МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Направление подготовки	**09.03.02 Информационные системы и технологии**
Направленность (профиль)	**Информационные системы и технологии**
Квалификация выпускника	Бакалавр

РАЗРАБОТАНО:
Доцент кафедры СУиИТ
_____ Мартиросян А.В.
«____» _____ 2020 г.

Пятигорск, 2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Методические рекомендации содержат перечень тем с вопросами для самостоятельной проработки, перечень практических и лабораторных работ с вопросами для самостоятельной проработки, материал для подготовки контрольной работы и курсового проекта.

Методические указания посвящены курсу «Администрирование информационных систем». Представлен дидактически и методически обработанный и систематизированный материал, раскрывающий основное содержание учебной дисциплины «Администрирование в информационных системах».

При изучении дисциплины «Администрирование в информационных системах» студенты опираются на знания, полученные после прохождения дисциплин «Информатика», «Информационные сети», «Структуры данных».

Знания, полученные в рамках «Администрирование в информационных системах», могут быть использованы при изучении курсов «Разработка Windows-приложений», «Информационные системы в управлении» «Анализ автоматизированных информационных систем предприятий».

В результате освоения дисциплины обучающийся должен:

- знать принципы построения систем администрирования и управления, их программную структуру, протоколы и службы, информационные базы данных управления, современные методы и средства разработки таких систем,
- перспективные направления развития систем администрирования и управления
- работать в информационных системах,
- администрировать и управлять из командной строки в современных информационных системах,
- использовать методы моделирования при выборе структуры администрирования и управления, методы и средства информационных и телекоммуникационных технологий; иметь опыт проектирования таких систем, выбора архитектуры и комплексирования аппаратных и программных средств администрирования и управления в информационных системах
- современными методиками администрирования и управления в информационных системах, обслуживающих сервисные и служебные программы, способностью дать оценку их характеристикам,
- способностью брать на себя ответственность за результаты работы по администрированию в информационных системах.

1. ЦЕЛЬ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Администрирование информационных систем» является формирование набора профессиональных компетенций будущего бакалавра по направлению подготовки 09.03.02 «Информационные системы и технологии».

Задачи освоения дисциплины: изучение и освоение принципов работы систем администрирования и управления в информационных системах; изучение их программной структуры, функций, специальных и общей процедур административного управления; умение выбирать аппаратно-программную платформу; изучение и освоение командной среды администрирования и управления.

2. ТЕМЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

№ темы	Наименование тем дисциплины, их краткое содержание	Обьем часов*

	8 семестр	
1	Тема 1. Функции, процедуры и службы администрирования Функции администрирования. Процедуры администрирования. Службы администрирования. Категории администраторов. Классификация администраторов баз данных.	12
2	Тема 2 Объекты администрирования Объекты администрирования. Компоненты в ведении администратора информационных систем. Разработчики приложений и служба безопасности. Реализация служб каталогов.	12
3	Тема 3. Методы администрирования Сканирование портов. Анализаторы полномочий. Trace Route. TERFIES. WHOIS. Сетевой мониторинг. Анализаторы связей. Мониторинг процессов. Системные информаторы.	12
	Итого за 5 семестр	36

3. ТЕХНОЛОГИЧЕСКАЯ КАРТА САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩЕГОСЯ

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
УК-1, ПК-10, ПК-21	Подготовка к лекциям	Конспект	Собеседование	1,35	0,15	1,5
УК-1, ПК-10, ПК-21	Подготовка к лабораторным работам	Индивидуальное задание	Отчет письменный	8,1	0,9	9
УК-1, ПК-10, ПК-21	Самостоятельное изучение литературы по темам 1,2,3	Конспект	Собеседование	22,95	2,55	25,5
			Итого	32,4	3,6	36

4. РЕКОМЕНДАЦИИ ДЛЯ САМОПОДГОТОВКИ

4.1 Подготовка к лекциям. Самостоятельное изучение литературы

Тема 1. Функции, процедуры и службы администрирования Базовый уровень

1. Функции администрирования
2. Процедуры администрирования
3. Службы администрирования
4. Категории администраторов

Повышенный уровень

1. Административные оповещения.
2. Классификация администраторов баз данных

3. Виды требований к информационной системе: функциональные требования, нефункциональные требования.

Тема 2. Объекты администрирования

1. Объекты администрирования
2. Компоненты в ведении администратора информационных систем

Повышенный уровень

1. Разработчики приложений и служба безопасности
2. Реализация служб каталогов

Тема 3. Методы администрирования

1. Сканирование портов
2 Анализаторы полномочий
3 Trace Route
4. Сетевой мониторинг

Повышенный уровень

1. Анализаторы связей
2. Мониторинг процессов
3. Системные информаторы
4. Телекс ресурсов

Тема 4. Домены Windows. Active Directory

1. Домены Windows. Active Directory.
2. Серверы имен.
3. Доменные роли

Повышенный уровень

1. Домены в Windows.
2. Параметры сети.

Тема 5. Серверы имен. DNS, WINS. Администрирование DNS

1. Адресация в Window.
2. Серверы имен.
3. DNS

Повышенный уровень

1.WINS.
2. Администрирование DNS

Тема 6. Группы безопасности. Управление пользователями. Понятие групповой политики

1. Блокировка рабочих столов пользователей.
2. Применение параметров безопасности.
3. Ограничение доступа к приложениям.

Повышенный уровень

1. Установка разрешения реестра и файловой системы.
2. Настройка конфигурации беспроводной сети.

Тема 7. Службы управления конфигурацией, контролем характеристик, ошибочными ситуациями, учетом и безопасностью, службы управления общего пользования

1. Службы управления конфигурацией
2. Службы контроля характеристик

3. Служба управления ошибочными ситуациями
4. Службы учета и безопасности системы
5. Службы управления общего пользования

Повышенный уровень

1. «ИБП»
2. ISM
3. LPD
4. MARS
5. TGS

Тема 8. Службы регистрации, сбора и обработки информации

1 Диспетчер регистрации
2 Диспетчер очереди печати
3 Диспетчер авто-подклчений удаленного доступа
4 Диспетчер подключений удаленного доступа
5 Диспетчер сеанса справки для удаленного рабочего стола

Повышенный уровень

1. Службы диспетчера отгрузки
2. Служба журнала событий
3. Служба журнала и оповещения производительности
4. Служба диспетчера сетевого DDE
5. Служба диспетчера сканеров и цифровых камер

Тема 9. Группы безопасности. Управление пользователями. Понятие групповой политики

1. Планировщик заданий
2. Поставщик поддержки безопасности
3. Уведомление о системных событиях
4. QoS PSVP

Повышенный уровень

1. Удаленный вызов процедур (RPC)
2. Удаленный реестр
3. Узел универсальных PnP-устройств
4. Управление приложениями

4.2 Подготовка к лабораторным работам

Лабораторная работа 1. Применение технологии виртуализации для решения задач администрирования

1. Функции администрирования
2. Процедуры администрирования
3. Службы администрирования
4. Категории администраторов
5. Административные оповещения.
6. Классификация администраторов баз данных
7. Виды требований к информационной системе: функциональные требования, нефункциональные требования.

Лабораторная работа 2. Объекты администрирования

1. Объекты администрирования
2. Компоненты в ведении администратора информационных систем
3. Разработчики приложений и служба безопасности
4. Реализация служб каталогов

Лабораторная работа 3. Методы администрирования

1. Сканирование портов
2 Анализаторы полномочий
3 Trace Route
4. Сетевой мониторинг
5. Анализаторы связей
6. Мониторинг процессов
7. Системные информаторы
8. Телекс ресурсов

Лабораторная работа 4. Домены Windows. Active Directory

1. Домены Windows. Active Directory.
2. Серверы имен.
3. Доменные роли
4. Домены в Windows.
5. Параметры сети.

Лабораторная работа 5. Серверы имен. DNS, WINS. Администрирование DNS

1. Адресация в Window.
2. Серверы имен.
3. DNS
4.WINS.
5. Администрирование DNS

Лабораторная работа 6. Группы безопасности. Управление пользователями. Понятие групповой политики

1. Блокировка рабочих столов пользователей.
2. Применение параметров безопасности.
3. Ограничение доступа к приложениям.
4. Установка разрешения реестра и файловой системы.
5. Настройка конфигурации беспроводной сети.

Лабораторная работа 7. Службы управления конфигурацией, контролем характеристик, ошибочными ситуациями, учетом и безопасностью, службы управления общего пользования

1. Службы управления конфигурацией
2. Службы контроля характеристик
3. Служба управления ошибочными ситуациями
4. Службы учета и безопасности системы
5. Службы управления общего пользования
6. «ИБП»
7. ISM
8. LPD
9. MARS
10. TGS

Лабораторная работа 8. Службы регистрации, сбора и обработки информации

1 Диспетчер регистрации
2 Диспетчер очереди печати
3 Диспетчер авто-подклчений удаленного доступа
4 Диспетчер подключений удаленного доступа
5 Диспетчер сеанса справки для удаленного рабочего стола
6. Службы диспетчера отгрузки
7. Служба журнала событий
8. Служба журнала и оповещения производительности
9. Служба диспетчера сетевого DDE
10. Служба диспетчера сканеров и цифровых камер

Лабораторная работа 9. Службы планирования и развития

1. Планировщик заданий
2. Поставщик поддержки безопасности
3. Уведомление о системных событиях
4. QoS PSVP
5. Удаленный вызов процедур (RPC)
6. Удаленный реестр
7. Узел универсальных PnP-устройств
8. Управление приложениями

5. ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ

Лекция 1. Функции, процедуры и службы администрирования

Поскольку информационные системы могут иметь много пользователей, должно существовать лицо или группа лиц, управляющих этой системой. Такое лицо называется администратором информационных систем. В любой организации должен быть хотя бы один человек, выполняющий административные обязанности; если информационная система большая, эти обязанности могут быть распределены между несколькими администраторами.

1.1 Функции администрирования

К функциям администрирования относятся:

- инсталляция и обновление версий сервера и прикладных инструментов;
- распределение дисковой памяти и планирование будущих требований системы к памяти;
- создание первичных структур памяти;
- создание первичных объектов по мере проектирования приложений разработчиками;
- модификация структуры данных в соответствии с потребностями;
- зачисление пользователей и поддержание защиты системы;
- соблюдение лицензионного соглашения;
- управление и отслеживание доступа пользователей к информационным системам;
- отслеживание и оптимизация производительности программ;
- планирование резервного копирования и восстановления;
- поддержание архивных данных на устройствах хранения информации;
- осуществление резервного копирования и восстановления;
- обращение в корпорации разработчиков или дилеров за техническим сопровождением.

1. 2. Процедуры администрирования

1 2.1 Исследование активности системы

Исследование активности системы с целью генерирования следующей общей информации:

- имя пользователя, выполнявшего отслеживаемое предложение;
- код действия, указывающий выполненное предложение;
- объекты, адресуемые в отслеживаемом предложении;
- дату и время выполнения отслеживаемого предложения.

Администратор обязан контролировать рост журнала и его размер. Когда генерируются записи использования системы, журнал системного администратора растет за счет двух факторов:

- числа включенных опций проверки;
- частоты выполнения отслеживаемых операций.

Для контроля за ростом журнала проверки надо использовать следующие методы:

1. Включать и выключать проверку информационной системы. Когда проверка включена, записи генерируются и поступают в журнал; когда проверка выключена, записи не генерируются.

2. Жестко контролировать возможности осуществлять проверку объектов. Это можно делать двумя различными способами:

3. Всеми объектами владеет администратор,

4. Все объекты содержатся в схемах, которые не соответствуют реальным пользователям информационной системы.

1.2.2 Очистка аудиторских записей из аудиторского журнала

После того, как проверка включена в течение некоторого времени, администратор может удалить записи из журнала, - как для того, чтобы освободить память, так и для облегчения управления этим журналом. Если информация журнала должна архивироваться для целей накопления истории, администратор может скопировать соответствующие записи.

1.2.3 Защита журнала проверки

Осуществляя отслеживание подозрительной деятельности в информационной системе, следует защищать целостность записей журнала проверки, чтобы гарантировать точность и полноту информации.

1.3. Службы администрирования

1.3.1 Служба соблюдения правил эксплуатации

Обязанности администратора: обеспечить правильную и надежную работу информационной системы.

Администратор должен определить обязанности и процедуры по администрированию и обеспечению функционирования компьютеров и сетей. Они должны быть зафиксированы в инструкциях и процедурах реагирования на инциденты. Для уменьшения риска некорректных или несанкционированных действий администратору следует применять принцип разделения обязанностей.

1 3.2 Службы проектирования и приемки информационных систем

Обязанности администратора: свести риск отказов информационных систем к минимуму.

Администратор обязан учитывать, что для обеспечения доступности ресурсов и необходимой производительности информационных систем требуется предварительное планирование и подготовка. Для уменьшения риска перегрузки систем необходимо учитывать будущие потребности и необходимую производительность. Эксплуатационные требования к новым системам следует определять, документировать и проверять до их приемки. Должны быть выработаны требования к переходу на аварийный режим для сервисов, поддерживающих несколько приложений.

1 3.3 Служба защиты от вредоносного программного обеспечения

Обязанности администратора: обеспечить целостность данных и программ.

