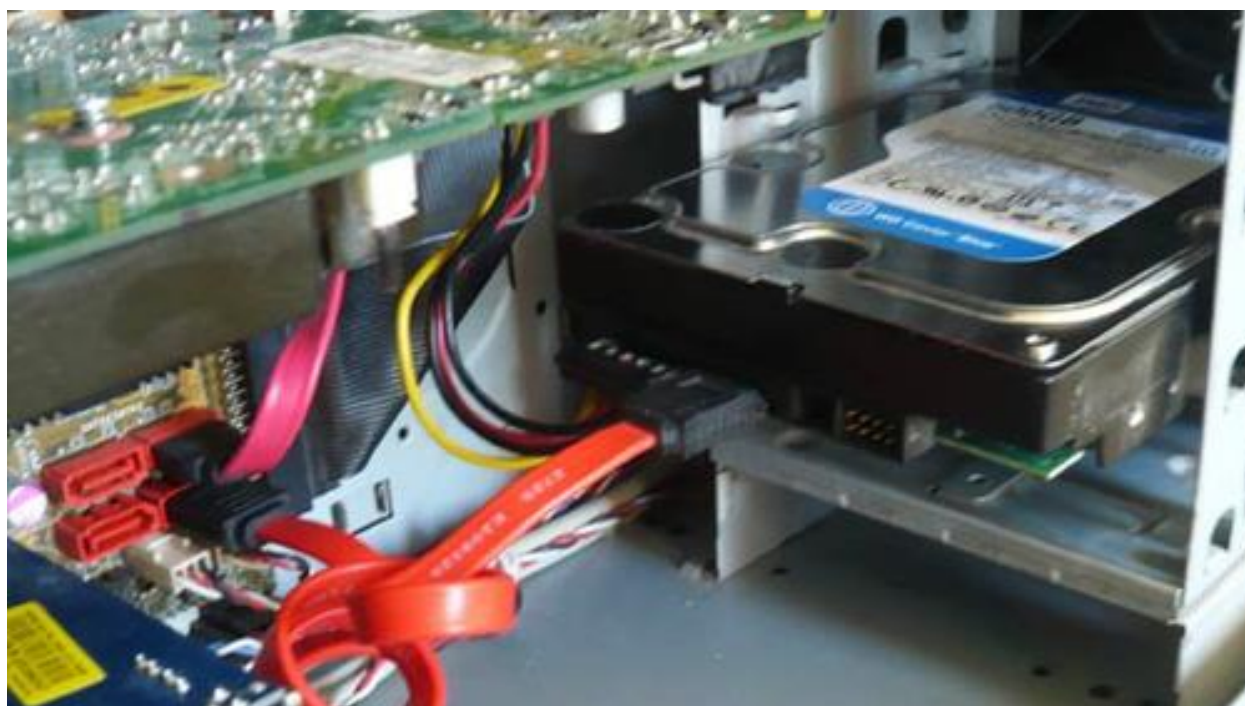


Особенности конструкции и инсталляции в корпуса дисков различных форм-факторов.

Очевидно, что самое основное отличие дисков различного форм-фактора – это их размер. Диски 3.5" больше; их монтаж в корпус ПК (сервера) чаще всего заключается в простой установке в корзину и подключении шлейфов питания и данных:



Диск в корзине, прикреплён на винты



Диск в корзине с подключенными шлейфами SATA

В некоторых случаях, диски монтируются сначала в специальные салазки, и вставляются в корзину уже в них:



Диск в салазках для установки в сервер

Диски 2.5" меньше размером, и соответственно монтируются немного по другому, в зависимости от места установки.

В ноутбуки такие диски монтируются напрямую:



В другие виды ПК такие диски, чаще всего, монтируются на салазках:



Диск в серверных салазках



Диск 2.5" в салазках для монтажа в корзину 3.5"

Аппаратные различия в жестких дисках разного форм-фактора (плотность записи, количество пластин, скорость оборотов шпинделя).

Не секрет, что в современных высокопроизводительных жёстких дисках форм-факторов 3.5" и 2.5" производители используют пластины одинакового размера - от 2.5" HDD. Потому, зачастую, и ёмкость, и параметры производительности 2.5" и 3.5" моделей жёстких дисков одного производителя выглядят одинаково. Более того, некоторые производители объявили о прекращении производства высокопроизводительных жёстких дисков размера 3.5", оставив топовые модели HDD только в форм-факторе 2.5". Доступность высокопроизводительных жёстких дисков форм-фактора 3.5" неуклонно снижается.

Исходя из реалий современного рынка, производители считают экономически нецелесообразным использование более 2-х пластин внутри одного жёсткого диска. Для справки, в жёсткий диск форм-фактора 2.5" (высотой 15мм) возможно установить до 3-х пластин, а в 3.5" HDD - до 5 пластин.

Такой параметр как линейная скорость чтения/записи на внешних треках, теоретически, должна быть выше у жёстких дисков 3.5" чем у 2.5" (при одинаковой скорости вращения шпинделя и при одинаковой плотности записи) просто за счёт физически большего размера пластин, но в реальности отличия незначительны, так как в высокопроизводительных жёстких дисках разных форм-факторов зачастую находятся пластины одинакового размера.

В общем случае, чем больше в сервере жёстких дисков, тем больше электропотребление (более мощными должны быть блоки питания), и больше тепловыделение (более мощной должна быть система вентиляции сервера и затраты на охлаждение). Однако, по сравнению с 3.5" моделями жёстких дисков, современные 2.5" жесткие диски имеют в 2 раза меньшее энергопотребление (во всех режимах) и, как следствие, меньшее тепловыделение и затраты на охлаждение. Таким образом, сервер с 24-мя 2.5" жёсткими дисками потребляет электричества и греет окружающее пространство меньше, чем сервер с 12-ю 3.5" жёсткими дисками.

Надёжности жёстких дисков всегда уделяется большое внимание. За счёт уменьшения габаритов (и дополнительных инженерных решений) 2.5" жёсткие диски обладают повышенной устойчивостью к вибрации и механическим воздействиям. Это подтверждается самими производителями, наработка на отказ (MTBF) у последних моделей 2.5" жёстких дисков составляет 2 млн. часов, по сравнению с лучшими моделями 3.5" жестких дисков, у которых MTBF декларируется на уровне 1,3-1,6 млн. часов.

Также, 2.5" диски производят при работе немного меньший шум по сравнению с 3.5" моделями.

Такие характеристики, как плотность записи и скорость оборотов шпинделя, от форм-фактора не зависят.

Интерфейсы обмена данными (SATA, IDE):

Чем отличаются IDE от SATA?

1. Разъемы интерфейсов.
2. Принцип передачи данных
3. Скорость передачи данных.



Внешний вид разъёма IDE



Внешний вид разъёма SATA I (II, III)

Особенности интерфейса IDE (где используется, какие ограничения присутствуют, скоростные характеристики);

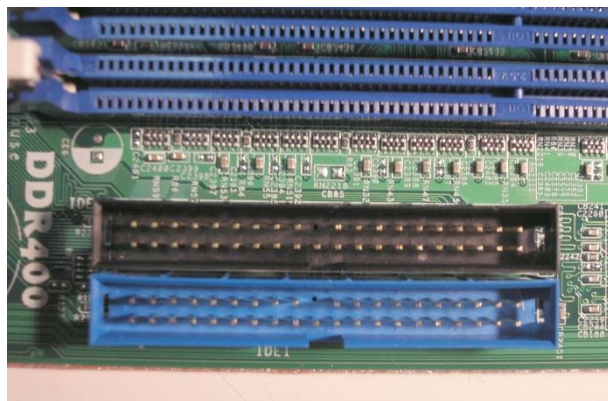
IDE (ATA) — параллельный интерфейс подключения накопителей (жёстких дисков и оптических дисководов) к компьютеру. В настоящее время

вытесняется своим последователем — SATA и с его появлением получил название PATA (Parallel ATA).

Для подключения жёстких дисков с интерфейсом PATA обычно используется 40-проводный кабель (именуемый также шлейфом). Каждый шлейф обычно имеет два или три разъёма, один из которых подключается к разъёму контроллера на материнской плате (в более старых компьютерах этот контроллер размещался на отдельной плате расширения), а один или два других подключаются к дискам. В один момент времени шлейф P-ATA передаёт 16 бит данных. Иногда встречаются шлейфы IDE, позволяющие подключение трёх дисков к одному IDE каналу, но в этом случае один из дисков работает в режиме read-only.



Шлейфы IDE



*Разъёмы IDE на материнской плате
(внизу)*

Долгое время шлейф ATA содержал 40 проводников, но с введением режима Ultra DMA/66 (UDMA4) появилась его 80-проводная версия. Все дополнительные проводники — это проводники заземления, чередующиеся с информационными проводниками. Таким образом вместо семи проводников заземления их стало 47. Такое чередование проводников уменьшает ёмкостную связь между ними, тем самым сокращая взаимные наводки. Ёмкостная связь является проблемой при высоких скоростях передачи, поэтому данное нововведение было необходимо для обеспечения нормальной работы установленной спецификацией UDMA4 скорости передачи 66 МБ/с (мегабайт в секунду). Более быстрые режимы UDMA5 и UDMA6 также требуют 80-проводного кабеля.

Стандарт ATA всегда устанавливал максимальную длину кабеля равной 46 см. Это ограничение затрудняет присоединение устройств в больших корпусах, или подключение нескольких приводов к одному компьютеру, и почти полностью исключает возможность использования дисков PATA в качестве внешних дисков. Хотя в продаже широко распространены кабели большей длины, следует иметь в виду, что они не соответствуют стандарту. То же самое можно сказать и по поводу «круглых» кабелей, которые также широко распространены. Стандарт ATA описывает только плоские кабели с конкретными характеристиками полного и ёмкостного сопротивлений. Это,

конечно, не означает, что другие кабели не будут работать, но, в любом случае, к использованию нестандартных кабелей следует относиться с осторожностью.