Для предотвращения и выявления случаев внедрения вредоносного программного обеспечения администратору требуется принятие соответствующих мер предосторожности. В настоящее время существует целый ряд вредоносных программ («компьютерные вирусы», «сетевые черви», «троянские кони» и «логические бомбы»), которые используют уязвимость программного обеспечения по отношению к несанкционированной модификации. Администраторы информационных систем должны быть всегда готовы к проникновению вредоносного программного обеспечения в информационные системы и принимать специальные меры по предотвращению или обнаружению его внедрения. В частности, важно принять меры предосторожности для предотвращения и обнаружения компьютерных вирусов на персональных компьютерах.

1.3.4 Служба обслуживания систем

Обязанности администратора: обеспечить целостность и доступность информационных сервисов.

Для поддержания целостности и доступности сервисов администратору требуется выполнение некоторых служебных процедур: должны быть сформированы стандартные процедуры резервного копирования, регистрации событий и сбоев, а также контроля условий функционирования оборудования.

1.3.5 Сетевая служба

Обязанности администратора: обеспечить защиту информации в сетях.

Управление безопасностью сетей, отдельные сегменты которых находятся за пределами организации, требует особого внимания. Для защиты конфиденциальных данных, передаваемых по открытым сетям, могут потребоваться специальные меры.

1.3.6 Служба защиты носителей информации

Обязанности администратора: предотвратить повреждение информационных ресурсов и перебои в работе организации.

Необходимо контролировать носители информации и обеспечивать их физическую защиту. Следует определять процедуры для защиты носителей информации (магнитные ленты, диски, кассеты), входных/выходных данных и системной документации от повреждения, хищения и несанкционированного доступа.

1.3.7 Служба обмена данными и программным обеспечением

Обязанности администратора: предотвратить потери, модификацию и несанкционированное использование данных.

Администратору следует контролировать, чтобы обмены данными и программами между организациями осуществлялись на основе формальных соглашений. Должны быть установлены процедуры и стандарты для защиты носителей информации во время их транспортировки. Необходимо уделять внимание обеспечению безопасности при использовании электронного обмена данными и сообщениями электронной почты.

1.4. Категории администраторов

1.4.1 Администратор

Администратор в Windows – это пользователь, ответственный за настройку и управление контроллерами домена и локальными компьютерами, ведение учетных записей пользователей и групп, присвоение паролей и разрешений, а также помогающий пользователям работать в сети. Администраторы являются членами одноименной группы и обладают полным доступом к домену или компьютеру. Пользователь, который имеет право вносить на компьютере изменения, на уровне системы, устанавливать программное обеспечение и имеет доступ ко всем файлам на компьютере. Пользователь с учетной записью администратора компьютера имеет полный доступ к другим учетным записям пользователей на компьютере.

1.4.2 Администратор кластера

Группа независимых компьютерных систем, называемых узлами, работающих вместе в виде единой системы таким образом, чтобы важные для работы приложения и ресурсы оставались доступными для клиентов, называется кластерами. **Кластер серверов** – производит реализацию данной службы. Приложение, используемое для настройки кластера и его узлов, групп и ресурсов, определяется как Администратор кластера. Администрирование кластера может выполняться на любом компьютере доверенного домена, независимо от принадлежности участника к категории узлов кластера.

Cluster.exe – программа, которой можно пользоваться вместо администратора кластера для управления кластерами из командной строки. Программа Cluster.exe также может использоваться для автоматизации задач администрирования при помощи командных сценариев.

1.4.3 Администратор компьютера

Пользователь, управляющий компьютером. Администратор компьютера вносит изменения в систему, включая установку программ и доступ ко всем файлам компьютера, а также может создавать, изменять и удалять учетные записи других пользователей.

1.4.4 Администратор сети

Пользователь, ответственный за планирование, настройку и управление ежедневной работой сети. Администратор сети называется также системным администратором.

1.4.5 Администратор базы данных (АБД)

Администратор базы данных – лицо, отвечающее за выработку требований к базе данных, её проектирование, реализацию, эффективное использование и сопровождение, включая управление учётными записями пользователей БД и защиту от несанкционированного доступа. Не менее важной функцией администратора БД является поддержка целостности базы данных.

Администратор БД отвечает за целостность информационных ресурсов компании. На нем лежит ответственность по созданию, обновлению и сохранности связанных между собой резервных копий файлов, исходя из задач предприятия. Этот человек должен в мельчайших подробностях знать существующие механизмы восстановления программного обеспечения БД.

Возможны ситуации, при которых администратору БД потребуется на основе логических прикладных моделей создавать элементы физической схемы, а также поддерживать связь пользователей с системой и обеспечивать соответствующий уровень информационной безопасности, следя за тем, чтобы доступ к данным имели только те люди, которые в нем нуждаются.

Администратор БД должен уметь определять узкие места системы, ограничивающие ее производительность, настраивать SQL и программное обеспечение СУРБД и обладать знаниями, необходимыми для решения вопросов оптимизации быстродействия БД.

Основные задачи администратора базы данных:

- проектирование базы данных;
- оптимизация производительности базы данных;
- обеспечение и контроль доступа к базе данных;
- обеспечение безопасности в базе данных;
- резервирование и восстановление базы данных;
- обеспечение целостности баз данных;
- обеспечение перехода на новую версию СУБД.

Обязанности администратора

Среди наиболее важных обязанностей администратора – резервное копирование и восстановление информации. Механизм резервирования и восстановления данных обязан учитывать зависимость бизнеса от информации. Другими словами, если в Вашей

прикладной системе приема заказов через Internet любая потеря информации является абсолютно недопустимой, то использование схемы "холодного" резервирования, т.е. подразумевающую полную остановку и отключение БД, в данном случае, совершенно неприемлемо. Для того, чтобы найти наилучшее решение, соответствующее запросам предприятия, администратор должен хорошо разбираться в многообразии методов резервирования и восстановления, знать плюсы и минусы каждого из них.

Кроме того, администратор должен контролировать рост БД. От него требуется держать руководство в курсе относительно предполагаемого роста БД, с тем чтобы иметь возможность своевременно заказать любое необходимое оборудование.

Настройка также является одной из основных зон ответственности администратора БД. И пользователи, и разработчики за советом будут обращаться именно к нему.

Администратор также занимается созданием тестовых конфигураций БД, управлением схемами приложений, внесением изменений в эти схемы, желательно безошибочных, поддержкой пользователей, выражающейся, к примеру, в добавлении в систему новых пользователей, обеспечением информационной безопасности в виде открытия доступа только к запрашиваемым объектам.

1. Профилактический монитор:

- избавляет администратора от экстренных мер
- разгружает администратора по вечерам и выходным
- ускоряет приобретение опыта.

2. Средства диагностики:

- превращают младшего АБД в старшего, позволяя последнему сконцентрироваться на других задачах.

3. Средства анализа:

- помогают при планировании роста БД и будущих затрат.

4. Средства технического обслуживания:

- помогают при резервном копировании и восстановлении данных, сокращая время операции и уменьшая число ошибок
- помогают при реорганизациях, экономя время, уменьшая количество ошибок и длительность профилактических окон (maintenance window)
- способствуют высокой доступности данных, создавая «незаметные» с точки зрения системы профилактические окна и помогая при резервировании / восстановлении системы.

1.4.5.1 Классификация администраторов баз данных (АБД)

Основные типы администраторов БД: системный администратор; архитектор БД; аналитик БД, разработчик моделей данных; администратор приложений; проблемно-ориентированный администратор БД; аналитик производительности; администратор хранилища данных.

Существует несколько видов администраторов БД, а их обязанности вполне могут отличаться от компании к компании.

1. Оперативные (operational) АБД:

- манипулируют дисковым пространством;
- наблюдают за текущей производительностью системы;
- реагируют на возникающие неисправности БД;
- обновляют системное ПО и ПО базы данных;
- контролируют структурные изменения БД;
- запускают процедуры резервного копирования данных;
- выполняют восстановление данных;
- создают и управляют тестовыми конфигурациями БД.

2. Тактические (tactical) АБД:

- реализуют схемы размещения информации;

- утверждают процедуры резервного копирования и восстановления данных;

- разрабатывают и внедряют структурные элементы БД: таблицы, столбцы, размеры объектов, индексацию и т.п.; сценарии (scripts) изменения схемы БД; конфигурационные параметры БД;

- утверждают план действий в случае аварийной ситуации.

3. Стратегические (strategic) АБД:

- выбирают поставщика БД;

- устанавливают корпоративные стандарты данных;

- внедряют методы обмена данными в рамках предприятия;

- определяют корпоративную стратегию резервирования и восстановления данных;

- устанавливают корпоративный подход к ликвидации последствий аварии и обеспечению доступности данных.

4. Старшие (senior) АБД:

- досконально знают свой персонал;

- пользуются высоким спросом;

- могут написать скрипт, который освободит их из запертого сундука, брошенного в океан, и чрезвычайно гордятся своими произведениями;

- тратят уйму времени на подготовку младших АБД;

- очень ценятся руководством и получают бешеные деньги

5. Младшие (junior) АБД:

- мечтают стать старшим АБД;

- не слишком сильны в написании скриптов;

- имеют большую склонность к использованию средств управления БД;

- тоже неплохо получают.

6. Прикладные (application) АБД:

- в курсе информационных нужд компании;

- помогают в разработке прикладных задач;

- отвечают за разработку схемы и ее изменения;

- вместе с системным АБД обеспечивают должный уровень резервирования / восстановления данных;

- занимаются построением тестовых БД.

7. Системные (system) АБД:

- отвечают за все необходимое для резервирования и восстановления данных;

- контролируют производительность системы в целом;

- осуществляют поиск и устранение неисправностей;

- в курсе нынешних и будущих потребностей БД в плане емкости;

- в курсе текущего состояния и нужд БД.

8. Наемные (contract) АБД:

- приглашаются под конкретную задачу или в качестве консультантов;

- передают персоналу необходимые знания;

- фиксируют свои действия;

- должны прекрасно разбираться в соответствующей области;

- хороши в качестве временного персонала, для оценки проекта или системы.

9. Администраторы-руководители:

- проводят еженедельные совещания;

- определяют перечень первоочередных задач;

- устанавливают и оглашают официальный курс и стратегию;

- утверждают и корректируют должностные инструкции и список обязанностей;

- следят за наличием соответствующей документации.

1.4.6 Административные оповещения

Оповещения, относящиеся к серверу или к использованию ресурсов. Они уведомляют пользователей о событиях, происходящих в системе безопасности и управления доступом, в сеансах пользователей, в системе управления питанием (при наличии источника бесперебойного питания), при репликации каталога и при печати. Если компьютер инициирует оповещение, сообщение направляется по заранее определенному списку пользователей и компьютеров.

Лекция 2. Объекты администрирования

На большинстве современных предприятий, где ведется активная работа с различными информационными системами, рано или поздно встает проблема ввода, систематизации, обработки и безопасного хранения значительных объемов информации. Версии прикладных инструментов, различные структуры памяти, системы защиты данных и разные виды электронной документации беспорядочно накапливаются в файловых системах компьютеров, затрудняя поиск информации, коллективную работу над документами, их согласование и соблюдение конфиденциальности. Таким образом, требуется средство управления, которое могло бы обеспечить высокую эффективность работы с информационными системами в масштабах всей организации. Для решения этой задачи используется администратор информационных систем.

2.1 Объекты администрирования

Объект №1: Непосредственно объекты информационных систем. Контроль за его бесперебойным функционированием, а в случае возникновения неисправностей своевременное сохранение важной информации и резервное копирование.

Объект №2: Программное обеспечение информационных систем, необходимое для предотвращения и выявления случаев внедрения вредоносных программ. Разработка и внедрение соответствующих мер предосторожности. Отслеживание новейших программ и средств для борьбы с возможным проникновением вирусов в систему.

Объект №3: Планирование и проектирование информационных систем. Подготовка и расчет будущей производительности, подробное изучение и корректировка, а возможно, и разработка проектной документации. Доработка критериев приемки информационных систем под данное конкретное производство.

Объект №4: Функционирование компьютеров и сетей. Обеспечение правильной и надежной работы информационных систем. Регулирование и проверка соблюдения правил эксплуатации оборудования пользователями.

Объект №5: Программное обеспечение, необходимое для защиты информации в сетях. Снабжение системы, имеющей конфиденциальные данные, передаваемые по открытым сетям специальными мерами и средствами, определяющими их правовую и информационную охрану.

Объект №6: Электронный обмен данными. Стандарты для защиты носителей информации во время их транспортировки. Отслеживание сроков действия лицензий.

Объект №7: Физическая защита носителей информации. Программное обеспечение, необходимое для предотвращения повреждений информационных ресурсов и возникновения перебоев в работе организации. Разработка средств защиты от хищения и несанкционированного доступа к секретным и конфиденциальным данным организации.

2.2 Компоненты в ведении администратора информационных систем

1. Пользователь. Создание и удаление учетных записей, их блокировка и разблокирование, настройка сценариев входа, консультирование пользователей по различным аспектам работы с системой и нахождению тех или иных ресурсов. Обозначить группу технической поддержки. И возложить на нее обязанности по

установке и настройке сетевого клиентского программного обеспечения на компьютерах пользователей.

2. Управление данными. Обозначение и установление грани доступа разных пользователей к конкретным ресурсам, профилактическое обслуживание баз данных (индексация, оптимизация, упаковка), организация резервного копирования.

3. Производительность и оптимизация системы. Отбор и конкретное изучение эмпирических правил, помогающих администратору вносить изменения в настройки с минимальным риском ухудшить другие показатели или сделать систему неработоспособной. Снижение риска возможного нарушения работы системы при отключении одного из компонентов.

4. Учет системных ресурсов. Повышение производительности системы при проведении соответствующей модернизации. Обеспечение возможности платного использования ресурсов. Контроль использования дискового пространства, печати, учет трафика

5.Техническое обслуживание и модернизация. Очистка от пыли, смазка вентиляторов, подтяжка креплений, контроль состояния аккумуляторов, изменение физической топологии сети. Разработка инструкций для службы технической поддержки. Грамотное формулирование заявок на изменение аппаратной конфигурации. Закупка дополнительных лицензий или обновленной версии программного обеспечения.

6. Управления активным сетевым оборудованием и сетью в целом.

7. Информационная безопасность. Составление плана доступа пользователей к ресурсам и контроль его исполнения. Отслеживание появления различных уязвимостей в используемых операционных системах.

2.3 Разработчики приложений и служба безопасности

В некоторых случаях база данных должна также иметь одного или нескольких сотрудников службы безопасности. Которые главным образом отвечают за регистрацию новых пользователей, управление и отслеживание доступа пользователей к базе данных, и защиту базы данных.

В обязанности разработчика приложений входит:

- проектирование и разработка приложений данных;
- проектирование структуры данных в соответствии с требованиями приложений;
- оценка требований памяти для приложения;
- формулирование модификаций структуры данных для приложения;
- передача вышеупомянутой информации администратору данных;
- настройка приложения в процессе его разработки;
- установка мер по защите приложения в процессе его разработки.

2.4 Реализация служб каталогов

Служба каталогов – это физически распределенное, но логически централизованное хранилище данных, используемое для администрирования всей вычислительной среды и позволяющее собрать всю информацию подобного рода в одной программе. Она обеспечивает универсальный доступ ко всем вычислительным ресурсам, причем для каждого пользователя ведется одна учетная запись, независимо от количества серверов и сервисов, которые этот пользователь получает в распоряжение. По существу, службы каталогов представляют собой системы указателей, размещаемых в базах данных. Служба каталогов должна обеспечивать единую согласованную информацию о сети, а так же средства идентификации, управления доступом, навигации и другие услуги. Одной из важнейших функций таких служб является установление соответствия между сетевыми именами, доступом пользователей или ресурсов и сетевыми адресами. Эта функция,

называемая службой имен, позволяет работать с простыми псевдонимами и переводить их в машинные адреса (или отображать в такой форме).

Служба каталогов обязана обладать следующим набором свойств:

1. Пользователь должен получать доступ ко всем разрешенным для него службам, ресурсам и приложениям после единственного подключения к сети. Для этого потребуется определенная степень открытости решений служб каталогов. Для успешного функционирования системы разработчикам приложений следует предусмотреть поддержку службы каталогов в своих приложениях.

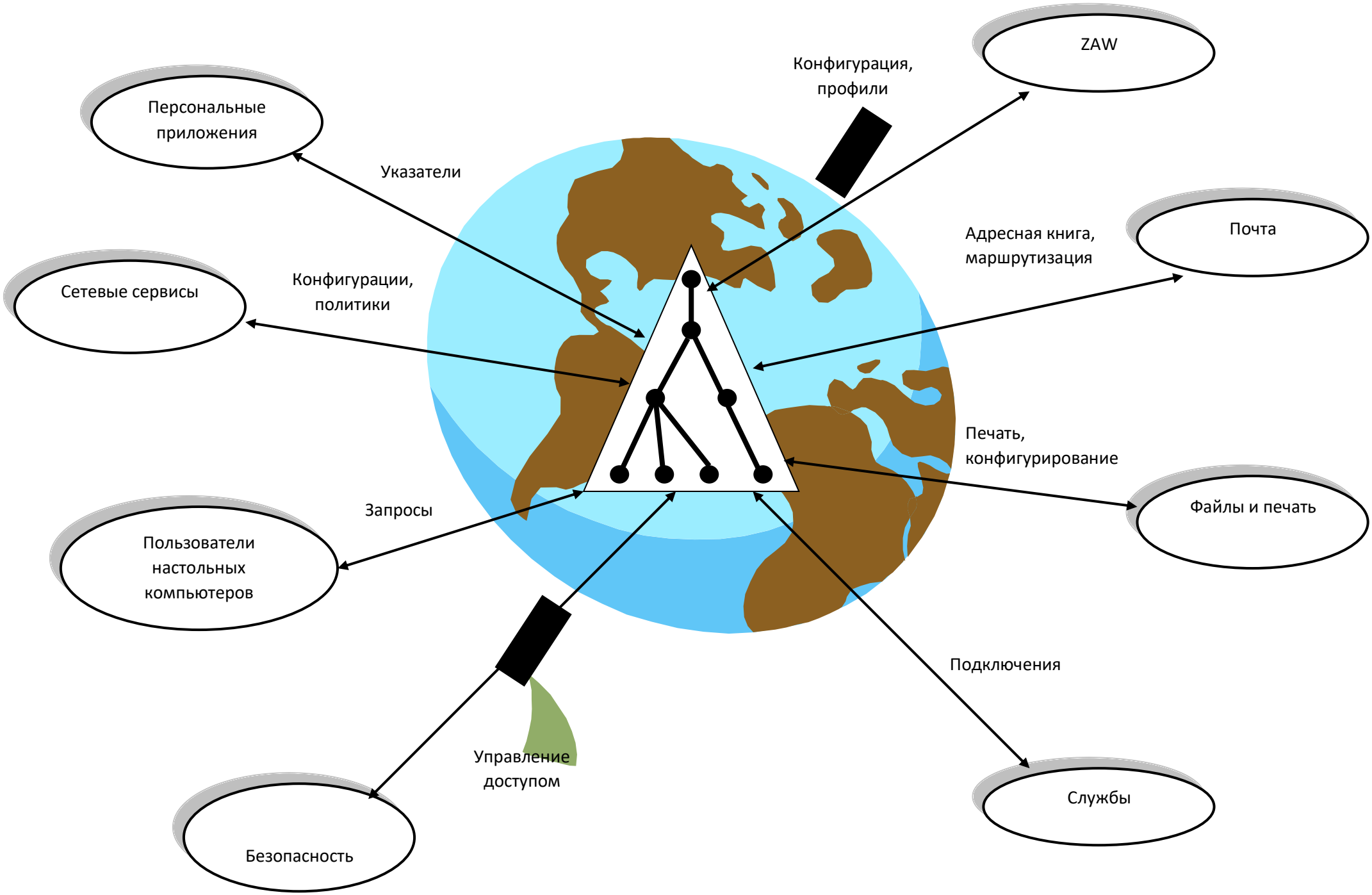
2. Вся информация о вычислительной среде должна хранится в распределенной форме. Данные следует реплицировать на несколько серверов. В этом случае пользователь или служба, которым потребовался доступ к информации, могут получать ее с относительно близкого и удобного для них сервера.

3. Для определения целостности информации, поступающей в распоряжение нескольких пользователей, нужна поддержка реплицирования данных. Изменения, внесенные в один из участков каталога, необходимо передавать всем абонентам сети для гарантии тождественности информации вне зависимости от места ее получения.

4. Система должна поддерживать запросы, составленные как на основании конкретных параметров (имя, номер телефона и т.п.), так и при расширенном поиске (например, все цветные принтеры на первом этаже). Служба каталогов действует по принципу справочного издания «Желтые страницы». 5. С ее помощью можно определять местоположение нужной службы по имени или производить поиск по определенным категориям.

6. Возможность администрирования не должна зависеть от физического расположения системы. Это означает отказ от необходимости четко определять местонахождения данных средств. К примеру, появляется возможность полного или частичного назначения прав администрирования отдельных участков каталога.

Задачи администрирования представлены на рисунке 2.1.


ZAW
Конфигурация, профили
Персональные приложения
Указатели
Почта
Адресная книга, маршрутизация
Сетевые сервисы
Конфигурации, политики
Печать, конфигурирование
Файлы и печать
Запросы
Пользователи настольных компьютеров
Подключения
Управление доступом
Службы
Безопасность

Лекция 3. Методы администрирования

3.1. Сканирование портов

Сканеры портов – определяют и анализируют возможные услуги системы, которые были установлены на ней. Исчерпывающий двигатель сканирования собирает всю информацию об услугах, проверяет, и т.п.. Сканер Порта AATools' точно определяет распределение активных услуг используя как TCP так и UDP опросы порта.

3.2 Анализаторы полномочий

А нализаторы Полномочий – тесты полномочий систем. Проверяют списки адресов в настоящих серверах. Анализаторы Полномочий обеспечивают наиболее подробную доступную информацию о возможных полномочиях, включая, заголовки, позиции и т.п.. Это – полностью загруженное средство для управления списками систем.

3.3. TRACE ROUTE

TraceRoute – определяют и сохраняют маршруты посылаемых пакетов информации от одной определенной машины в некоторую другую машину в сети. Требуется как маршрутизатор. При необходимости показывают IP адреса (и обычно фактическое имя) каждого маршрутизатора. В течение процесса, TraceRoute будут иметь отношение к DNS-серверу и сообщать DNS- адреса и IP адреса каждого узла, который пакеты информации повстречают по пути.

3.4. TERIFIES

Верификаторы Электронной Почты – определяют каждый адрес электронной почты возможных корреспондентов.

3.5. WHOIS

Whois – полезные сетевые утилиты информации, которые позволяют обнаруживать всю доступную информацию о IP адресах или главном имени. В отличие от стандартных Whois утилит, AATools' Whois может найти информацию о компьютере расположенном в любой части мира, с пониманием спрашивая правовую базу данных и доставляя все связанные записи в пределах нескольких секунд. Если пользователь не удовлетворяется результатами, обнаруживающимися в базе данных, он может произвести программный специфический запрос через whois-сервер.

3.6. Сетевой мониторинг

Сетевой Мониторинг – вторгающиеся средства обнаружения /проверки, которые определяют и открывают все локальные TCP/IP и UDP порты, отображают услуги, которые активны в данных портах, и отображают порты в их соответствующих приложениях (для Windows NT/2000/XP только), обеспечивают полезную информацию о сетевых интерфейсах.

3.7. Анализаторы связей

Анализаторы Связей – новые современные утилиты, которые при необходимости просканируют все существующие связи от любой папки до HDD и уведомят, если какая-либо связь изменяется или становится инвалидом. Анализаторы Связей допускают сканирование целой системы и обнаруживают все URL файлы. Анализаторы Связей также проверяют динамические HTML страницы, URLs с CGI и могут перемещать испорченные файлы, но прежде данные условия необходимо определить в соответствующем диалоговом окне.

3.8. Мониториги процессов

Мониторинги Процессов – позволяют увидеть любой процесс, работающий на PC и вручную остановить любую подозрительную деятельность.

3.9. Системные информаторы

Системные Информаторы – обеспечивают чрезвычайно большой массой вспомогательной информации об анализируемом локальном PC: процессоре, памяти, WinSock данные, и т.п..

3.10. Телекс ресурсов

Телекс ресурсов предназначается для просмотра ресурсов выполняемых файлов (с расширением .exe и .dll). Телекс Ресурсов отображает исчерпывающую информацию о программных ресурсах, включая диалоги, иконки, строки и далее. Телекс Ресурсов позволяет также сохранять ресурсы любых избранных модулей на жестком диске.

3.11. Чистильщики

Чистильщики Регистратуры разрабатываются, чтобы навести порядок данных в регистратуре. Использование AATools Чистильщика Регистратуры увеличивает компьютерное пространство, ускоряет загрузку системы функционирования и уменьшает количество неудач.

3.12. CPU мониторинги

CPU мониторинги использования – обеспечивают информацией о CPU использовании всего системного процесса.

Улучшенные административные методы – мультипрошитая сеть и системные исследователи. Улучшенные административные методы включают: сканеры портов, анализаторы полномочий, CGI анализаторы, @-mail верификаторы, анализаторы связей, сетевые мониторинги, мониторинги процессов, Whois, системные информатизаторы, телексы ресурсов и чистильщики регистратуры. Отчет должен накопить данные, относящиеся к сетевому статусу и доступности, используя все самые последние инструментальные средства разработки в исследовании сети. AATools – безопасность, которая обнаруживает дыры перед атакой злоумышленников. AATools должна быть частью пакета разработчика безопасности и ее необходимо применять.

3.13. Работа с системой от имени администратора

Работа в Windows 2000 или Windows XP и т.д. в качестве администратора делает систему уязвимой для троянских коней и других программ, угрожающих безопасности. Простое посещение Web-узла может очень сильно повредить систему. На незнакомом Web-узле может находиться троянская программа, которая будет загружена в систему и выполнена. Если в это время находиться в системе с правами администратора, такая программа может переформатировать жесткий диск, стереть все файлы, создать новую учетную запись пользователя с административным доступом и т.д.

Простому пользователю лучше всего добавить себя в группу «Пользователи» или «Опытные пользователи». Войдя в систему в качестве члена группы «Пользователи», можно выполнять обычные задачи, в том числе выполнение программ и посещение узлов в Internet, не подвергая компьютер излишнему риску. Члены группы «Опытные пользователи» могут, кроме того, устанавливать программы, добавлять принтеры и использовать большинство компонентов панели управления. Если необходимо выполнить такие задачи администрирования, как обновление операционной системы или настройка системных параметров, выйдите из системы и войдите в нее как администратора.

При необходимости часто входить в систему и запускать программы с правами администратора можно использовать для этого команду **runas**.