Если к одному шлейфу подключены два устройства, одно из них обычно называется ведущим (англ. master), а другое ведомым (англ. slave). Обычно ведущее устройство идёт перед ведомым в списке дисков, перечисляемых BIOS'ом компьютера или операционной системы. В старых BIOS'ах (486 и раньше) диски часто неверно обозначались буквами: «C» для ведущего диска и «D» для ведомого.

Если на шлейфе только один привод, он в большинстве случаев должен быть сконфигурирован как ведущий. Некоторые диски (в частности, производства Western Digital) имеют специальную настройку, именуемую single (то есть «один диск на кабеле»). Впрочем, в большинстве случаев единственный привод на кабеле может работать и как ведомый (такое часто встречается при подключении CD-ROM'а на отдельный канал).

Настройка, именуемая cable select (то есть «выбор, определяемый кабелем», кабельная выборка), была описана как опциональная в спецификации ATA-1 и стала широко распространена начиная с ATA-5, поскольку исключает необходимость переставлять перемычки на дисках при любых переподключениях. Если привод установлен в режим cable select, он автоматически устанавливается как ведущий или ведомый в зависимости от своего местоположения на шлейфе. Для обеспечения возможности определения этого местоположения шлейф должен быть с кабельной выборкой.

80-проводные кабели, введённые для UDMA4, лишены указанных недостатков. Теперь ведущее устройство всегда находится в конце шлейфа, так что, если подключено только одно устройство, не получается этого ненужного куска кабеля. Кабельная же выборка у них «заводская» — сделанная в самом разъёме просто путём исключения данного контакта. Поскольку для 80-проводных шлейфов в любом случае требовались собственные разъёмы, повсеместное внедрение этого не составило больших проблем. Стандарт также требует использования разъёмов разных цветов, для более простой идентификации их как производителем, так и сборщиком. Синий разъём предназначен для подключения к контроллеру, чёрный — к ведущему устройству, серый — к ведомому.

Скорость передачи данных для жёстких дисков с интерфейсом IDE - 133Мб/с, а пропускная способность шины PATA (IDE) в последней версии составляет около 1064 Мбит/с.

Особенности интерфейса SATA (где используется, какие ограничения присутствуют, скоростные характеристики, различие между версиями, применение в современной технике и развитие).

SATA (англ. Serial ATA) — последовательный интерфейс обмена данными с накопителями информации. SATA является развитием параллельного интерфейса ATA (IDE), который после появления SATA был переименован в PATA (Parallel ATA).

Разъём SATA-кабеля и разъёмы SATA на материнской плате

SATA использует 7-контактный разъём вместо 40-контактного разъёма у PATA. SATA-кабель имеет меньшую площадь, за счёт чего уменьшается сопротивление воздуху, обдуваемому комплектующие компьютера, упрощается разводка проводов внутри системного блока.

SATA-кабель за счёт своей формы более устойчив к многократному подключению. Питающий шнур SATA также разработан с учётом многократных подключений. Разъём питания SATA подаёт 3 напряжения питания: +12 В, +5 В и +3,3 В; однако современные устройства могут работать без напряжения +3,3 В, что даёт возможность использовать пассивный переходник со стандартного разъёма питания IDE на SATA. Ряд SATA-устройств поставляется с двумя разъёмами питания: SATA и Molex.

Стандарт SATA отказался от традиционного для PATA подключения по два устройства на шлейф; каждому устройству полагается отдельный кабель, что снимает проблему невозможности одновременной работы устройств, находящихся на одном кабеле (и возникавших отсюда задержек), уменьшает возможные проблемы при сборке (проблема конфликта Slave/Master устройств для SATA отсутствует), устраняет возможность ошибок при использовании нетерминированных PATA-шлейфов.

В отличие от PATA, стандарт SATA предусматривает горячую замену активного устройства (используемого операционной системой) (начиная с SATA Revision 1.0).

Ревизии SATA:

SATA 1.x

Первая ревизия интерфейса предусматривает частоту функционирования 1.5 ГГц, что обеспечивает полосу пропускания 1.5 Гбит/с. Около 20% отнимается на нужды системы кодирования типа 8b\10b, где в каждые 10 бит вкладывается ещё 2 бита служебной информации. Таким образом, максимальная скорость равняется 1.2 Гбит/с (150 Мб/с). Это совсем немного быстрее самой быстрой PATA/133, но намного лучшее быстродействие достигается в режиме AHCI, где работает поддержка NCQ (Native Command Queuing). Это значительно улучшает производительность в много-поточных задачах, но не все контроллеры поддерживают AHCI на первой версии SATA.

SATA 2.x

Частота функционирования была увеличена до 3.0 ГГц, что увеличило пропускную способность до 3.0 Гбит/с. Эффективная пропускная способность равняется 2.4 Гбит/с (300 Мб/с), то есть в 2 раза выше чем у SATA 1. Совместимость между первой и второй ревизией сохранилась. Интерфейсные кабели тоже были сохранены прежние и полностью совместимы между собой.

SATA 3.0

В июле 2008 года, SATA-IO представила спецификации SATA 3.0, с пропускной способностью 6 Гбит/с. Полный 3.0 стандарт был выпущен в мае 2009 года.

Эффективная пропускная способность составила 600Мб/с, а частота функционирования 6.0ГГц (то есть поднята только частота). Совместимость сохранилась как в методе передачи данных, так и в разъёмах и проводах; улучшено управление питанием.

Основной сферой применения, где требовалась такая пропускная способность – SSD (твёрдотельные) накопители. Для жёстких дисков, такая пропускная способность не требовалась. Выигрыш для них был в более высокой скорости передачи данных из кэш (DRAM-cache) памяти диска.

eSATA (External SATA) — интерфейс подключения внешних устройств, поддерживающий режим «горячей замены» (англ. Hot-plug). Был создан несколько позже SATA (в середине 2004). Основные особенности eSATA:

Разъёмы менее хрупкие и конструктивно рассчитаны на большее число подключений.

Требует для подключения два провода: шину данных и кабель питания. В новых спецификациях планируется отказаться от отдельного кабеля питания для выносных eSATA-устройств.

Длина кабеля увеличена до 2 м. Средняя практическая скорость передачи данных выше, чем у USB или IEEE 1394. Существенно снижается нагрузка на центральный процессор. Уменьшены требования к сигнальным напряжениям по сравнению с SATA.

Power eSATA

Изначально eSATA передаёт только данные. Для питания должен использоваться отдельный кабель. Компания MicroStar создала новый вид eSATA-разъёма, совместив eSATA (для данных) с USB (для питания). Новый вид разъёма имеет название Power eSATA.

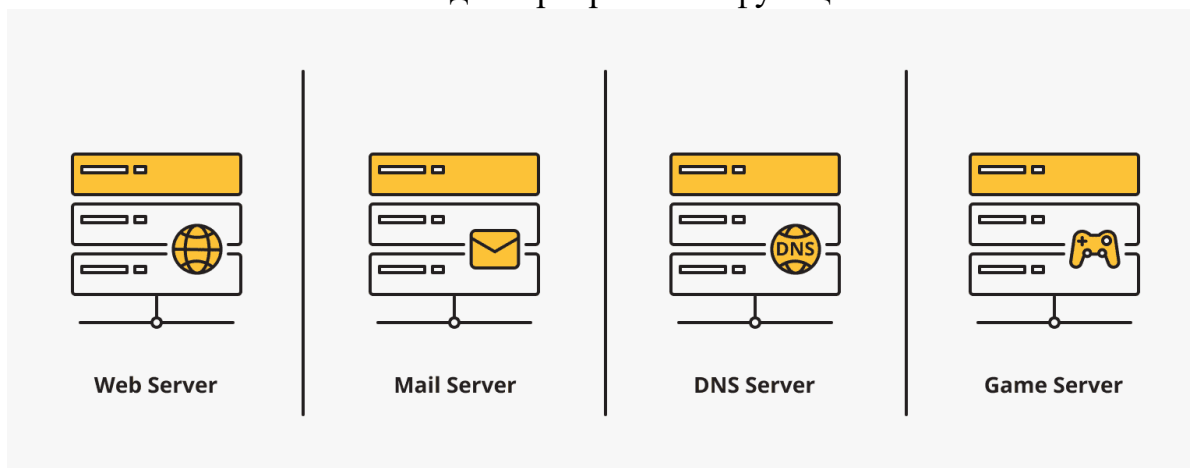


Интерфейс SAS (англ. Serial Attached SCSI) обеспечивает подключение по физическому интерфейсу, аналогичному SATA, устройств, управляемых набором команд SCSI. Обладая обратной совместимостью с SATA, он даёт возможность подключать по этому интерфейсу любые устройства, управляемые набором команд SCSI — не только HDD, но и сканеры, принтеры и др. По сравнению с SATA, SAS обеспечивает более развитую топологию, позволяя осуществлять параллельное подключение одного устройства по двум или более каналам. Также поддерживаются расширители шины, позволяющие подключить несколько SAS-устройств к одному порту.

SAS и SATA2 в первых редакциях были синонимами. Но, позже производители посчитали, что реализовывать SCSI полностью в настольных компьютерах нецелесообразно, поэтому мы сейчас наблюдаем такое разделение. К слову, такие высокие скорости, заложенные в стандарте SATA, на первый взгляд могут показаться излишними — обычный SATA HDD использует, в лучшем случае, 40-45 % пропускной способности шины. Однако работа с буфером винчестера происходит на полной скорости интерфейса.

Жёсткие диски с интерфейсом SATA применяются на данный момент практически во всех современных ПК и серверах, и продолжают развиваться.

2.1. Виды серверов и их функции



Веб-серверы

Веб-серверы отвечают за обработку HTTP-запросов и предоставление веб-контента пользователям через интернет. Они работают под управлением различных операционных систем, таких как Linux, Windows Server, BSD и другие. Основные функции веб-сервера включают:

- Обработка HTTP-запросов.
- Сервисные возможности, такие как статические страницы, динамические сайты, базы данных и т.д.
- Защита от несанкционированного доступа и DDoS-атак.

Почтовые серверы

Почтовые серверы обрабатывают входящую и исходящую электронную почту. Они также могут выполнять функции антиспама и антивирусной защиты.