3.14. Запуск программы от имени администратора

Чтобы запустить программу от имени администратора:

1. В проводнике Windows щелкнуть исполняемый файл программы, который требуется открыть.
2. Нажать клавишу SHIFT и, не отпуская ее, щелкнуть значок программы правой кнопкой мыши, а затем выбрать команду **Запуск от имени**.
3. Чтобы войти в систему с использованием учетной записи администратора, необходимо установить переключатель **Учетную запись указанного пользователя**.
4. В поля **Пользователь** и **Пароль** ввести имя и пароль нужной учетной записи администратора.

- Данная процедура используется для выполнения административных задач пользователями, вошедшими в систему в качестве членов другой группы, например «Пользователи» или «Опытные пользователи».

- Чтобы запустить программу от имени администратора домена, перед именем учетной записи администратора в поле **Имя пользователя** необходимо указать имя домена. Например: **Имя Домена \ Имя Администратора**

- Использование команды **От имени** не ограничено учетными записями администраторов.

- При запуске таких программ, как консоль MMC или компонент панели управления, из сети с помощью команды **Запуск от имени** возможен сбой, поскольку учетные данные для подключения к общему ресурсу сети отличаются от учетных данных, используемых для запуска программы. Учетные данные, используемые для запуска программы, могут не обеспечить получение доступа к тому же общему сетевому ресурсу.

- Если команда **Запуск от имени** не выполняется, возможно, не запущена служба вторичного входа.

- Можно также использовать команду **runas** из командной строки.

- Служба вторичного входа принимает только проверку пароля. Если политика требует использования смарт-карт для входа в систему, команда **runas** выполняться не будет.

3.15. Создание ярлыка без входа в систему

Часто у администратора возникает необходимость создания ярлыка на рабочем столе не находя программу в проводнике. Чтобы создать ярлык с помощью команды **runas** необходимо:

1. Щелкнуть правой кнопкой мыши рабочий стол, выбрать пункт **Создать**, а затем – **Ярлык**.

2. В поле **Укажите местоположение объекта** ввести **runas** и нужные параметры команды. Примеры приведены в следующей таблице.

Для создания ярлыка	Вводится	Описание
Командной строки с учетными данными администратора	**runas /user:**ИмяКомпьютера**administrator cmd**	В строке заголовка данного окна будут указаны учетные данные, используемые для его открытия
Оснастки «Управление компьютером» с учетными данными администратора	**runas /user:**ИмяКомпьютера**administrator "mmc %windir%\system32\compmgmt.msc "**	В окне «Управление компьютером» не указываются используемые учетные данные. При запуске двух и более окон «Управление компьютером» в разных контекстах безопасности это может привести к путанице
Оснастки «Active Directory — пользователи и компьютеры» с учетными данными администратора	**runas /user:**ИмяДомена**administrator "mmc %windir%\system32\dsa.msc"**	В окне «Active Directory — пользователи и компьютеры» не указываются используемые учетные данные. При запуске двух и более окон «Active

домена (только для Windows 2000 Server)		Directory — пользователи и компьютеры» в различных контекстах безопасности это может привести к путанице
Оснастки «Active Directory — пользователи компьютеры» в другом лесе (только для Windows 2000 Server)	**runas /netonly /user:**ИмяДомена\ИмяПользователя **"mmc.exe dsa.msc"**	В окне «Active Directory — пользователи и компьютеры» не указываются используемые учетные данные. При запуске двух и более окон «Active Directory — пользователи и компьютеры» в разных контекстах безопасности это может привести к путанице

1. Нажать кнопку **Далее**, ввести имя ярлыка и нажать кнопку **Готово**.

- Ярлык будет выполняться с разрешениями, предоставленными соответствующему пользователю. При использовании учетной записи администратора или члена группы «Администраторы» возможно выполнение административных задач.

- Использование команды **runas** не ограничено учетными записями администраторов.

- Если команда **runas** не выполняется, возможно, не запущена служба вторичного входа.

3.16. RUNAS

Запускает конкретные средства и программы с разрешениями, отличными от тех, которые предоставляет текущая учетная запись.

Синтаксис

runas [{/profile|/noprofile}] [/env] [/netonly] [/smartcard] [/showtrustlevels] [/trustlevel] /user:учетная_запись_пользователя program

Параметры:

/profile – загружает профиль пользователя. Параметр /profile используется по умолчанию;

/no profile – определяет, что профиль пользователя не надо загружать. Это позволяет загрузить приложение быстрее, но также может привести к сбоям в некоторых приложениях;

/env – задает использование текущей сетевой среды вместо локальной среды пользователя;

/netonly – показывает использование введенных сведений о пользователе только для удаленного доступа;

/smartcard – определяет необходимость поддержки учетных данных с помощью смарт-карты;

/showtrustlevels – выводит список параметров /trustlevel;

/trustlevel – указывает уровень проверки подлинности, на котором необходимо выполнить приложение. Использовать параметр /showtrustlevels лучше всего для просмотра доступных уровней доверия;

/user:учетная_запись_пользователя – задает имя учетной записи пользователя, которая будет использована для запуска программы. Учетная запись пользователя должна быть представлена в формате пользователь@домен или домен\пользователь;

program – задает команду или программу, которая будет запущена с помощью учетной записи, указанной в параметре /user;

/? – отображает справку в командной строке.

Примечания.

1. Администраторам рекомендуется использовать учетную запись с ограниченными разрешениями для выполнения повседневных задач, не связанных с администрированием, и учетную запись с более широкими правами только для выполнения отдельных административных задач. Чтобы реализовать такой подход без выхода из системы и повторного входа, следует войти в систему с обычной учетной записью и использовать команду runas для запуска программ, требующих более широких прав.

2. Использование команды runas не ограничено административными учетными записями, хотя именно такой способ является наиболее употребительным. Любой пользователь с несколькими учетными записями может использовать runas для запуска программы, консоли MMC или компонента панели управления с другими личными данными.

3. Если необходимо использовать учетную запись администратора на своем компьютере, в качестве параметра /user: надо ввести одно из следующих значений:

/user:учетная_запись_администратора@имя_компьютера

/user:имя_компьютера\учетная_запись_администратора

4. Чтобы использовать данную команду в качестве администратора домена, вводится одно из следующих значений параметра:

/user:учетная_запись_администратора@имя_домена

/user:имя_домена\учетная_запись_администратора

5. С помощью команды runas можно выполнять программы (*.exe), запускать сохраненные консоли MMC (*.msc), ярлыки программ и сохраненных консолей MMC и компоненты панели управления. Их можно запускать в качестве администратора, даже если вход в систему был произведен с учетной записью члена другой группы, например группы пользователей или опытных пользователей.

6. Можно использовать команду runas для запуска любой программы, консоли MMC или компонента панели управления. Поскольку указываются соответствующие сведения об имени пользователя и его пароле, учетная запись пользователя предоставляет возможность подключения к компьютеру, а программа, консоль MMC или компонент панели управления становятся доступными в системе для учетной записи пользователя.

7. Команда runas позволяет администрировать сервер в другом лесе (компьютер, с которого запускается программа, и сервер располагаются в разных доменах).

8. При попытке запуска программы, консоли MMC или компонента контрольной панели из сети с помощью runas выполнение может окончиться неудачей, поскольку личные сведения, использованные для подключения к сетевому ресурсу, могут отличаться от тех, что использованы при запуске программы. Личные сведения, использованные при запуске программы, могут не позволить получить доступ к тому же сетевому ресурсу.

9. Некоторые компоненты, например папка «Принтеры» и элементы рабочего стола, открываются косвенно. Эти компоненты не могут быть запущены командой runas.

10. Если выполнение команды runas заканчивается неудачей, может оказаться, что служба вторичного входа не запущена или используемая учетная запись пользователя недопустима. Чтобы проверить состояние службы вторичного входа, в компоненте «Управление компьютером» необходимо щелкнуть узел Службы и приложения, а затем – Службы. Чтобы проверить учетную запись пользователя, надо попытаться подключиться к соответствующему домену с помощью этой учетной записи.

Примеры

1. Чтобы в качестве администратора на локальном компьютере запустить экземпляр интерпретатора командной строки, необходимо ввести команду: runas /user:имя_локального_компьютера\administrator cmd

После запроса ввести пароль администратора.

2. Чтобы запустить экземпляр оснастки «Управление компьютером», используя учетную запись администратора домена companydomain\domainadmin, ввести команду:

runas /user:companydomain\domainadmin "mmc %windir%\system32\compmgmt.msc"

После запроса ввести пароль соответствующей учетной записи.

3. Чтобы запустить экземпляр блокнота, используя учетную запись администратора домена user в домене domain.microsoft.com, ввести команду:

runas /user:user@domain.microsoft.com "notepad my_file.txt"

После запроса ввести пароль соответствующей учетной записи.

4. Чтобы запустить экземпляр окна командной строки, сохраненную консоль MMC, компонент панели управления или программу, которая будет администрировать сервер в другом лесе, ввести команду:

runas /netonly /user:домен\имя_пользователя "команда"

В параметре домен\имя_пользователя должен быть указан пользователь с разрешениями, достаточными для администрирования сервера. После запроса ввести пароль соответствующей учетной записи.

Условные обозначения форматирования

Формат	**Значение**
Курсив	Сведения, вводимые пользователем
Полужирный	Элементы, вводимые без изменений
Многоточие (...)	Параметр может быть введен в командной строке несколько раз
В квадратных скобках ([])	Необязательные элементы
В фигурых скобках ({}); варианты, разделенные вертикальной линией (|), пример: {even|odd}	Набор вариантов, из которых необходимо выбрать один
Шрифт Courier	Выходные данные программы

Лекции 4 – 5. Домены Windows. Active Directory.

Серверы имен. DNS, WINS. Администрирование DNS

Windows NT опирается на NetBIOS и использует сервер имен NetBIOS, называемый Windows Internet Naming Service (WINS, служба имен Интернета для Windows), чтобы выявлять компьютеры в сети и разрешать их имена в IP-адреса. Основное ограничение NetBIOS и WINS заключается в том, что они используют плоское пространство имен, в то время как пространство имен Active Directory - иерархическое. Пространство имен AD основано на том же принципе, что и пространство системы доменных имен (DNS), поэтому для разрешения имен и выявления контроллеров домена каталог использует вместо WINS-серверов DNS-серверы. Чтобы служба Active Directory работала корректно, необходимо наличие в сети хотя бы одного сервера DNS.

Домены в Active Directory называются стандартными доменными именами DNS, которые могут совпадать или не совпадать с именами, применяемыми организацией в Интернете. Например, если уже есть зарегистрированное доменное имя mycorp.com, предназначенное для Интернет-серверов, то можно задать это же имя родительскому домену в дереве AD или создать новое имя для внутреннего использования. Новое имя не обязательно регистрировать, так как область его применения будет ограничена только сетью Windows 2000.

DNS основана на записях о ресурсах (resource records), которые содержат информацию об определенных машинах в сети. Традиционно администраторы должны создавать эти записи вручную, но в сети Windows 2000 это вызовет проблемы. Задача создания записей о сотнях компьютеров вручную является долгой и трудной, и она усложняется использованием протокола DHCP (Dynamic Host Configuration Protocol, протокол динамической конфигурации хоста), который служит для автоматического назначения сетевым системам IP-адресов. Из-за того, что IP-адреса систем, управляемых DHCP, могут меняться, должен быть способ, который позволил бы обновлять записи DNS, чтобы отразить эти изменения.

Microsoft DNS Server, включенный в Windows 2000, поддерживает новый тип SRV записей о ресурсах, который позволяет клиентским системам использовать запросы DNS для выявления контроллеров доменов Windows 2000. Сервер DNS от Microsoft также поддерживает динамическую систему DNS (DDNS), которая работает вместе с Microsoft DHCP Server, чтобы динамически обновлять записи о ресурсах для определенных систем при изменении их IP-адресов. Многие из более старых серверов DNS, используемых сегодня (такие как BIND версии 4.xx), не поддерживают новые возможности и не будут работать с Active Directory. Тем не менее, эти новые возможности DNS были стандартизированы и реализованы в программных продуктах других производителей, таких как последние версии BIND. Поддержка записей о ресурсах типа SRV является единственной из этих новых возможностей, непременно требуемой для Active Directory. Иные возможности, такие как DDNS, защищенная DDNS и инкрементные зонные передачи, являются рекомендуемыми, но не необходимыми.

Active Directory все еще сравнительно новый продукт, и он должен пройти некоторую проверку на зрелость, которая может затронуть связь между службой каталогов и DNS. Если AD развертывается в сети предприятия, то использование Microsoft DNS Server станет хорошим выбором, так как он, несомненно, будет обновляться, чтобы соответствовать любым изменениям, происходящим в самой службе каталогов.

Любой отдельный сервер или сервер-член домена, работающий под управлением Windows 2000 Server, может получить статус контроллера домена.

Перед тем как приступить к настройке, используйте диск CD-ROM для "чистой" установки Windows 2000 Server на компьютер или модернизируйте существующий отдельный сервер или сервер-член домена до Windows NT 4.0 Server.

Замечание: Для повышения статуса вы должны зарегистрироваться, используя учетную запись локального администратора. Не регистрируйтесь с использованием глобальной учетной записи — члена группы локальных администраторов. В последующих версиях вы сможете использовать глобальную учетную запись при повышении статуса.

Модернизация контроллеров домена Windows NT 4.0
Вы можете также модернизировать главный (PDC) или резервный (BDC) контроллер домена, работающий под управлением Windows NT 4.0. Главный контроллер домена должен быть модернизирован в первую очередь. После модернизации PDC могут быть по возможности модернизированы серверы BDC. После модернизации BDC вы можете сохранить его в качестве дублирующего в том домене, где он находится, либо превратить его в сервер-член домена.

Если вы решили модернизировать контроллер домена Windows NT 4.0, процесс повышения статуса начнется автоматически после того, как обновление операционной системы завершится и компьютер будет перезагружен.

Создание первого домена в лесу
Первый домен в лесу становится вершиной первого дерева в лесу. Домены Active Directory используют систему имен DNS, например “nttest.microsoft.com”. Если вы создаете дочерние домены в дереве “nttest.microsoft.com,” имена всех доменов дерева

должны оканчиваться на “nttest.microsoft.com”. Начните обдумывать, какое имя присвоить своему первому домену, уже сейчас.

Настройка контроллера первого домена выполняется в два этапа:

1. Установка Microsoft DNS Server.

2. Запуск мастера установки Active Directory.

Замечание: Если контроллер вашего первого домена Active Directory — модернизированный PDC Windows NT 4.0, мастер Active Directory Promotion будет автоматически запущен сразу после завершения обновления системы. Однако перед повышением статуса вы должны выполнить дополнительную настройку, как это описано далее. Прервав в этот момент работу мастера повышения статуса, вы сможете запустить его позднее.

Установка Microsoft DNS Server

Клиенты Active Directory используют DNS для поиска контроллеров домена. Microsoft рекомендует использовать DNS-сервер, который входит в состав Windows 2000, однако допускается использование и других серверов DNS, если они удовлетворяют определенным функциональным требованиям. Более подробную информацию об использовании DNS-серверов сторонних производителей вы можете найти в главе “Использование DNS-серверов сторонних поставщиков” в конце настоящего документа.

Если вы уже установили и настроили DNS-сервер для поддержки домена Active Directory и контроллеров этого домена, вы можете перейти к следующему этапу. Если нет — Microsoft рекомендует установить Windows 2000 DNS на первом контроллере домена.

Во время установки вам может быть выдан запрос на установку статического IP-адреса сервера. Серверы DNS требуют для корректной работы указания как минимум одного постоянного IP-адреса на компьютере.
Чтобы установить Microsoft DNS Server

1. Зарегистрируйтесь, используя локальную учетную запись администратора. Если вы модернизируете главный контроллер домена Windows NT 4.0 — вы уже зарегистрированы.

2. В меню Start выберите пункт Settings, а затем — пункт Control Panel.

3. Дважды щелкните по значку Add/Remove Programs.

4. Нажмите кнопку Add/Remove Windows Components.

Будет запущена программа-мастер Windows Components Wizard.

5. Выберите пункт Networking Services и нажмите кнопку Details.

Замечание: Не устанавливайте флажок Networking Services во включенное положение. В этом случае будут установлены все сетевые службы. Просто выберите пункт Networking Services.

6. Установите во включенное положение флажок рядом с пунктом Dynamic Name Service (DNS).

7. Нажмите кнопку OK, чтобы закрыть диалоговое окно.

8. Нажмите кнопку Next для установки программного обеспечения сервера DNS. Если диск Windows 2000 Beta 3 еще не вставлен в дисковод CD-ROM, программа предложит вам сделать это.

9. Если появится запрос с предложением указать статический IP-адрес, нажмите кнопку OK и проделайте следующее:

a. В диалоговом окне Local Area Connection Properties, которое должно появиться после этого, выберите пункт Internet Protocol (TCP/IP) и нажмите кнопку Properties.

b. Установите переключатель в положение Use the following IP address и укажите значения в полях IP address, Subnet mask и Default Gateway. Если вы не знаете, какие значения использовать, обратитесь к администратору сети. Если вы работаете в собственной сети, вы можете использовать значения из зарезервированного диапазона 10.x.x.x адресов класса A. Например, установите IP-адрес компьютера равным 10.0.0.1,

используйте предложенное по умолчанию значение маски подсети и оставьте поле адреса шлюза пустым. Каждый компьютер должен иметь свой уникальный IP-адрес.

c. Если в вашей сети имеются другие серверы DNS, установите переключатель в положение Use the following DNS server addresses и введите IP-адрес сервера DNS в поле Primary DNS Server. Если у вас в сети нет других серверов DNS, оставьте переключатель в положении Obtain DNS server address automatically или оставьте поле Primary DNS Server пустым.

d. Нажмите кнопку OK, чтобы закрыть диалоговое окно Internet Protocol (TCP/IP) Properties.

e. Нажмите кнопку OK, чтобы закрыть панель Connection configuration.

f. Нажмите кнопку Finish для завершения установки DNS.

10. Закройте окно Add/Remove Programs. Сервер DNS установлен.

Если вы указали в пункте "c" существовавший ранее сервер DNS, вам придется настроить его так, чтобы он делегировал обслуживание имен в домене Active Directory серверу DNS, который вы только что установили. Это делается путем добавления ресурсных записей Name Server в файл зоны, ответственной за обслуживание имен вашего домена Active Directory. О том, как это осуществить, вы можете узнать из документации к своему DNS-серверу. Сделайте это после того, как работа мастера установки Active Directory будет завершена.

Если вы не указывали существующего сервера DNS, компьютер будет автоматически настроен для использования установленного на нем сервера DNS.

Замечание: В отличие от предыдущих версий Windows 2000, вам больше не нужно вручную настраивать DNS перед повышением статуса сервера. Теперь это делается автоматически в процессе повышения статуса, если на компьютере установлен DNS-сервер. В последующих версиях сервер DNS будет устанавливаться автоматически, и выполнять эти действия не потребуется.

Запуск мастера установки Active Directory

Повышение статуса серверов до контроллеров домена происходит с помощью программы-мастера установки Active Directory, известной также под названием DCpromo.

Для запуска DCpromo

1. В меню Start выберите пункт Run.

2. Введите dcpromo и нажмите кнопку OK.

3. Будет запущена программа-мастер DCpromo. Нажмите кнопку Next, чтобы продолжить работу с ней.

4. Если появится сообщение о том, что выбранный вами путь не принадлежит разделу NTFS 5.0 и в системе существует только раздел FAT, вам придется преобразовать его в NTFS 5.0. Если это сообщение не появится — пропустите следующие два пункта.

a. Нажмите кнопку OK, чтобы закрыть окно сообщения.

b. Нажмите кнопку Cancel, чтобы прервать работу DCpromo.

c. В меню Start выберите пункт Programs, а затем пункт Command Prompt.

d. Введите команду

convert /FS:NTFS

где — имя логического диска, где установлена Windows 2000.

e. Утилита Convert сообщит вам о текущей файловой системе раздела и проинформирует о необходимости перезагрузки. Введите Y и нажмите клавишу Enter.

f. Перезагрузите систему. Логический том будет преобразован в NTFS 5.0 в процессе загрузки. Зарегистрируйтесь и вновь запустите DCpromo, пролистайте окна до окна System Volume path и продолжайте работу.

5. Выберите пункт New domain и нажмите кнопку Next.

6. Выберите пункт Create new domain tree и нажмите кнопку Next.

7. Выберите пункт Create a new forest of domain trees и нажмите кнопку Next.

8. Введите полное DNS-имя, которое вы выбрали для своего первого домена Active Directory, например “nttest.microsoft.com”, и нажмите кнопку Next. DCpromo проверит, не используется ли уже введенное вами имя.

9. DCpromo предложит вам NetBIOS-имя домена. Для обеспечения обратной совместимости с такими клиентами, как Windows NT 4.0, это имя будет использоваться ими для идентификации домена. Используйте предложенное имя или введите другое и нажмите кнопку Next.

10. DCpromo предложит вам путь для размещения базы данных и файлов журнала Active Directory. Прочтите советы по выбору путей файлов и примите предложенный или укажите новый, а затем нажмите кнопку Next.

11. DCpromo предложит путь файла для создания резервной копии системного тома. Прочтите советы по выбору путей файлов и примите предложенный или укажите новый, а затем нажмите кнопку Next.

12. Если появится предупреждение о том, что DCpromo не может связаться с DNS-сервером для разрешения указанного вами имени, нажмите кнопку OK.

13. Выберите Yes, чтобы DCpromo настроил для DNS и нажмите кнопку Next.

14. Прочитайте информацию в окне подтверждения и нажмите кнопку Next для запуска процесса повышения статуса. Он займет несколько минут.

15. Нажмите кнопку Finish.

16. Нажмите кнопку Restart Now, чтобы перезагрузить компьютер. Поздравляем, вы только что создали свой первый домен Active Directory! После того, как компьютер перезагрузится, вы можете зарегистрироваться, используя глобальную учетную запись администратора. Используйте тот же самый пароль, что и до повышения статуса сервера.

Теперь вы можете продолжить добавление контроллеров домена с различным статусом или сразу приступить к экспериментам с каталогом. Добавление серверов и рабочих станций в домен

Серверы и рабочие станции подключаются к домену так же, как и в Windows NT 4.0.

На компьютерах, работающих под управлением Windows 2000, необходимо настроить как минимум один IP-адрес сервера DNS, чтобы они могли обнаружить контроллер домена в процессе подключения. IP-адрес сервера DNS может сообщаться клиентским системам автоматически при помощи DHCP или устанавливаться вручную в окне настройки сетевых соединений.

Windows NT 4.0 и клиентские системы Microsoft Windows 9x используют для обнаружения контроллеров домена службу WINS. Вы должны установить и запустить WINS, если хотите, чтобы такие клиенты участвовали в домене Windows 2000.

Учетные записи для подключаемых компьютеров можно создать в домене заранее или в процессе присоединения к домену. Если вы хотите сделать это заранее, то можете воспользоваться средством Active Directory Manager.

Включение в домен Windows 2000 серверов или рабочих станций, работающих под управлением Windows 2000, производится следующим образом.

Чтобы присоединить сервер или рабочую станцию Windows 2000 к домену

1. В меню Start выберите пункт Settings, а затем — пункт Control Panel.

2. Щелкните дважды по значку System. (Вместо этого вы можете щелкнуть правой клавишей мыши по значку My Computer на Рабочем столе и выбрать в динамическом меню пункт Properties.)

3. Щелкните закладке Network Identification.

4. Нажмите кнопку Change, чтобы изменить статус членства компьютера.

5. В списке Member of выберите пункт Windows NT secure domain.

6. В текущем поле ввода укажите полное DNS-имя домена, к которому вы хотите присоединить компьютер, например “nttest.microsoft.com”.

7. Нажмите кнопку OK.

8. Введите имя и пароль учетной записи домена, обладающей достаточными привилегиями для выполнения операции присоединения компьютера к домену. Если вы создали учетную запись для данного компьютера заранее, введите имя и пароль пользователя, который будет на нем работать. Если вы хотите создать учетную запись в процессе присоединения, введите имя и пароль пользователя, имеющего полномочие на создание объектов в используемом по умолчанию контейнере Computers. В любом случае, полномочий администратора домена будет достаточно.

9. Нажмите кнопку OK для отправки имени и пароля.

10. Если попытка присоединения окончится неудачей, возможно, вы неправильно указали имя домена или использовали учетную запись пользователя, не обладающего достаточными полномочиями. Если присоединение произошло успешно, появится подтверждающее сообщение. Нажмите кнопку OK.

11. Нажмите кнопку OK, чтобы закрыть окно предупреждения о перезагрузке.

12. Нажмите кнопку OK, чтобы закрыть панель System.

13. Нажмите кнопку Yes для перезагрузки компьютера.

После перезагрузки компьютер будет присоединен к домену.

Лекция 6. Группы безопасности. Управление пользователями. Понятие групповой политики

Групповые политики (GP) представляют собой основной метод обеспечения централизованного управления конфигурацией безопасности в Windows 2000 и Windows 2003. Они могут применяться на уровне сайта, домена и OU, а также могут применяться к пользователям и компьютерам (Users and Computers) в Active Directory. GP используются для выполнения следующих действий.

- Блокировка рабочих столов пользователей.
- Применение параметров безопасности.
- Ограничение доступа к приложениям.
- Установка разрешения реестра и файловой системы.
- Настройка конфигурации беспроводной сети.

Совет

Настоятельно рекомендуется использовать утилиту Group Policies вместо Local System Policies, если это возможно.

Параметры конфигурации

Утилита Group Policies разделена на две области - User (Пользователь) и Computer (Компьютер). Область настройки пользователя User Configuration содержит такие элементы, как параметры рабочего стола, параметры безопасности и сценарии входа и выхода их системы. Эти элементы определены под деревом User Configuration и применяются при входе в систему или обновлении групповой политики. Computer Configuration используется для настройки работающей системной среды (а не пользовательской оболочки), включая параметры служб, параметры безопасности и сценарии загрузки/отключения. Эти элементы определены в дереве Computer Configuration и применяются при загрузке и обновлении Group Policy.

По умолчанию GP применяются в зависимости от расположения настраиваемого объекта. Пользовательские GP зависят от того, в каком сайте, домене и организационной единице находится объект "пользователь". То же самое относится и к компьютеру. GP применяются к компьютерам в зависимости от расположения объекта "компьютер" (сайт, домен и организационная единица, в которой находится компьютер). Это означает, что если GP применяется к объекту User (Пользователь), то используется конфигурация пользователя, а конфигурация компьютера групповой политики игнорируется. И

наоборот, если GP применяется к объекту Computer (Компьютер), используется конфигурация компьютера, а конфигурация пользователя игнорируется.