Основные функции почтового сервера включают:

- Прием, передача и хранение электронной почты.
- Фильтрация спама и вирусов.
- Поддержка протоколов SMTP, POP3, IMAP.

Файловые серверы

Файловые серверы предоставляют централизованное хранилище файлов для совместного использования внутри сети. Они часто используются для хранения документов, медиафайлов и других данных. Основные функции файлового сервера:

- Хранение и управление данными.
- Обеспечение доступа к данным для авторизованных пользователей.
- Резервное копирование данных.

2.2. Установка, настройка и обновление операционных систем



Операционные системы являются основой для большинства серверных приложений. Процесс установки и настройки ОС включает следующие этапы:

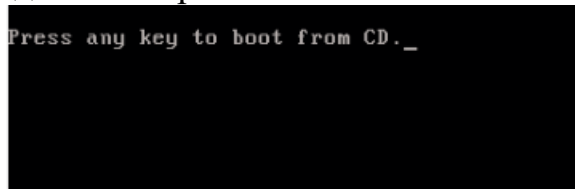
- Выбор и подготовка аппаратного обеспечения.
- Установка операционной системы.
- Настройка сетевых параметров.
- Инсталляция и настройка необходимых приложений и сервисов.
- Обновление операционной системы и установленного ПО.
- Создание резервных копий.

Установка ОС Windows с HDD, CD, Flash - накопителей

Разница в установке ОС Windows с HDD, CD, Flash - накопителей не имеет каких то особых различий. Но есть два момента на которых мы остановимся.

Первое - при включении компьютера в Биосе должна стоять загрузка с нужного нам носителя - с HDD, CD или Flash - накопителя. Конфигурирование приоритетов загрузки описано в пункте 3.1.2.1.

Второе - при загрузке с CD загрузчик ОС Windows проверяет наличие установленной системы на жестком диске компьютера. Если система найдена то на экран выдается запрос.



```
Press any key to boot from CD._
```

"Press any key to boot from CD." - Для загрузки с CD нажмите любую клавишу.

Этот момент важен тем, что при процесс установки ОС Windows требует перезагрузки компьютера. И если мы ставим систему с CD, то через 5 секунд после вывода данного сообщения начинается загрузка с жесткого диска. Если мы ставим ОС windows с HDD или Flash - накопителя, то при первой перезагрузке установщика надо будет зайти в биос и переключить загрузку компьютера на тот жесткий диск, на который мы ставим ОС.

Установка Windows .

После включения/перезагрузки компьютера, если на компьютере в этот момент уже установлена какая-либо операционная система Windows, то через какое-то время на экране мы увидим надпись «Press any key to boot from CD» (Нажмите на любую клавишу для загрузки с компакт-диска), нажимаем любую клавишу.

Сообщение будет ожидать нажатия только 5 секунд для входа в установку системы. Если началась загрузка текущей операционной системы, значит, возможность начать инсталляцию была упущена и следует заново перезагрузить компьютер для следующей попытки.

Затем появится экран установки базового программного обеспечения Windows XP, требующий вмешательства только в случае если вы планируете устанавливать систему на массив жестких дисков (RAID) или высокосортной диск SCSI.

Именно здесь следует нажать клавишу "F6", для установки дополнительных драйверов этих устройств, руководствуясь сообщениями в нижней строке экрана. В большинстве случаев такого вмешательства не требуется и следует просто дождаться экрана приветствия.

На экране приветствия вам будет предложено:

Установить Windows XP. Следует выбрать, нажав клавишу "ВВОД" ("Enter"), в случае новой установки или восстановления предыдущей копии Windows, с использованием графического интерфейса.

Восстановление Windows с помощью консоли восстановления. Следует выбирать опытным пользователям для восстановления системы с помощью DOS-команд, запускаемых из командной строки. Позволяет устранять мелкие ошибки системы без прохождения полной

процедуры установки. Наиболее часто используется для восстановления загрузочного сектора файловой системы и основной загрузочной записи (MBR); точечном копировании, переименовании или удалении папок и файлов операционной системы; создания и форматирования разделов на дисках.

Консоль восстановления вызывается клавишей "R".

В случае отказа от установки следует нажать клавишу "F3".

Выбираем первый пункт "Приступить к установке Windows XP" (даже если вы собираетесь переустанавливать систему), нажав клавишу ВВОД, после чего появиться окно с лицензионным соглашением, которое необходимо принять, что бы продолжить установку, нажав "F8".

Далее инсталлятор начинает поиск предыдущих копий Windows, установленных на вашем компьютере. Если таковые будут найдены, то вы увидите экран со списком этих систем и меню, в котором будет предложено:

Восстановить найденную копию Windows, нажав клавишу "R" . Выбрав этот пункт, вам придется пройти через полную процедуру установки системы, в процессе которой все системные файлы старой копии будут заменены новыми с компакт-диска. Все ваши данные,

настройки и установленные программы будут сохранены. Восстановление помогает в случае повреждения, удаления или подмены зараженными файлами, системных файлов Windows.

Установить новую копию Windows, нажав клавишу "ESC".

Окно со списком установленных систем вы не увидите, в случае если вы устанавливаете систему на новый компьютер/жесткий диск, а так же если предыдущая копия Windows имеет другую редакцию или сервис-пак.

Следующим шагом в установке является распределение дискового пространства под операционную систему. Это очень важный момент и отнестись к нему следует внимательно, а все действия выполнять очень осторожно.

С этого момента ход инсталляции может пойти двумя путями:

Вариант 1: У вас новый компьютер и жесткий диск никогда не был распределен. В таком случае перед вами возникнет окно следующего плана:

Размер неразмеченной области – это объем вашего жесткого диска и конечно совпадать с указанным в скриншоте абсолютно не должен. Для продолжения установки необходимо создать раздел на диске (системный раздел), в который в дальнейшем будет установлена ОС, и указать его размер. Как правило, для Windows XP и сопутствующего программного обеспечения, достаточно 40 – 60 Гб, но не менее 20 Гб. Нажав клавишу "C" в появившемся окне введите требуемый размер создаваемого раздела.

Размер необходимо указывать в мегабайтах. Рассчитывайте его исходя из того, что 1 Гб = 1024 Мб. Таким образом, если вы хотите отвести под системный раздел 60 Гб, в поле размера необходимо ввести число 61440.

Нажав клавишу "ВВОД" ("Enter") вы вернетесь к окну разбиения жесткого диска, где созданный раздел будет выделен отдельной строкой с указанием присвоенной буквы из латинского алфавита (как правило "C"), файловой системы – в нашем случае «новый (неформатированный)» и его размера. Ниже будет располагаться строка с оставшейся не распределенной областью, которую точно таким же способом вы сможете разбить на необходимое вам количество разделов. Правда, здесь этим заниматься совсем не обязательно, так как после установки это можно сделать средствами Windows.

Создав системный раздел, выделите его с помощью стрелок на клавиатуре и нажмите клавишу ВВОД, после чего вы увидите последнее диалоговое окно, в котором вам будет предложено его форматировать.

Смело выбирайте вариант быстрого форматирования, нажав ВВОД, так как во втором случае происходит проверка физической поверхности диска, что занимает довольно продолжительное время, тем более, если раздел имеет большой размер.

После выбора файловой системы начнется непосредственно установка Windows.

Вариант 2 - Если на вашем компьютере была установлена система. Тогда ваш жесткий диск уже был распределен на логические области, и вы увидите окно с перечислением всех найденных разделов.

Внимание! Все дальнейшие манипуляции с найденными разделами могут привести к потере ваших данных, так что будьте очень аккуратны в своих действиях. Если текущее разбиение жесткого диска вас не устраивает, то можно удалить существующие разделы полностью или частично, нажав клавишу D. Выбор нужного раздела осуществляется с помощью клавиш стрелок вверх и вниз. После удаления раздела, область, которую он занимал, становится неразмеченной, а все данные находившиеся на этом логическом диске удаляются. При удалении нескольких разделов, они превращаются в единую неразмеченную область, которую в дальнейшем вы сможете распределить, как вы пожелаете. Принцип распределения неразмеченного участка жесткого диска описан выше.

После всех перераспределений или в случае если существующая структура жесткого диска вас устраивает, вам остается только выбрать желаемый раздел, в который вы планируете установить систему и нажать клавишу ВВОД.

Если для установки ОС вы выбрали уже существовавший ранее раздел жесткого диска с существующими на нем данным, вам будет предложено на выбор несколько вариантов, как поступить далее. Осторожно, форматирование раздела в любой файловой системе приведет к потере данных, находившихся в нем! Система FA" является устаревшей и форматирование имеет смысл производить только в NTFS (быстрое предпочтительнее). Сделав выбор, нажмите "ВВОД" ("Enter") для начала форматирования и копирования системных файлов.

Если по каким-то причинам вы все же хотите сохранить информацию, находящуюся в выбранном вами разделе, то следует выбрать пункт «Оставить текущую файловую систему без изменений». В таком случае все данные находившиеся на нем будут не тронуты. Более того, если именно в этом разделе была установлена предыдущая копия Windows (наиболее вероятный вариант), то в таком случае инсталлятор вам выдаст предупреждение о том, что папка

«Windows» уже существует, предложив либо затереть существующую копию нажав , либо выбрать новую папку для установки. Здесь однозначно жмите , так как все равно старая папка с системой будет переименована автоматически и сохранена.

Следует отметить, что после такой установки, категорически рекомендуется произвести ручную чистку вашего системного раздела, а именно удаление большого количества дублирующих друг друга файлов. Дело в том, что установщик Windows, не только сохранит старую копию системы, но и все файлы существовавших в ней учетных записей. Из этого всего добра для вас возможно полезным будет папки «Мои документы», «Избранное» и «Рабочий стол». Все остальное окажется бесполезным мусором, занимающим гигабайты места на жестком диске. Именно поэтому предпочтительнее позаботиться о сохранении ваших данных заранее, а новую систему устанавливать в чистый раздел, предварительно отформатированный.

На этом ветвления инсталлятора заканчиваются, и дальнейшая установка проходит линейно. После выбора раздела жесткого диска для установки новой операционной системы начинается копирование основных системных файлов Windows.