Групповые политики по умолчанию

Имеются две групповые политики, установленные по умолчанию, создаваемые при создании домена: Default Domain Policy (Политика домена по умолчанию) и Default Domain Controller Policy (Политика контроллера домена по умолчанию). Политика домена по умолчанию применяется к контейнеру домена. Она может быть применена ко всем компьютерам в домене по умолчанию. Политика контроллера домена по умолчанию применяется к "специальному" контейнеру контроллера домена в домене и, кроме того, применима только к контроллерам домена.

Параметры конфигурации в групповой политике

Так как мы не можем рассказать подробно о групповых политиках, уложившись в одну лекцию, то обсудим наиболее важные элементы, связанные с безопасностью, которые могут (и должны) быть применены через групповую политику. Как уже говорилось ранее, каждая групповая политика имеет два основных дерева данных конфигурации: Computer Configuration (Конфигурация компьютера) и Users Configuration (Конфигурация пользователей). Эти области отображаются в виде двух раздельных секций в окне Group Policy Object Editor (Редактор объекта групповой политики) (см. рис.16).

Конфигурация компьютера:

- Account Policies: Password Policy (Политики учетных записей: политика паролей). Позволяет настраивать историю, требования к возрасту, длине и сложности паролей.
- Account Policies: Account Lockout Policy (Политики учетных записей: политика блокировки учетных записей). Позволяет настраивать число попыток, длительность и сброс.
- Local Policies: Audit Policies (Локальные политики: политики аудита). Позволяет включать аудит в системах.

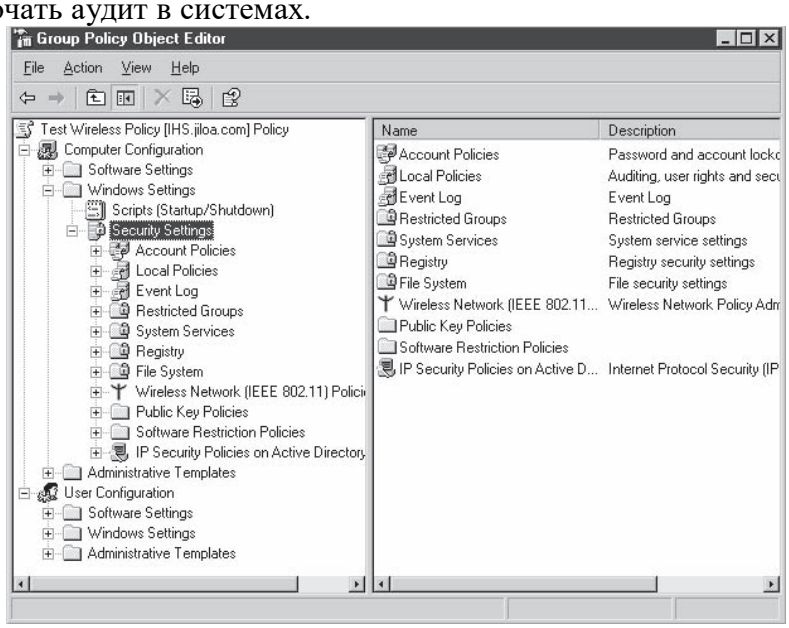


Рис.16

- Local Policies: User Rights Assignment (Локальные политики: присвоение прав пользователей). Позволяет присваивать пользовательские права пользователям и группам.
- Local Policies: Security Options (Локальные политики: параметры безопасности). Позволяет настраивать политики, связанные с безопасностью, включая подписи SMB, ограничения безопасности каналов, автоматический выход, уровень аутентификации LAN Manager, текстовое сообщение входа и примечание, а также множество других элементов (40 по умолчанию).

• Event Log: Settings for Event Logs (Журнал событий: параметры журналов событий). Позволяет настраивать объем журнала, ограничения доступа, параметры сохранения, а также необходимость отключения системы по заполнении журналов.

• Restricted Groups: Members of Restricted Group (Ограниченные группы: члены ограниченной группы). Предписывает членство в группе. Если пользователь или группа входят в список членов ограниченной группы, но не находятся в группе, происходит добавление в группу этого пользователя или группы. Если пользователь или группа является членом группы, но отсутствует в списке членов ограниченной группы, то этот пользователь или группа удаляется.

• Restricted Groups: Restricted Group Is Member Of (Ограниченные группы: ограниченная группа входит в). Если ограниченная группа не входит в группу, которой она должна принадлежать, она добавляется в нее. В отличие от предписания членства в группе, описанного выше, если ограниченная группа принадлежит группе, которая здесь отсутствует, то эта ограниченная группа не удаляется.

• IP Security Policies (Политики безопасности IP). Позволяет настраивать списки и действия фильтров, правила политик, методы защиты и аутентификации, типы соединений и ключевые параметры и методы обмена.

Конфигурация пользователя:

• Windows Settings: Internet Explorer Maintenance: Security (Настройки Windows: обслуживание Internet Explorer: безопасность). Позволяет настраивать особые зоны безопасности, оценку содержимого и параметры аутентификации.

• Windows Settings: Scripts (Настройки Windows: сценарии). Позволяет указывать сценарии входа и выхода из системы.

• Administrative Templates: Windows Components: Windows Explorer (Шаблоны администрирования: компоненты Windows: Проводник Windows). Позволяет настраивать пользовательские параметры для Проводника Windows. Среди этих параметров следует отметить удаление меню File (Файл), опций Map Network Drive (Подключить сетевой диск) и Disconnect Network Drive (Отключить сетевой диск), скрытие вкладки Hardware (Оборудование), запрос аутентификационных данных для сетевых инсталляций и многое другое.

• Administrative Templates: Windows Components: Windows Installer (Шаблоны администрирования: компоненты Windows: программа установки Windows Installer). Позволяет запретить пользователям производить установку со съемных носителей, а также вносить другие изменения в конфигурацию.

• Administrative Templates: Start Menu and Taskbar (Шаблоны администрирования: меню Пуск и панель задач). Позволяет удалять папки пользователя из меню Start (Пуск), отключать и удалять ссылки на Windows Update, отключать опцию Log Off (Выход из системы) в меню Start (Пуск), отключать и удалять команду Shut Down (Завершение работы), удалять отдельные меню и др.

• Administrative Templates: Desktop (Шаблоны администрирования: Рабочий стол). Используется для скрытия всех значков Рабочего стола, запрета на изменение пользователями пути к папке My Documents (Мои документы), необходимости сохранения параметров при выходе и др. Также позволяет настраивать элементы, связанные с Active Desktop, и взаимодействие пользователей с Active Directory.

• System: Group Policy (Система: групповая политика). Позволяет настраивать пользовательские параметры, такие как интервал обновления пользователей, выбор контроллера домена, автоматическое обновление файлов ADM и др.

Выше приведены наиболее важные компоненты оснастки Group Policies с указанием того, каким образом они связаны с безопасностью. Это лишь очень общее описание рассматриваемой области, а не полноценный обзор. Обязательно ознакомьтесь с более детальной информацией по данной теме перед тем, как вплотную заняться работой с оснасткой Group Policies.

Дополнения групповой политики в Windows 2003

В Windows 2003 в групповую политику добавлены два отдельных элемента, связанных с безопасностью систем в AD. Этими элементами являются Software Restriction Policies (Политики ограничения программного обеспечения) (о них уже говорилось выше) и Wireless Network (IEEE 802.11) Policies (Политики беспроводных сетей [IEEE 802.11]).

Политики ограничения программного обеспечения. Функции оснастки Group Policy такие же, как у оснастки Local Security Policy (Локальная политика безопасности), однако эту оснастку можно применить к домену или OU. Параметры, связанные с безопасностью, настраиваемые с помощью данной групповой политики, включают в себя следующие настройки.

- Тип беспроводной сети, к которой могут осуществлять доступ клиенты: Ad Hoc (Точка доступа), Infrastructure (Инфраструктура) или Any (Любая).
- Возможность запрета на использование беспроводными клиентами Windows локальных параметров Windows для настройки их параметров беспроводных сетевых соединений.
- Возможность разрешить пользователям подключаться только к предпочитаемым сетям.
- Возможность требовать аутентификацию 802.1X при каждом подключении к беспроводным сетям 802.11 (см.рис.17).
- Указание типа EAP: Smart Card or other certificate (Смарт-карта или другой сертификат) или Protected EAP (PEAP) (Защищенный EAP).
- Выбор метода аутентификации для использования в PEAP: Secured password (EAP-MSCHAP v2) (Защищенный пароль EAP-MSCHAP v2) или Smart Card or other certificate (Смарт-карта или другой сертификат).

[PAGEBREAK]

Старшинство

Ниже приведены шаги, автоматически выполняемые системой при оценке/применении Group Policy.

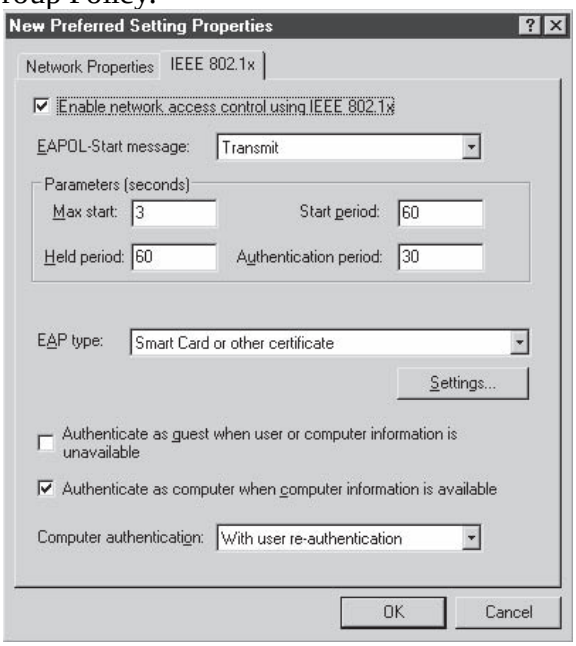


Рис.17

При загрузке системы:

1. Область Computer Configuration (Конфигурация компьютера) оснастки Local Security Policy (Локальная политика безопасности).
2. Область Computer Configuration (Конфигурация компьютера) оснастки Group Policies (Групповые политики), связанной с сайтом (в порядке предпочтения - от наименее до наиболее предпочтительного).

3. Область Computer Configuration (Конфигурация компьютера) оснастки Group Policies (Групповые политики), связанной с доменом.

4. Область Computer Configuration (Конфигурация компьютера) оснастки Group Policies (Групповые политики), связанной с OU, в порядке предпочтения - от самой внешней организационной единицы до самой внутренней, и внутри OU - с самого низкого уровня до самого высокого.

При входе пользователя:

1. Области User Configuration (Конфигурация пользователя) оснастки Local Security Policy (Локальная политика безопасности).

2. Области User Configuration (Конфигурация пользователя) оснастки Site Group Policies (Групповые политики сайта) в порядке предпочтения.

3. Области User Configuration (Конфигурация пользователя) оснастки Domain Group Policies (Групповые политики домена) в порядке предпочтения.

4. Области User Configuration (Конфигурация пользователя) оснастки OU Group Policies (Групповые политики организационного подразделения) в порядке предпочтения.

Замыкание на себя

Ранее мы говорили о том, что по умолчанию GP применяются в зависимости от расположения настраиваемого объекта. Чтобы обойти эту возможность для пользователей, компания Microsoft реализовала замыкание на себя (loopback). Эта возможность используется для конфигурации пользователя групповых политик, а также конфигурации компьютера, в зависимости от расположения объекта "компьютер" (не пользователь) при входе пользователя в систему. Таким образом, каждый пользователь, осуществляющий вход в систему компьютера, получает конфигурацию пользователя (User Configuration) из групповых политик этого компьютера. При включении опции можно также указать функцию Merge (Слияние) (объединение конфигурации из всех групповых политик) или Replace (Замещение) (только применение конфигураций пользователей в зависимости от расположения объекта "компьютер").

Наследование

Во многом аналогично наследованию списков ACL, параметры GP передаются от самых дальних к самым ближним, причем ближние/низшие имеют большее старшинство. Порядок оценки таков: Local Security Policy (Локальная политика безопасности), Site Group Policies (Групповые политики сайта), Domain Group Policies (Групповые политики домена) и OU Group Policies (Групповые политики организационного подразделения). Существует возможность блокировки наследования политики, если не требуется наследовать параметры. Это позволит блокировать групповые политики, связанные с сайтами, доменами или организационными единицами высших уровней от применения их к текущему сайту, домену или организационному подразделению и к их дочерним объектам. Как администратору верхнего уровня вам может понадобиться включение принудительного использования некоторых политик верхнего уровня (например, минимальная длина пароля); для этого существует опция No Override (Игнорирование невозможно). Эту опцию можно включить для того, чтобы предотвратить обход (включая блокировку) политики любым дочерним объектом.

Примечание

По большому счету, между сайтами и доменами в действительности нет никакого "наследования". Будет происходить оценка только тех групповых политик, связанных с конкретным сайтом или доменом, в котором находится пользователь или компьютер. Организационная единица является единственным контейнером, для которого действительно наблюдается наследование при проходе вниз по дереву элементов.

Средства управления групповой политикой

Следующие утилиты весьма полезны для управления групповыми политиками и просмотра результатов их работы.

Group Policy Management Console. Утилита Group Policy Management Console (Консоль управления групповой политикой) представляет собой оснастку MMC и набор сценариев, предоставляющих единый интерфейс управления групповой политикой на предприятии. Интерфейс показан на рис.18 с отображением части политики домена по умолчанию (Default Domain Policy) для домена jiloa.com.

Group Policy Results. Консоль управления групповой политикой предоставляет средство для определения результирующей политики для данного пользователя и/или системы. (Этот метод отличается от средства Resultant Set of Policy, обсуждаемого ниже.) Чтобы сгенерировать запрос Group Policy Results (Результаты групповой политики) для пользователя/компьютера, нужно открыть лес, щелкнуть правой кнопкой мыши на пункте Group Policy Results (Результаты групповой политики) и затем выбрать Group Policy Results Wizard (Мастер результатов групповой политики). Выполните предписания мастера и введите соответствующую информацию в окнах ввода данных. На рис.19 показаны результаты запроса Group Policy Results для администратора в IHS в домене jiloa.com.

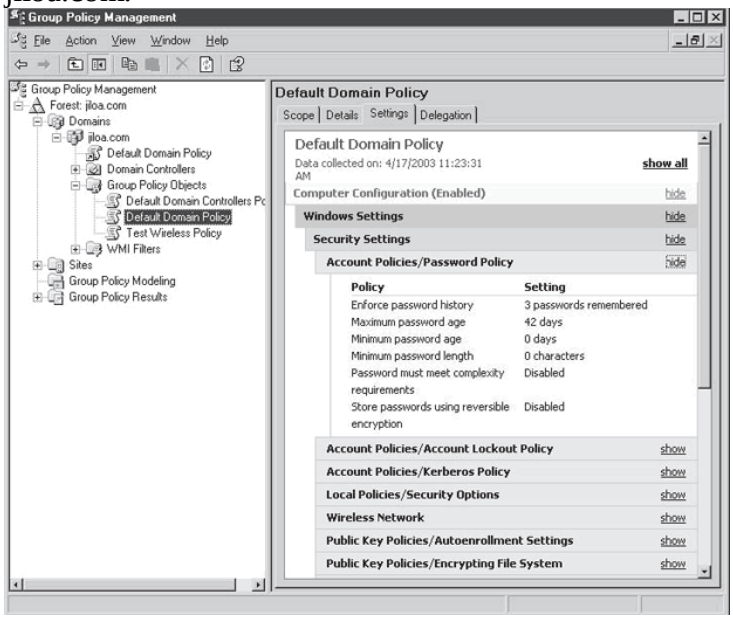


Рис.18

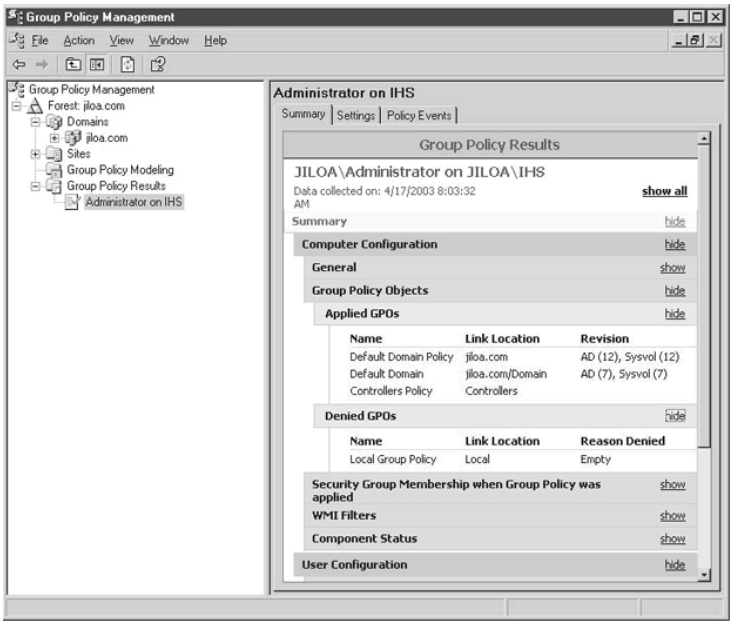


Рис.19
[PAGEBREAK]

Resultant Set of Policy (RSoP). Утилита предназначена для облегчения процессов применения политик и устранения неполадок в них. Она предоставляет детальные сведения обо всех сконфигурированных параметрах политики и может помочь определить набор примененных политик и порядок, в котором они применяются. Это очень полезно, когда несколько политик применяются на различных уровнях, таких как сайт, домен и организационное подразделение (единица).

Эта утилита используется для симуляции результатов применения параметров политики, которые вы собираетесь применить к компьютеру или пользователю, а также для определения параметров текущей политики для пользователя, находящегося в данный момент в системе компьютера. На рисунке 20 приведен пример RSoP для политики аудита системы IHS. RSoP находится в оснастке MMC и открывается в консоли управления Microsoft (MMC), оснастке Active Directory Users and Computers (Пользователи и компьютеры Active Directory) или оснастке Active Directory Sites and Services (Сайты и службы Active Directory).

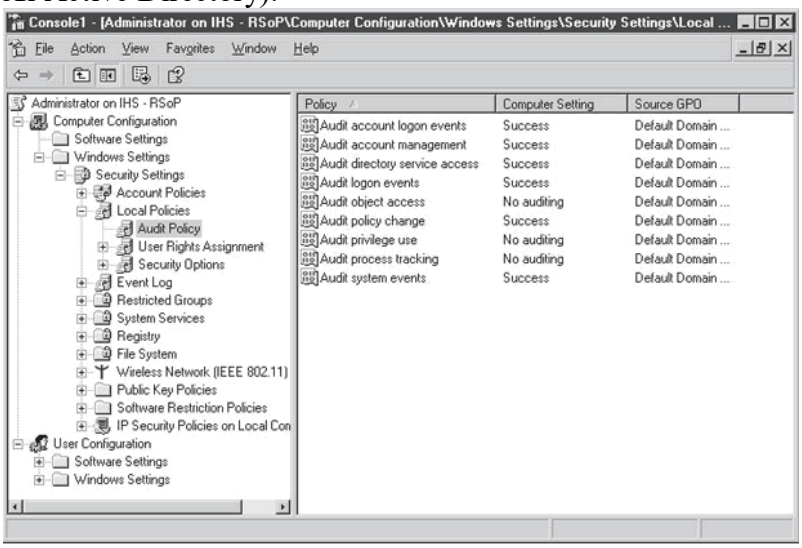


Рис.20

Управление пользователями и группами AD

Необходимо обеспечить правильность настроек безопасности для всех учетных записей. Это можно сделать двумя способами: посредством политики учетной записи через групповую политику в домене с рассматриваемой учетной записью или посредством отдельных ограничений в свойствах пользовательской учетной записи для конкретного объекта User (Пользователь). Политики учетных записей применяются через оснастку Local Security Policy (Локальная политика безопасности) (об этом рассказывалось выше) или через механизм Group Policy (Групповые политики) в домене, в котором находится учетная запись. Свойства учетной записи пользователя устанавливаются для пользователей в индивидуальном порядке. Так как эти параметры специфичны для каждого пользователя, у них нет ничего общего с групповой политикой или локальными параметрами безопасности; они являются атрибутами объекта User. С помощью оснастки Active Directory Users and Computers (Пользователи и компьютеры Active Directory) можно осуществлять администрирование пользователей домена, а посредством оснастки Local Users and Groups (Локальные пользователи и группы) - администрирование локальных пользователей.

Оснастка Active Directory Users and Computers (Пользователи и компьютеры Active Directory)

При создании учетных записей пользователей основной используемой утилитой администрирования является оснастка Active Directory Users and Computers (Пользователи и компьютеры Active Directory), предназначенная для администрирования учетных записей в рамках домена Active Directory. Оснастка Active Directory Users and Computers

(Пользователи и компьютеры Active Directory) (см. рис.21) используется для управления пользователями, группами и другими элементами, такими как организационные единицы для доменов в лесу. По умолчанию оснастка запускается из меню Start/Programs/Administrative Tools (Пуск/Программы/Администрирование) на каждом контроллере домена. Эту оснастку также можно добавить в любую консоль MMC.

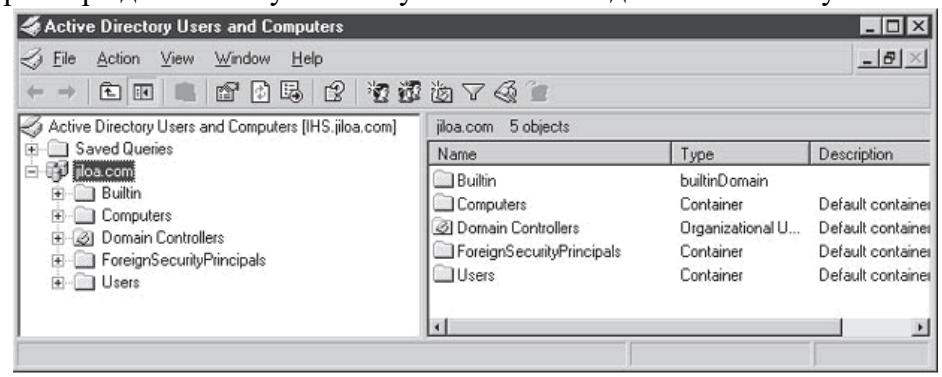


Рис.21

Лекция 7. Службы управления конфигурацией, контролем характеристик, ошибочными ситуациями, учетом и безопасностью, службы управления общего пользования

Служба – программа или процесс, выполняющий конкретную системную функцию по поддержке других программ, особенно на низком (близком к аппаратному) уровне. Если доступ к службам осуществляется по сети, они могут быть опубликованы в Active Directory, что упрощает их администрирование и использование. Примеры служб: диспетчер учетных записей безопасности, служба репликации файлов, служба маршрутизации и удаленного доступа.

Важную роль в оптимизации производительности операционных систем играет настройка системы служб.

Управление ими производится при помощи вызова оснастки управления службами через **Пуск → Выполнить → services. msc**.

При стандартной установке тип запуска многих служб настраивается как «авто», т.е. они автоматически запускаются при старте системы или при первом вызове службы. При настройке типа запуска службы «вручную» для задействования службы ее необходимо задействовать вручную. Если тип запуска настроен как «отключено», службу нельзя запустить ни автоматически, ни вручную.

Многие службы зависимы от других, поэтому если отключить многие из служб, то можно столкнуться с такой ситуацией, когда не удастся включить все обратно. Чтобы этого избежать, необходимо, перед тем как производить эксперименты со службами, сохранить раздел реестра, отвечающий за запуск системных служб –

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services],

например, щелкнув на указанном разделе правой кнопкой мыши и выбрав пункт “Экспортировать”.

7.1. Службы управления конфигурацией

Далее указаны стандартные службы, их функции, рекомендации по изменению типа запуска служб, зависимости служб, а также тип запуск/вход от имени, действующие по умолчанию. Для оптимизации работы системы часть служб можно подвергнуть отключению, причем внимание нужно обратить на службы с типом запуска «авто». DHCP-клиент.

7.1.1 Plug and Play

Позволяет компьютеру распознавать изменения в установленном оборудовании и подстраиваться под них, либо не требуя вмешательства пользователя, либо сводя его к

минимуму. Остановка или отключение этой службы может привести к нестабильной работе системы. От данной службы зависят следующие компоненты: Windows Audio, Диспетчер логических дисков», «Служба администрирования диспетчера логических дисков», «Служба сообщений», «Смарт-карты» и «Телефония». Тип запуска / Вход от имени – Авто / Локальная система.

7.1.2 Machine Debug Manager:

Управляет конфигурацией сети посредством регистрации и обновления IP-адресов и DNS-имен. Если нет сети (ни локальной, ни модема), то данную службу можно отключить. Зависит от служб «NetBios через TCP/IP», «Драйвер протокола TCP/IP» и «Среда сетевой поддержки AFD».Тип запуска / Вход от имени – Авто / Локальная система.

7.1.3 DNS

DNS – клиент. Разрешает для данного компьютера DNS – имена в адресе и помещает их в кэш.

Если служба остановлена, то не разрешаются DNS – имена и нельзя разместить службу каталогов Active Directory контроллеров домена. Если Active Directory не используется и нет сети, службу можно отключить. Зависит от службы «Драйвер протокола TCP/IP». Тип запуска / Вход от имени – Авто/Сетевая служба.

7.2 Службы контроля характеристик

7.2.1 Адаптер производительности

WMI – Предоставляет информацию о библиотеках производительности от поставщиков WMI HiPerf. Если у системы нет резидентов, вроде MBM, PC Alert и прочего, то эту службу можно отключить. Зависит от службы «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Вручную / Локальная система.

7.2.2 Беспроводная настройка

Предоставляет автоматическую настройку 802.11 адаптеров. Если таковых нет, тогда службу следует отключить. Зависит от служб «Удаленный вызов процедур (RPC)» и «NDIS – протокол ввода/вывода пользовательского режима». Тип запуска / Вход от имени – Авто / Локальная система.

7.2.3 Защита журнала проверки

Осуществляя отслеживание подозрительной деятельности в информационной системе, следует защищать целостность записей журнала проверки, чтобы гарантировать точность и полноту информации.

7.3. Службы управления ошибочными ситуациями

7.3.1 Служба администрирования диспетчера логических дисков

Выполняет настройку жестких дисков и томов. Эта служба выполняется только во время процессов настройки: запуск / Вход от имени – Вручную / Локальная система.