По завершению копирования произойдет перезагрузка компьютера, где вам не нужно ничего делать, а лишь дождаться появления экрана установщика уже с графической оболочкой.

Далее открывается окно, в котором можно изменить региональные настройки и язык ввода. По умолчанию уже в качестве местонахождения установлена Россия и русский язык. Так что без надобности ничего менять не надо, нажимаем "Далее".

В следующем окне необходимо ввести имя пользователя (ваше имя) и организации (необязательно). Нажимаем "Далее".

Для дальнейшего продолжения установки в окне ввода ключа, необходимо ввести серийный номер Windows с лицензионной наклейки.

Далее необходимо ввести имя вашего компьютера, под которым он будет виден в сети, используя только латинские буквы. Ввод пароля администратора можно отложить на потом.

В окне настройки времени и даты, при необходимости меняем время, дату и указываем нужный часовой пояс. Нажимаем на кнопку "Далее".

Следующие два окна вы увидите только в том случае, если в дистрибутиве Windows XP содержится драйвер для вашей сетевой карты.

Здесь не следует ничего менять, оставив выбранной опцию «Обычные параметры», впрочем, так же как и в следующем, где название рабочей группы/домена целесообразней выбрать после установки.

После нажатия кнопки "Далее" начнется окончательная фаза установки, а нам лишь останется только дождаться ее окончания. Через несколько минут произойдет автоматическая перезагрузка компьютера, после которой начнется первый запуск новой операционной системы.

При начальном запуске Windows мы увидим еще несколько диалоговых окон. Первым из них будет «Параметры экрана», где нужно просто нажать кнопку "ОК".

После автоматической настройки разрешения экрана, Windows попросит вас подтвердить их, что и следует сделать, нажав «ОК».

На экране приветствия настраивать нечего, поэтому просто жмем "Далее".

Следующим шагом станет возможность выбора параметров автоматического обновления Windows, предназначенного регулярно проверять через сеть интернет наличие всевозможных исправлений безопасности системы, критических обновлений и сервис-паков на официальном сайте технической поддержки. Включение автоматического обновления является желательным, но на этом этапе необязательным, так как более гибкую настройку этого параметра вы сможете выполнить после установки из панели управления.

Если во время установки были установлены драйверы сетевой карты, то вы увидите еще два окна: первое – проверки и настройки подключения к интернету, которое стоит пропустить и второе - регистрация системы, которую так же лучше отложить на потом.

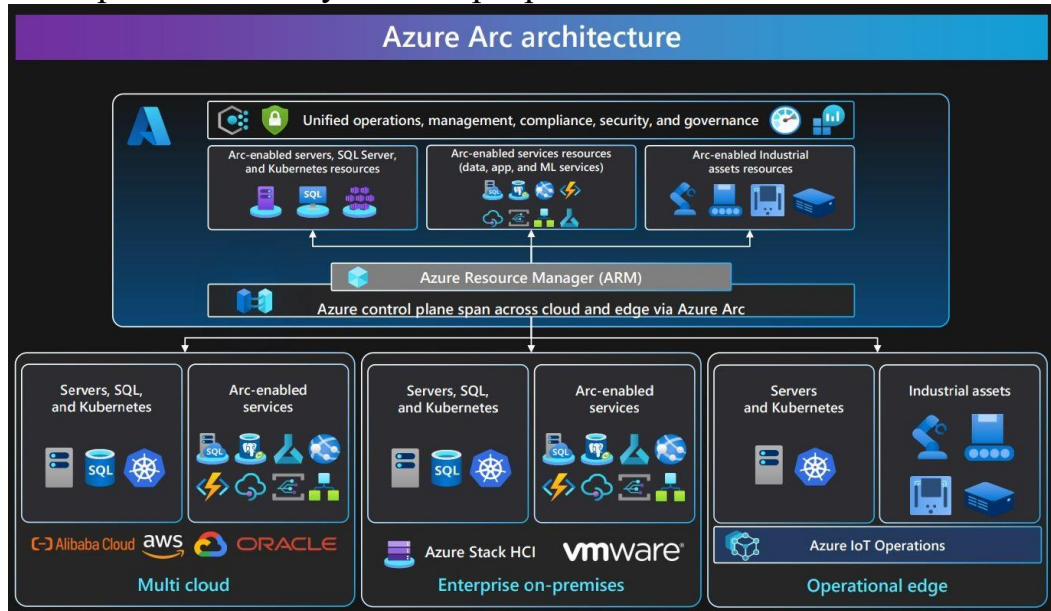
Последним параметром, который вам придется ввести для окончательной загрузки Windows, будет имя учетной записи пользователя, под которой вы будете работать в системе. Заполните поле "Имя вашей учетной записи". Если пользователей много, то в последствии их можно добавить через "Панель управления" - "Учетные записи пользователей".

В завершении вы увидите окно, сообщающее об окончании установки операционной системы.

На этом установку Windows можно считать законченной и после нажатия кнопки "Готово" наконец мы увидим рабочий стол системы.

Сразу же после ее завершения, следует установить все необходимые драйверы установленных устройств, после чего можно приступить к установке программного обеспечения.

2.3. Управление доступом к серверам



Управление доступом к серверам является ключевым аспектом безопасности серверной инфраструктуры. Основные методы управления доступом включают:

- Аутентификация и авторизация пользователей.
- Разграничение прав доступа на уровне пользователей и групп.
- Использование многофакторной аутентификации (MFA).
- Мониторинг и аудит действий пользователей.

Современные системы управления серверами предлагают множество инструментов для реализации перечисленных методов, что позволяет эффективно контролировать доступ к серверам и защищать их от несанкционированных действий.

Глава 3. Сетевое администрирование

3.1. Основы сетевых технологий



Сетевые технологии являются фундаментом для обмена информацией между устройствами в рамках компьютерной сети. Основные компоненты сетевой архитектуры включают:

- Хосты: конечные устройства, такие как компьютеры, смартфоны, серверы и принтеры.
- Маршрутизаторы: оборудование, которое направляет пакеты данных между различными сегментами сети.
- Коммутаторы: устройства, соединяющие хосты в пределах одной локальной сети.
- Шлюзы: промежуточное оборудование, позволяющее устройствам взаимодействовать через различные протоколы и сети.
- Брандмауэры: средства защиты сети от несанкционированного доступа.

Основные сетевые протоколы включают:

- IP (Internet Protocol) - основной протокол для адресации и маршрутизации пакетов данных.

- TCP (Transmission Control Protocol) - протокол, отвечающий за гарантированную доставку данных.
- UDP (User Datagram Protocol) - упрощенный вариант передачи данных без гарантии доставки.
- DNS (Domain Name System) - система преобразования имен доменов в IP-адреса.

Примеры сетевых топологий включают:

- Звезда - все устройства подключены к центральному коммутатору.
- Шина - устройства подключены последовательно друг к другу.
- Кольцо - данные передаются по кругу от одного устройства к другому.

Важно отметить, что выбор топологии зависит от требований к производительности, надежности и масштабируемости сети.

3.2. Настройка сетевого оборудования



Настройка сетевого оборудования включает в себя ряд шагов:

- Установка и настройка сетевых устройств (маршрутизаторов, коммутаторов, брандмауэров).
- Настройка IP-адресов и масок подсетей для устройств.
- Определение правил маршрутизации для направления трафика.
- Создание VLAN (Virtual Local Area Networks) для разделения сети на логические сегменты.

- Внедрение протоколов качества обслуживания (QoS) для приоритезации трафика.
- Настройка политики безопасности, включая фильтрацию контента и ограничение доступа.

Для упрощения этих задач используются специализированные инструменты, такие как командные оболочки, графические интерфейсы управления (GUI), а также системы управления сетью (например, Cisco Network Manager).

3.3. Wi-Fi точка доступа.

Всё больше и больше клиентов используют в своей работе технологию беспроводной передачи данных – Wi-Fi. В этой статье рассматриваются некоторые режимы работы и варианты использования устройств, работающих с данной технологией.

Что такое беспроводная (Wi-Fi) точка доступа.

Беспроводная точка доступа (англ. *Wireless Access Point*, WAP) — это беспроводная базовая станция, предназначенная для обеспечения беспроводного доступа к уже существующей сети (беспроводной или проводной) или создания новой беспроводной сети.

Три основных режима работы точки доступа – режим «точка доступа».

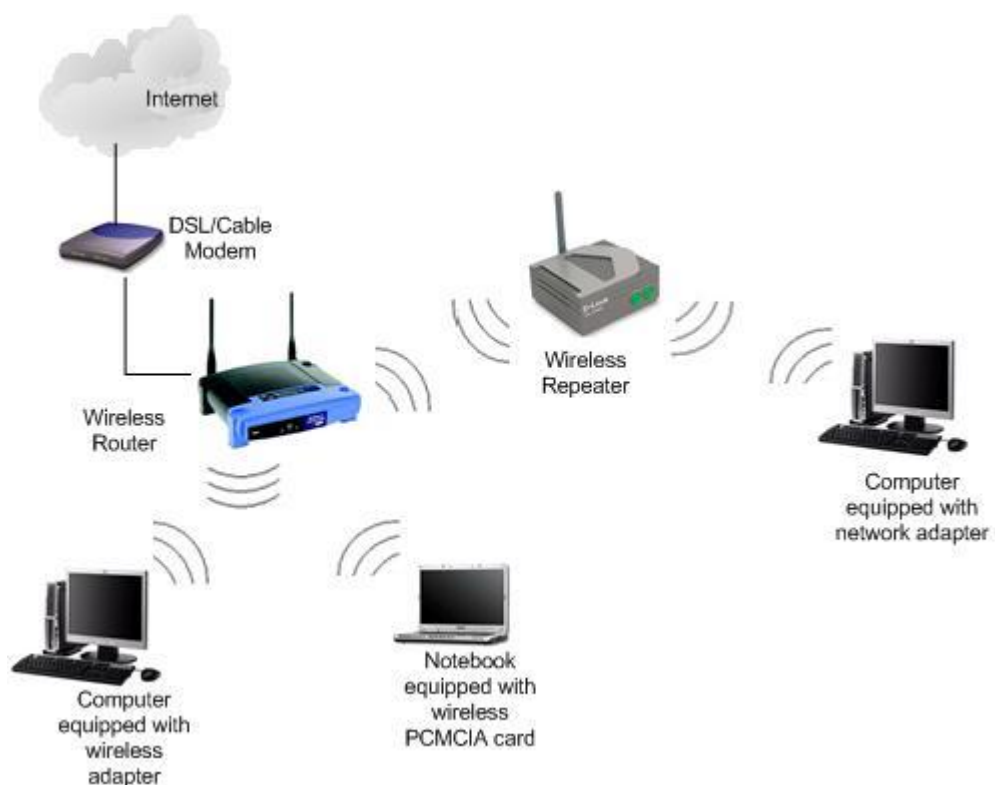
В этом режиме устройство будет работать в качестве обычной беспроводной точки доступа Wi-Fi, т.е. в этом режиме предоставлена возможность клиентам (ноутбуки, настольные компьютеры, КПК, коммуникаторы, смартфоны и др.) получать беспроводной доступ к устройству (при наличии у клиентских устройств беспроводного адаптера Wi-Fi 802.11b/g/n) для подключения к сети Интернет и к ресурсам проводной сети. Режим Access Point (Точка Доступа) - самый простой и самый часто используемый режим работы беспроводной точки доступа.



Беспроводная точка доступа имеет идентификатор SSID (Service Set Identifier, идентификатор беспроводной сети), который используется для идентификации беспроводной сети (определяет название сети), и именно его видит беспроводной адаптер при просмотре доступных беспроводных сетей и затем использует для подключения.

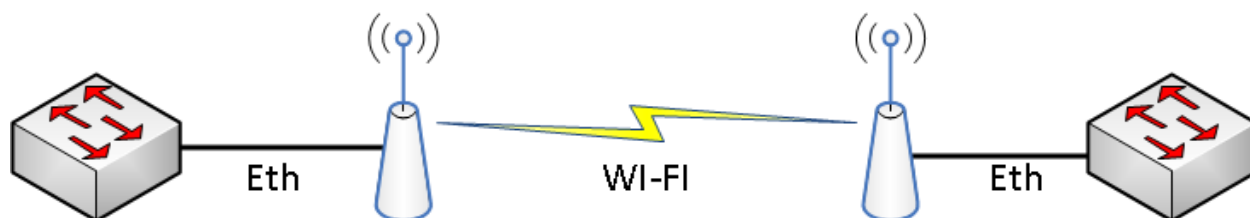
Три основных режима работы точки доступа – режим «репитер» (ретранслятор).

Функционируя в режиме беспроводного репитера, точка доступа расширяет диапазон действия беспроводной сети посредством повтора сигнала удаленной точки доступа. Для того чтобы точка доступа могла выполнять функции беспроводного расширителя радиуса действия другой точки доступа, в её конфигурации необходимо указать Ethernet MAC-адрес удаленной точки доступа. В данном режиме беспроводные клиенты могут обмениваться данными с точкой доступа. Работает как правило только с точками доступа построенных на одинаковых чипах.



Три основных режима работы точки доступа – режим «мост».

Беспроводной мост point-to-point - Режим Point-to-Point / Wireless Bridge позволяет беспроводной точке обмениваться данными с другой точкой доступа, поддерживающей режим беспроводного моста point-to-point. Однако имейте в виду, что большинство производителей используют свои собственные оригинальные настройки для активации режима беспроводного моста в точке доступа. Обычно данный режим используется для беспроводного соединения аппаратуры в двух разных зданиях. Беспроводные клиенты не могут обмениваться данными с точкой доступа в этом режиме. Работает как правило только с одинаковыми точками доступа. Работоспособность с разными устройствами невозможна ввиду отсутствия стандартов на технологию WDS.



Варианты использования Wi-Fi точек доступа (примеры).

1. Использование точки доступа для предоставления доступа к сети (интернету).

Самый часто встречающийся вариант использования точки доступа Wi-Fi. Точка доступа подключена к домашней (корпоративной) сети и предоставляет прямой (без пароля, редко) или защищённый (с паролем) доступ к интернету. Все подключающиеся устройства получают ip-адрес в той же подсети и получают доступ в интернет в соответствии с общими правилами предприятия.

2. Использование точки доступа для предоставления гостевого доступа.

Точка доступа так же предоставляет доступ к сети (интернету), закрыта паролем, но все устройства, подключающиеся к ней, получают адрес в другой подсети, и не имеют доступа в общую сеть предприятия.

3. Использование точек доступа для связи двух удалённых офисов (подразделений).

Точки доступа расположены в пределах видимости друг друга и настроены на трансляцию данных между друг другом, например, для организации видеонаблюдения с удалённого склада при невозможности связать склад с основным офисом через проводной канал.

4. Использование точки доступа как ретранслятора.

Применяется при необходимости передачи Wi-Fi сигнала на расстояние, большее чем позволяет одна точка (либо при ограничении сигнала препятствиями, стенами и пр.).

3.4. Обеспечение безопасности сети



Задача обеспечения безопасности сети включает в себя защиту от различных видов угроз:

- Фишинг и социальная инженерия.
- Вредоносное ПО и вирусы.

- Неавторизованный доступ к ресурсам сети.
- Манипуляции с конфиденциальными данными.

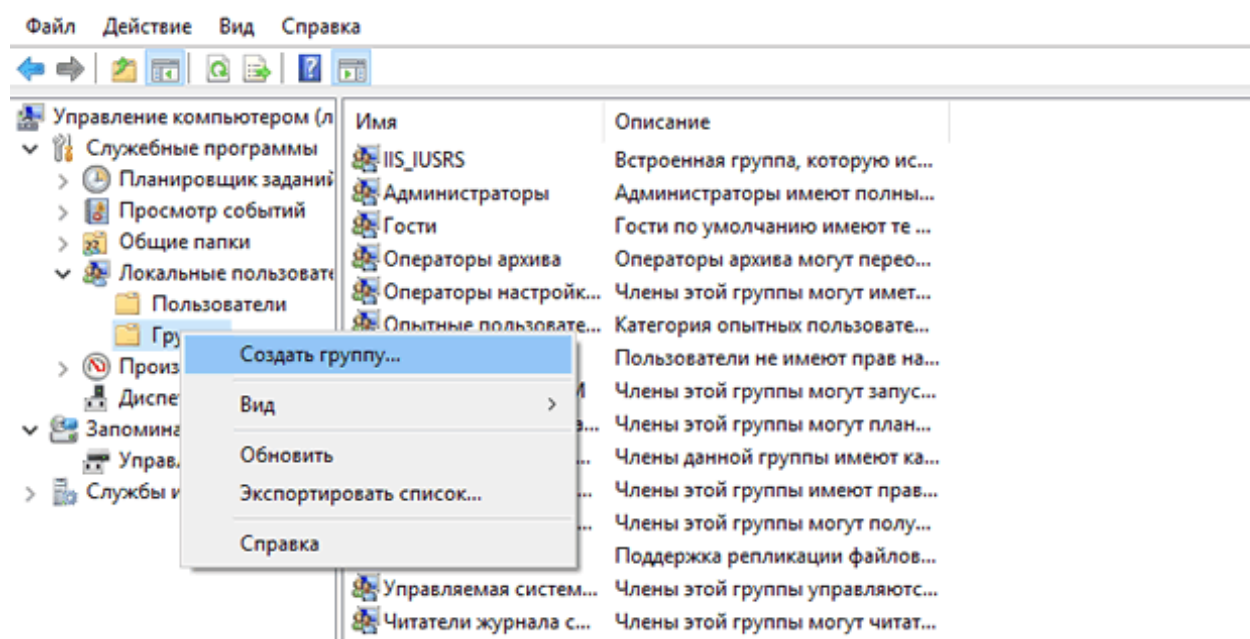
Способы обеспечения безопасности включают:

- Использование антивирусного ПО и средств защиты от вредоносного ПО.
- Внедрение межсетевых экранов (брандмауэр) и систем обнаружения вторжений (IDS/IPS).
- Реализация политик доступа, включая аутентификацию и авторизацию пользователей.
- Регулярное обновление программного обеспечения и систем безопасности.
- Обучение пользователей основам кибербезопасности.

Современные сети должны быть гибкими, надежными и защищенными, чтобы соответствовать растущим требованиям бизнеса и обеспечивать безопасность информации.

Глава 4. Управление пользователями и группами

4.1. Создание и управление учетными записями пользователей



Обычный доступ – это очень хороший тип учётной записи для человека, который только-только начал постигать компьютерный мир, то есть для начинающего. Работая под учётной записью пользователя с обычным доступом, вы сможете устанавливать некоторые программы, а вот антивирусную программу установить не сможете, для этого вам понадобится знать пароль администратора компьютера или войти в операционную систему под учётной записью администратора.

Администратор – опытный пилот, берущий на себя полное управление современным самолётом под названием Windows и понимающий всю ответственность за это. Пользователь с правами администратора может совершать все фигуры высшего пилотажа, включая сложнейшую «Кобру». Он может изменять любые настройки операционной системы, включая редактирование критически важных значений реестра и редактирование настроек влияющих на всех пользователей в системе. Так же он несёт ответственность за других участников полёта (других пользователей ПК).

Гость – изначально встроенная учетная запись, которую не нужно создавать. Применяют для пьяных гостей, желающих оттянуться на вашем компьютере во время гулянки. А если серьёзно, то она специально придумана для временного доступа к компьютеру и сильно ограничена в правах. Работая под этой учётной записью, вы никогда ничего не испортите в вашей операционной системе, но она сильно понизит ваш уровень безопасности, поэтому советую вам её включать только в случае необходимости.

Роль - совокупность прав доступа на объекты компьютерной системы.

Формирование ролей призвано определить четкие и понятные для пользователей компьютерной системы правила разграничения доступа. Ролевое

разграничение доступа позволяет реализовать гибкие, изменяющиеся динамически в процессе функционирования компьютерной системы правила разграничения доступа.

Такое разграничение доступа является составляющей многих современных компьютерных систем. Как правило, данный подход применяется в системах защиты СУБД, а отдельные элементы реализуются в сетевых операционных системах. Ролевой подход часто используется в системах, для пользователей которых четко определен круг их должностных полномочий и обязанностей. Группа доступа – группа, предназначенная для обеспечения каждому пользователю права доступа к элементам информационной системы.

Группы облегчают управление контролем доступа на уровне ресурса, позволяя задать и поддерживать управление доступом для групп, а не для отдельных пользователей. Роль, напротив, подразумевает набор разрешений на доступ к ресурсу, которые основаны на определениях роли (т.е. отношениях роли к поставленной задаче и отношениях роли к операции, которую нужно выполнить).

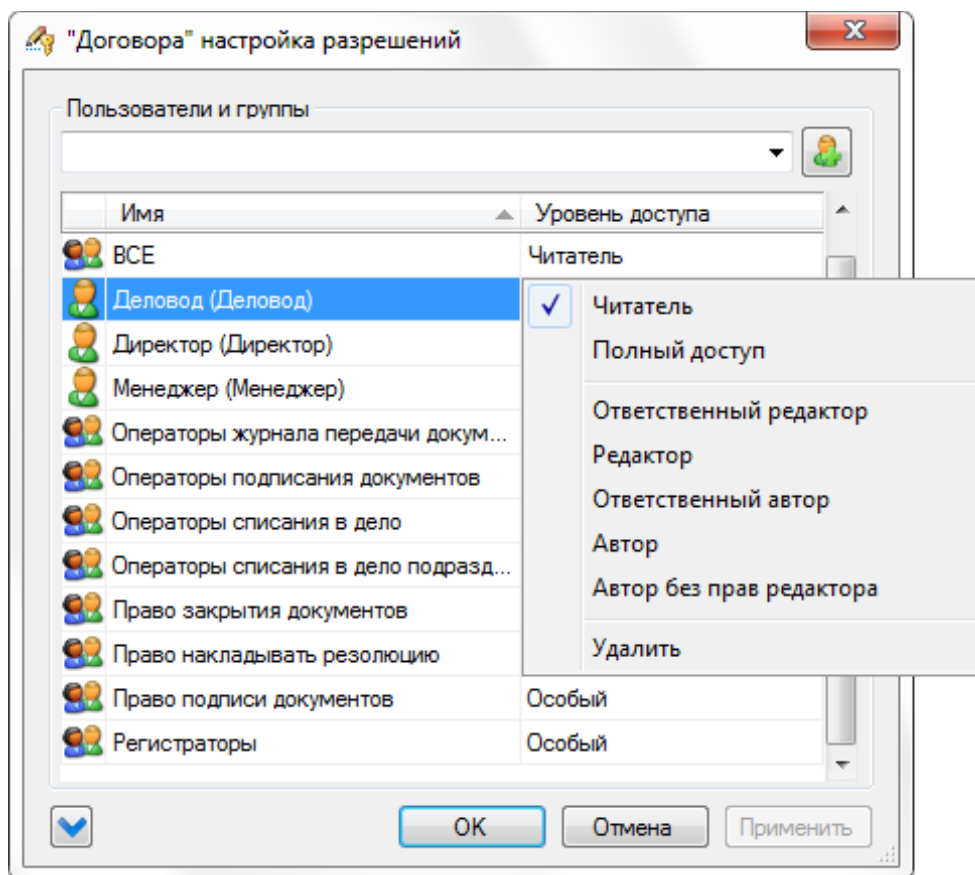
Создание и управление учетными записями пользователей является важной частью системного администрирования. Этот процесс включает в себя следующие шаги:

- Регистрация нового пользователя: добавление новой учетной записи пользователя в систему, включая имя пользователя, пароль и права доступа.
- Изменение учетной записи: изменение имени пользователя, пароля или других параметров учетной записи.
- Деактивация учетной записи: удаление доступа пользователя к системе путем деактивации его учетной записи.
- Удаление учетной записи: полное удаление учетной записи и связанных с ней данных из системы.

Для удобства управления учетными записями могут использоваться специализированные инструменты, такие как Active Directory в Windows или LDAP в Unix-подобных системах. Эти инструменты позволяют централизованно

управлять учетными данными, применять групповые политики и автоматизировать многие административные задачи.

4.2. Назначение прав и разрешений



Права и разрешения определяют, какие действия пользователь может выполнять в системе. Основные типы прав включают:

- Чтение: право просматривать информацию.
- Запись: право изменять информацию.
- Исполнение: право запускать программы и исполнять команды.
- Администраторские права: полный доступ к системе, включая возможность изменения системных настроек и файлов.

Назначение прав осуществляется путем создания групп пользователей и назначения этим группам определенных прав и привилегий. Например, группа "Администраторы" может иметь полный доступ ко всем ресурсам системы, тогда как группа "Пользователи" будет иметь ограниченные права.

4.3. Обеспечение безопасности доступа пользователей



Обеспечение безопасности доступа пользователей включает меры по защите учетных записей от несанкционированного доступа. Основные методы включают:

- Сложные пароли: использование длинных и сложных паролей, которые трудно угадать или подобрать.
- Двухфакторная аутентификация (2FA): дополнительный шаг проверки личности пользователя, например, через SMS-код или приложение-аутентификатор.
- Лимиты на количество попыток входа: ограничение числа неудачных попыток входа в систему для предотвращения брутфорс-атак.
- Парольные политики: обязательное использование комбинаций букв, цифр и специальных символов, а также регулярная смена паролей.
- Шифрование данных: защита важных данных с помощью шифрования, чтобы даже при утечке они были нечитаемыми для злоумышленников.

Эти меры помогают минимизировать риски взлома учетных записей и обеспечить безопасность доступа пользователей к системе.

Глава 5. Системный мониторинг и диагностика

5.1. Инструменты системного мониторинга



Системный мониторинг играет ключевую роль в управлении и обслуживании ИТ-инфраструктуры. Основные инструменты системного мониторинга включают:

- SNMP (Simple Network Management Protocol): стандартный протокол для сбора данных о состоянии сетевых устройств и служб.
- Zabbix: популярная система мониторинга, поддерживающая широкий спектр платформ и способная собирать разнообразные метрики и оповещать о проблемах.
- Prometheus: платформа для мониторинга и анализа времени исполнения (time series), известная своей гибкостью и масштабируемостью.
- Graphite: система для сбора и отображения временных рядов, часто используется вместе с инструментами типа StatsD для получения подробных метрик.
- Logstash: инструмент для сбора, обработки и анализа логов, часто интегрируется с Elasticsearch и Kibana для построения дашбордов и отчетов.

Эти инструменты позволяют системным администраторам следить за состоянием серверов, сетей, приложений и других компонентов инфраструктуры, а также оперативно реагировать на возникающие проблемы.

5.2. Обнаружение и устранение неисправностей

Выберите дополнительные параметры для: Windows 7
(Выберите нужный элемент с помощью клавиш со стрелками.)

Устранение неполадок компьютера

Безопасный режим

Безопасный режим с загрузкой сетевых драйверов

Безопасный режим с поддержкой командной строки

Ведение журнала загрузки

Включение видеорежима с низким разрешением (640x480)

Последняя удачная конфигурация (дополнительно)

Режим восстановления служб каталогов

Режим отладки

Отключить автоматическую перезагрузку при отказе сист

Отключение обязательной проверки подписи драйверов

Диагностика и устранение неполадок в ИТ-системе включает несколько этапов:

- Локализация проблемы: определение источника проблемы, будь то аппаратная неисправность, программный сбой или проблема с сетью.
- Анализ данных: использование собранных метрик и логов для понимания причины проблемы.
- Исправление: применение соответствующих мер для устранения проблемы, таких как обновление ПО, замена оборудования или настройка конфигурации.

- Тестирование и проверка: повторное тестирование исправленной системы для подтверждения того, что проблема была решена.

Для ускорения процесса диагностики и уменьшения времени простоя применяются такие практики, как журналирование всех значимых событий, сбор и архивирование логов и использование инструментов автоматического анализа данных.

5.3. Резервное копирование и восстановление данных



Резервное копирование и восстановление данных являются неотъемлемой частью любого плана аварийного восстановления. Основные шаги включают:

- Планирование: определение частоты резервного копирования, типов данных, которые необходимо защитить, и критериев восстановления.
- Создание резервных копий: регулярное создание копий важных данных, предпочтительно в несколько мест для обеспечения избыточности.
- Хранение резервных копий: использование безопасных носителей и удаленных хранилищ для защиты от физических повреждений и потерь данных.
- Восстановление: периодическая проверка возможности восстановления данных из резервной копии, а также быстрое восстановление данных в случае необходимости.

Инструменты для резервного копирования и восстановления данных включают:

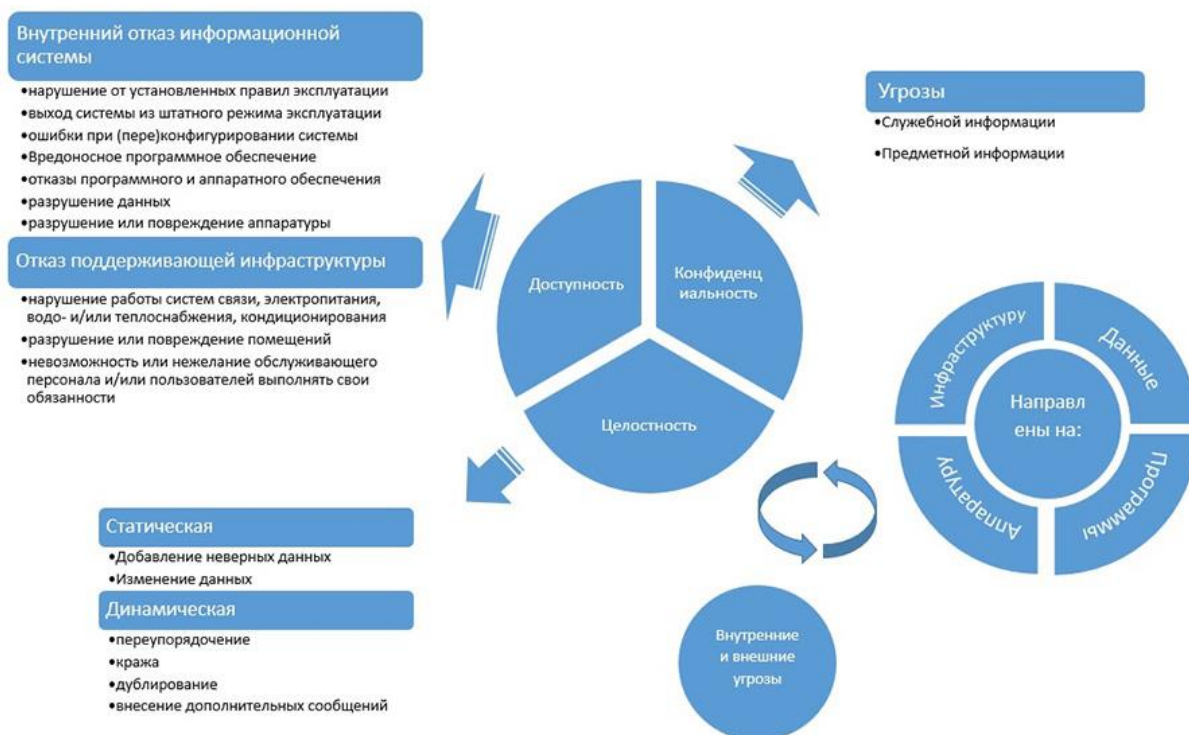
- Rsync: утилита для синхронизации и резервного копирования файлов.
- Bacula: свободное ПО для резервного копирования и восстановления.
- Cloudberry Backup: инструмент для резервного копирования в облако.

Резервные копии служат гарантией того, что важные данные будут сохранены и доступны в случае возникновения катастрофических событий

Глава 6. Безопасность информационных систем

6.1. Угрозы безопасности информационных систем

КЛАССИФИКАЦИЯ ВИДОВ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



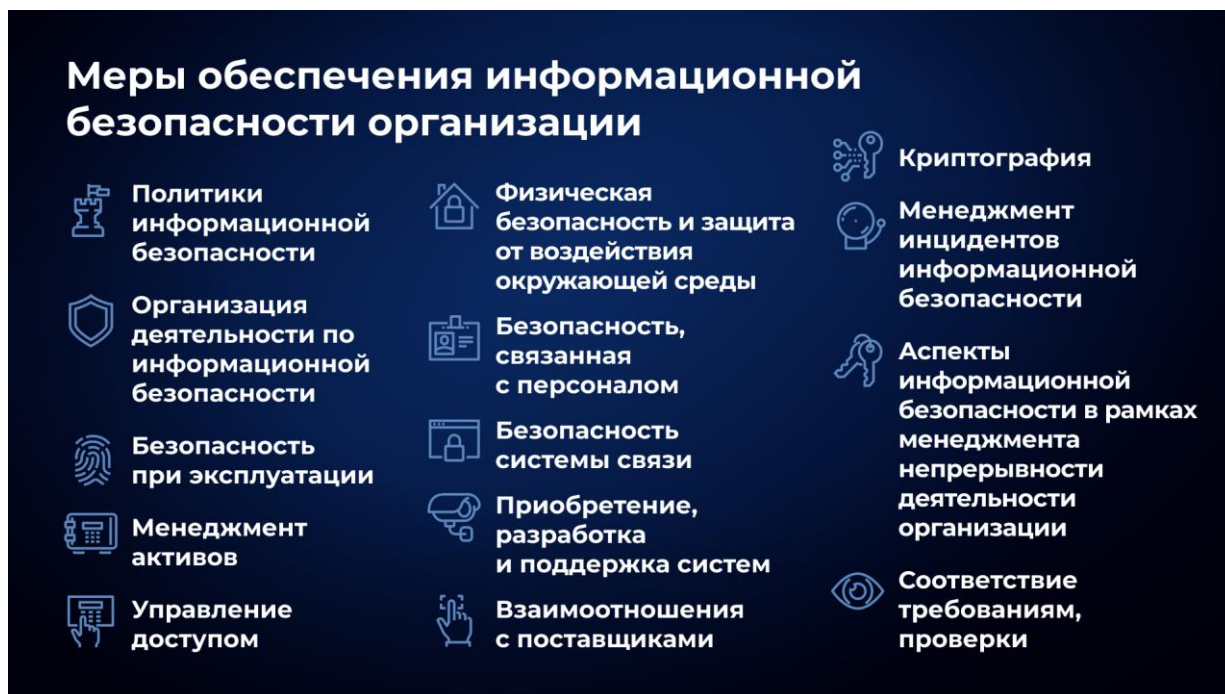
Безопасность информационных систем подвержена различным угрозам, которые могут привести к потере данных, нарушению работоспособности систем и ущербу для бизнеса. Основные угрозы включают:

- Вредоносное ПО: вирусы, троянские программы, черви и другие виды вредоносного ПО, которые могут повредить или украсть данные.

- Фишинг и социальная инженерия: мошеннические методы, направленные на получение конфиденциальной информации, используя психологические манипуляции.
- Неавторизованный доступ: попытки получить доступ к системам без должных полномочий.
- Сбои в работе систем: отказ оборудования, программные ошибки, человеческий фактор, которые могут нарушить нормальное функционирование систем.
- Киберпреступность: организованные группы, атакующие информационные системы с целью кражи денег, личных данных или для нанесения другого вреда.

Каждая из этих угроз требует особого подхода к защите и предотвращению возможных негативных последствий.

6.2. Меры по обеспечению безопасности



Для защиты информационных систем от угроз безопасности применяются следующие меры:

- Шифрование данных: использование криптографических алгоритмов для защиты конфиденциальных данных.
- Парольная политика: строгие правила для создания и смены паролей, использование двухфакторной аутентификации.

- Антивирусное ПО и сканеры уязвимостей: регулярное сканирование систем на наличие вредоносного ПО и уязвимостей.
- Межсетевые экраны и системы обнаружения вторжений: контроль и фильтрация трафика, предотвращение несанкционированного доступа.
- Резервное копирование данных: создание регулярных резервных копий важных данных для быстрого восстановления в случае потери или повреждения.
- Обучение сотрудников: повышение осведомленности персонала о рисках и методах защиты от угроз.

Эти меры помогают снизить риск успешных кибератак и минимизировать ущерб от них.

6.3. Мониторинг безопасности и реагирование на инциденты



Мониторинг безопасности включает в себя постоянное наблюдение за системой и обнаружение подозрительной активности. Основные этапы мониторинга:

- Сбор данных: использование систем мониторинга для сбора информации о состоянии системы.
- Анализ данных: обработка и анализ собранных данных для выявления аномалий и потенциальных угроз.
- Оповещение: уведомление ответственных лиц о возникновении инцидентов безопасности.
- Реакция: принятие мер для нейтрализации угрозы и минимизации ущерба.

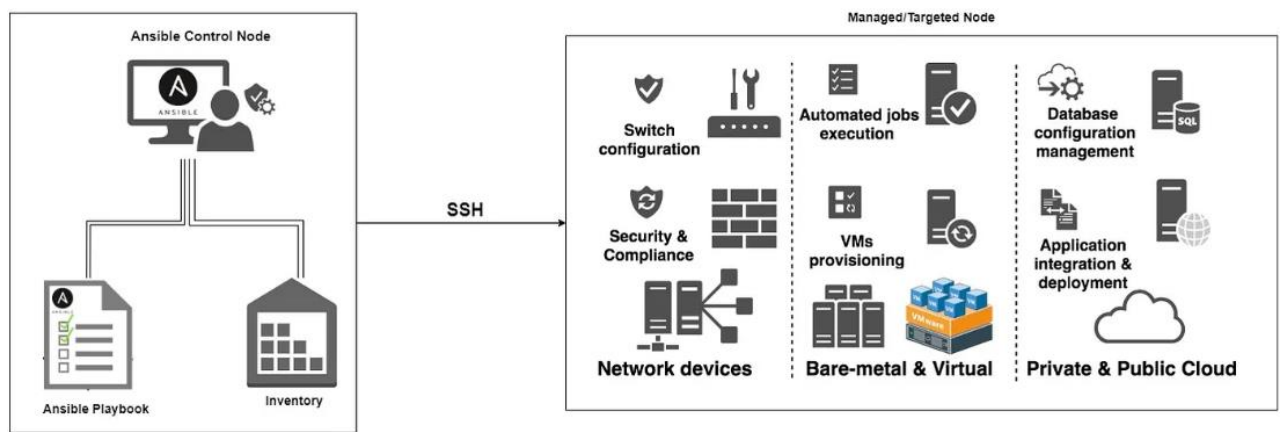
Реагирование на инциденты безопасности включает:

- Оценку серьезности инцидента.

- Определение источника угрозы.
- Принятие мер по изоляции и устранению угрозы.
- Документирование инцидента для последующего анализа и предотвращения подобных ситуаций в будущем.

Глава 7. Инструменты системного администрирования

7.1. Автоматизация задач

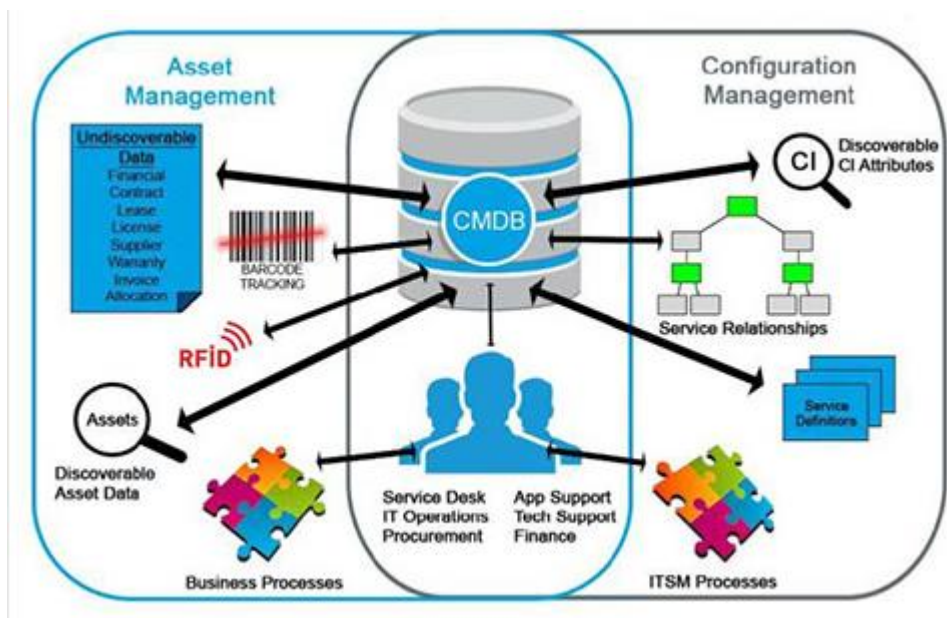


Автоматизация задач системного администрирования помогает снизить нагрузку на администраторов, повысить эффективность и уменьшить вероятность ошибок. Основные инструменты для автоматизации включают:

- **Ansible:** инструмент для автоматизации задач на основе YAML-скриптов. Он позволяет легко разворачивать, конфигурировать и управлять серверами и приложениями.
- **Chef:** система управления конфигурациями, которая использует декларативный подход к описанию инфраструктуры. Она поддерживает множество платформ и языков программирования.
- **Puppet:** еще одна система управления конфигурациями с возможностью автоматического развертывания и конфигурирования серверов и приложений.
- **SaltStack:** мощный инструмент для управления конфигурацией и автоматизации, известный своей высокой скоростью и гибкостью.

Эти инструменты позволяют создавать скрипты и сценарии для автоматизации повторяющихся задач, таких как установка и настройка операционных систем, обновление ПО, управление учетными записями пользователей и многое другое.

7.2. Системы управления конфигурациями



Системы управления конфигурациями помогают централизовать управление конфигурационными файлами и параметрами системы. Основные преимущества таких систем:

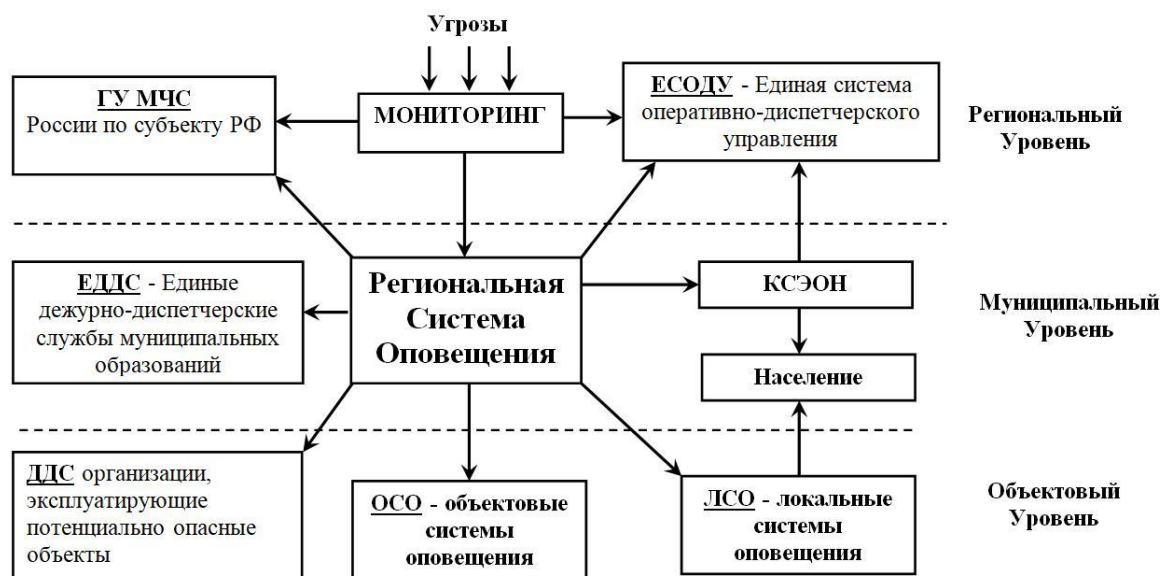
- Централизованное управление: все изменения производятся в одном месте, что облегчает контроль версий и аудит изменений.
- Совместная работа: несколько администраторов могут работать одновременно над одним проектом, избегая конфликтов и дублирования усилий.
- Повторяемость: возможность воспроизводить определенные конфигурации на множестве серверов, что особенно важно при масштабировании инфраструктуры.

Примеры систем управления конфигурациями:

- Chef
- Puppet
- SaltStack

Каждый из этих инструментов предлагает свой уникальный набор возможностей и подходит для различных сценариев использования.

7.3. Системы мониторинга и оповещения



Для мониторинга состояния систем и уведомления администраторов о критических событиях используются специальные системы мониторинга. Основные функции таких систем:

- Сбор метрик производительности и состояния систем.
- Отслеживание пороговых значений и триггеров для оповещений.
- Генерация отчетов и дашбордов для анализа исторических данных.
- Оповещение администраторов через различные каналы связи (email, SMS, мессенджеры).

Примеры систем мониторинга:

- Zabbix
- Nagios
- Prometheus

Использование систем мониторинга позволяет быстро обнаруживать и решать проблемы, предотвращая простои и минимизируя влияние на бизнес-процессы.

Глава 8. Практическое применение системного администрирования

8.1. Применение системного администрирования в различных отраслях

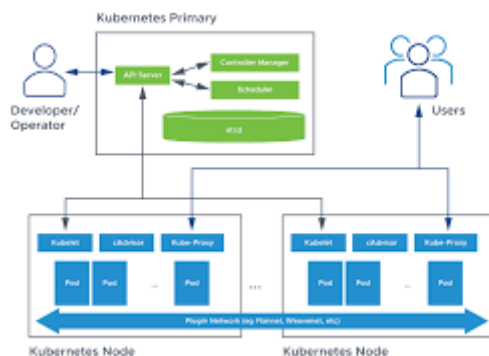


Системное администрирование находит широкое применение в различных сферах деятельности. Вот некоторые примеры:

- Финансовый сектор: управление банковскими системами, обеспечение безопасности транзакций и соответствие регуляторным требованиям.
- Здравоохранение: поддержка медицинских информационных систем, защита персональных данных пациентов.
- Образование: администрирование учебных сетей, обеспечение доступа к образовательным ресурсам.
- Государственное управление: обслуживание государственных информационных систем, соблюдение законодательных норм.
- Транспорт и логистика: мониторинг транспортных средств, управление складами и поставками.

Во всех этих случаях системное администрирование играет ключевую роль в обеспечении стабильной и безопасной работы информационных систем.

8.2. Управление крупномасштабными ИТ-системами



Управление крупными ИТ-инфраструктурами требует особых подходов и инструментов. Основные аспекты:

- Масштабируемость: способность системы расширяться и адаптироваться к увеличению нагрузки.
- Высокая доступность: минимизация времени простоя за счет резервирования и кластеризации компонентов.
- Безопасность: усиленная защита от внешних и внутренних угроз, включая регулярные аудиты и тесты на проникновение.
- Автоматизация: использование систем автоматизации для управления конфигурациями и мониторингом.
- Документация: тщательная документация всех процессов и процедур для обеспечения прозрачности и контроля.

Для управления такими системами часто используются специализированные решения, такие как OpenStack, Kubernetes и AWS, которые позволяют управлять большим количеством серверов и приложений в едином пространстве.

8.3. Карьерный рост в системном администрировании



Путь карьерного роста в сфере системного администрирования может быть разным в зависимости от индивидуальных интересов и целей. Некоторые возможные пути развития:

- Специализация в определенной области, например, безопасность, сети или облачные технологии.
- Переход на руководящие позиции, такие как менеджер по инфраструктуре или директор по ИТ.
- Работа в качестве независимого консультанта или предпринимателя в области ИТ-услуг.
- Переход в смежные области, такие как DevOps, где требуется сочетание навыков разработки и администрирования.

Важную роль в развитии карьеры играют непрерывное обучение, сертификация и участие в профессиональных сообществах.

Заключение

В данном дипломном проекте были рассмотрены основы системного администрирования, включая понятия, задачи и роли системного администратора, а также основные функции современных систем управления серверами. Особое внимание было уделено сетевому администрированию, управлению пользователями и группами, системному мониторингу и диагностике, а также вопросам безопасности информационных систем. Были подробно изучены инструменты автоматизации задач, системы управления конфигурациями и мониторинга, а также способы обеспечения безопасности данных.

Основные результаты исследования показали, что современные системы управления серверами играют ключевую роль в обеспечении надежной и безопасной работы информационных систем. Важность автоматизации и мониторинга подчеркивается необходимостью минимизации человеческого фактора и снижения вероятности ошибок. Также были выявлены тенденции к интеграции систем управления конфигурациями с другими инструментами, такими как системы мониторинга и оповещения, что способствует повышению общей эффективности и управляемости ИТ-инфраструктур.

Перспективы дальнейших исследований связаны с развитием и внедрением новых технологий в области системного администрирования. В частности, интерес представляют методы искусственного интеллекта и машинного обучения для автоматизации мониторинга и прогнозирования проблем, а также адаптивные системы безопасности, способные оперативно реагировать на изменяющиеся условия и угрозы.

Таким образом, данный дипломный проект внес вклад в понимание основных принципов и методов системного администрирования и предложил пути для дальнейшего совершенствования этой области.

Список литературы

1. Р.П. Орлов, С.А. Орлова. Системное администрирование. М.: Академия, 2019.
2. М.Л. Штерн, С.В. Бокштейн. Основы системного администрирования. М.: Русская редакция, 2020.
3. N.N. Assetta. Server and Network Security. New York: CRC Press, 2019.
4. R.T. Crowley. User and Group Management: A Practical Guide. New York: John Wiley & Sons, 2018.
5. G.V. Geetha, M.R. Balamurugan. System Administration: Concepts, Tools, and Technologies. New York: Springer, 2018.