7.3.2 Служба восстановления системы

Выполняет функции восстановления системы. Чтобы остановить службу следует отключить восстановление системы на вкладке «Восстановление системы» свойств компьютера. Насчет целесообразности отключения данной службы: если достаточно места на диске и хватает ресурсов компьютера, то рекомендуется оставить эту службу работать. Можно только запретить функцию восстановления дисков для тех разделов, где у вас находятся динамические архивы (которые постоянно обновляются). Зависит от службы «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Авто / Локальная система.

7.3.3 Служба времени

Windows. Управляет синхронизацией даты и времени на всех клиентах и серверах в сети. Если эта служба остановлена, синхронизация даты и времени не будет доступна. Можно отключить. Тип запуска / Вход от имени – Авто / Локальная система.

7.4. Службы учета и безопасности систем

7.4.1 Защищенное хранилище

Обеспечивает защищенное хранение секретных данных, таких, как закрытые ключи, используется для предотвращения несанкционированного доступа служб, процессов или пользователей. Можно отключить, особенно при отсутствии Internet. Зависит от службы «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Авто / Локальная система.

7.4.2 MS Software Shadow Copy Provider

Управляет теневыми копиями, полученными при помощи теневого копирования тома. Можно отключить. Зависит от службы «Удаленный вызов процедур (RPS)». Тип запуска / Вход от имени – Авто / Локальная система.

7.4.3 NetMeeting Remote Desktop Sharing

Разрешает проверенным пользователям получать доступ к рабочему столу Windows, используя NetMeeting. Можно отключить. Тип запуска / Вход от имени – Вручную / Локальная система.

7.4.4 Диспетчер учетных записей безопасности

Хранит информацию о безопасности учетной записи локального пользователя. Целесообразно не отключать. Зависит от службы «Удаленный вызов процедур (RPC)». От данной службы зависит «Координатор распределенных транзакций». Тип запуска / Вход от имени – Авто / Локальная система.

7.5. Службы управления общего пользования

7.5.1 Machine Debug Manager

Управляет местной и удаленной отладкой с помощью компонен-товVisual Studio. Появляется после установки Office, можно отключить. Зависит от службы «Удаленный вызов процедур (RPS)». Тип запуска / Вход от имени – Авто / Локальная система.

7.5.2 Доступ к HID- устройствам

Обеспечивает универсальный доступ к HID-устройствам (Human Interface Devices), который активизирует и поддерживает использование заранее определенных клавиш быстрого вызова на клавиатуре, устройствах управления или иных устройствах мультимедиа. Служба отключена по умолчанию (если нет таковых устройств). Зависит от службы «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Отключено / Локальная система.

7.6. Службы

7.6.1 ИБП

Служба, управляющая подключенным к компьютеру источником бесперебойного питания (ИБП).

7.6.2 ISM

Служба, поддерживающая транспорты для асинхронного обмена сообщениями между узлами. Каждый транспорт выполняет две основные функции: приемо-передача и топологические запросы (например, какие узлы соединены данным транспортом и какова стоимость соединения). В состав Windows входят две службы межузлового обмена сообщениями – RPC и SMTP (почта).

7.6.3 LPD

Служба сервера печати, получающая документы (задания печати) от программ LPR, выполняемых клиентскими системами.

7.6.4 MARS

Служба сопоставления IP-адресов многоадресной рассылки адресам ATM клиентов, входящих в группу многоадресной рассылки. Для распределения данных многоадресной рассылки через многоточечные подключения MARS может работать совместно с MCS и клиентами.

7.6.5 TGS

Служба Kerberos V5, предоставляемая центром распространения ключей (KDC) Kerberos V5, которая выдает билеты, позволяющие пользователям проверять подлинность служб домена.

7.6.6 WINS (WINDOWS INTERNET NAME SERVICE)

Программная служба, динамически сопоставляющая IP-адреса именам компьютеров (именам NetBIOS). Это позволяет пользователям осуществлять доступ к ресурсам по именам, а не по IP-адресам, распознавание и запоминание которых труднее. Серверы WINS обеспечивают поддержку клиентов с операционными системами Microsoft Windows NT 4.0 и более ранних версий.

7.6.7 Служба журналов событий

Служба, выполняющая регистрацию событий в системном журнале, журнале безопасности и журнале приложений. Служба журнала событий вызывается в окне просмотра событий.

7.6.8 Служба каталогов

Источник сведений каталога, а также служба, обеспечивающее доступ к этим сведениям и их использование. Служба каталогов позволяет находить объекты по любому из их атрибутов.

7.6.9 Служба кластеров

Обязательный программный компонент, управляющий всеми элементами работы кластера и обслуживающий его базу данных. Каждый узел кластера серверов выполняет один экземпляр службы кластеров.

7.6.10 Служба обозревателя сети

Служба, поддерживающая текущий список компьютеров, а также предоставляющая этот список по запросу приложениям. Обозреватель компьютеров выводит также списки компьютеров в диалоговых окнах **Мое сетевое окружение**, **Выбор компьютера** и **Выбор домена**, а также (только для Windows 2000 Server) в окне диспетчера серверов.

7.6.11 Служба оповещения

Служба, используемая сервером и другими службами для уведомления пользователей и компьютеров о происходящих системных событиях. Для работы службы оповещения необходима служба сообщений.

7.6.12 Служба сетевого DDE

Служба, предоставляющая сетевой транспорт и защиту для сеансов связи DDE.

7.6.13 Служба сообщений

Компонент, отвечающий за отправку и прием сообщений администраторов или службы оповещения.

7.6.14 Служба текстового ввода

Программа, обеспечивающая ввод и редактирование текста пользователем. Службы текстового ввода включают раскладки клавиатур, программы распознавания рукописного ввода и речи, а также редакторы методов ввода (IME). Редакторы методов ввода (IME) служат для ввода с клавиатуры знаков восточно-азиатских языков.

7.6.15 Служба факсов

Системная служба, обеспечивающая работу с факсимильными сообщениями для локальных и удаленных клиентов. Она позволяет получать и отправлять документы, а также использовать мастер рассылки факсов и электронную почту.

7.6.16 Служба IIS

Программные службы, поддерживающие создание, настройку и управление Web-узлами, а также другие средства Internet. Службы IIS включают протоколы NNTP, FTP и SMTP.

7.6.17 Служба NDS

Распределенная база данных в сетях Novell NetWare 4.0, содержащая сведения о каждом ресурсе сети и предоставляющая доступ к этим ресурсам.

7.6.18 Служба маршрутизации

Служба маршрутизации сообщений сервера системы «Очередь сообщений». При соответствующей настройке эта служба может применяться для:

- организации связи между компьютерами, использующими разные сетевые протоколы;

- уменьшения числа сеансов при использовании в качестве шлюза для всех входящих или исходящих сообщений независимых клиентов;

- маршрутизации сообщений между узлами посредством маршрутных ссылок.

7.6.19 Служба установки

Программные службы, позволяющие администратору осуществлять удаленную настройку клиентских компьютеров без посещения соответствующих рабочих мест. Клиентские компьютеры должны поддерживать удаленную загрузку.

Лекция 8. Службы регистрации сбора и обработки информации

8.1.1 Диспетчер логических дисков:

Обнаружение и наблюдение за новыми жесткими дисками и передача информации о томах жестких дисков службе управления диспетчера логических дисков. Если эта служба остановлена, то состояние дисков и информация о конфигурации не обновляется. Лучше оставить «Авто», если подключаются дополнительные диски. Зависит от служб «Plug and Play» и «Удаленный вызов процедур (RPC)». От данной службы зависит «Служба администрирования диспетчера логических дисков». Тип запуска / Вход от имени – Авто / Локальная система.

8.1.2 Диспетчер очереди печати

Загружает в память файлы для последующей печати. Полезная вещь, если есть принтер, тогда следует оставить «Авто». Зависит от службы «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Авто / Локальная система.

8.1.3 Диспетчер авто-подключений удаленного доступа

Диспетчер авто-подключений удаленного доступа. Создает подключение к удаленной сети, когда программа обращается к удаленному DNS- или NetBIOS-имени (адресу). Можно отключить, тогда при автономном просмотре Web-страниц система не будет пытаться лезть в Internet. Зависимости – «Диспетчер подключений удаленного доступа», «Телефония». Тип запуска / Вход от имени – Вручную / Локальная система.

8.1.4 Диспетчер подключений удаленного доступа

Создает сетевое подключение. Если есть модем, то службу необходимо оставлять «Вручную». Зависит от службы «Телефония». От данной службы зависят «Брандмауэр Internet (ICF) / Общий доступ к Internet (ICS)» и «Диспетчер авто-подключений удаленного доступа». Тип запуска / Вход от имени – Вручную / Локальная система.

8.1.5 Диспетчер сеанса справки для удаленного рабочего стола

Управляет возможностями «Удаленного помощника». Перед остановкой службы в окне «Свойства» на вкладке «Зависимости» проверяются зависимости служб. Зависит от службы «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Вручную / Локальная система.

8.1.6 Служба индексирования

Индексирует содержимое и свойства файлов на локальном и удаленных компьютерах, обеспечивает быстрый доступ к файлам с помощью языка запросов. С поиском средствами Windows XP имеются проблемы. Зависит от службы «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Вручную / Локальная система.

8.1.7 Служба обнаружения SSDP

Включает обнаружение UPnP-устройств в домашней сети. Реально пользы в наших условиях от нее мало. От данной службы зависит «Узел универсальных PnP-устройств». Тип запуска / Вход от имени – Вручную / Локальная служба.

8.2. Службы сбора и обработки информации

8.2.1 Диспетчер отгрузки

Управляет синхронной и асинхронной передачей файлов между клиентами и серверами в сети. Если эта служба остановлена, синхронная и асинхронная передача

файлов между клиентами и серверами в сети не будет выполняться. Если сети нет, то службу лучше отключить. Зависит от службы «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Авто / Локальная система.

8.2.2 Журнал событий

Обеспечивает поддержку сообщений журналов событий, выдаваемых Windows – программами и компонентами систем, и просмотр этих сообщений. Эта служба не может быть остановлена. От данной службы зависит «Инструментарий управления Windows». Тип запуска / Вход от имени – Авто / Локальная система.

8.2.3 Журналы и оповещения производительности

Управляет сбором данных о производительности с локального или удаленного компьютеров, выполняемых на основе заданного расписания, обеспечивая запись этих данных в журналы или инициируя оповещение. Службу можно отключить. Если эта служба остановлена, то данные о производительности не собираются. Тип запуска / Вход от имени – Вручную / Сетевая служба.

8.2.4 Диспетчер сетевого DDE

Управляет сетевыми общими ресурсами динамического обмена данными (DDE). Если эта служба остановлена, ресурсы DDE будут не доступны. При отсутствии сети службу лучше отключить. От данной службы зависит «Служба сетевого DDE». Тип запуска / Вход от имени – Вручную / Локальная система.

8.2.5 Диспетчер сканеров и цифровых камер

Если таковых нет, то службу лучше отключить (хотя при этом она часто уже сама выключена). Зависит от службы «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Авто / Локальная система.

8.2.6 Служба сетевого DDE

Обеспечивает сетевой транспорт и безопасность динамического обмена данными (DDE) для программ, выполняющихся на одном или на различных компьютерах. Если сети нет, то службу лучше отключить. Зависит от службы «Диспетчер сетевого DDE». От данной службы зависит «Сервер папки обмена». Тип запуска / Вход от имени – Вручную / Локальная система.

8.2.7 Служба сетевого расположения (NLA)

Собирает и хранит сведения о размещении и настройках сети, а также уведомляет приложения об их изменении. Опять же, если сети нет, то и нет надобности в этой службе. Зависит от служб «Драйвер протокола TCP/IP», «Среда сетевой поддержки AFD», а от данной службы зависит «Брандмауэр Internet (ICF) / Общий доступ к Internet (ICS)». Тип запуска / Вход от имени – Вручную / Локальная система.

8.2.8 Служба сообщений

Посылает и получает сообщения, переданные администраторами или службой оповещений. Данная служба не имеет отношения к программе Windows Messenger. Можно отключить. Зависит от следующих компонентов: «Plug and Play», «Интерфейс NetBIOS», «Рабочая станция», «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Авто / Локальная система.

8.2.9 Служба шлюза уровня приложения

Оказывает поддержку сторонних протоколов PnP для общего доступа к подключению к Internet и подключений к Internet с использованием брандмауэра. Если встроенный брандмауэр не используется, то можно отключить. От данной службы зависит «Брандмауэр Internet (ICF) / Общий доступ к Internet (ICS)». Тип запуска / Вход от имени – Вручную / Локальная служба.

8.2.10 Службы IPSEC

Сервис безопасности протокола TCP/IP. Если вы не пользуетесь этим протоколом, то можно этот сервис выключить. Эта служба зависит от «Драйвер IPSEC» и «Драйвер протокола TCP/IP», «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Авто / Локальная система.

8.3. Программа «Сведения о системе»

Программа «Сведения о системе» собирает и отображает данные о конфигурации системы, как для локальных, так и для удаленных компьютеров. Сюда входит информация о конфигурации оборудования, компонентах компьютера, а также программном обеспечении, в том числе о подписанных и неподписанных драйверах. При устранении неполадок, связанных с конфигурацией системы, сотрудникам службы технической поддержки необходимы определенные данные о компьютере. Программа «Сведения о системе» позволяет быстро собрать необходимые данные.

Для хранения данных о системе предназначены файлы с расширением .nfo. Кроме того, программа «Сведения о системе» работает с файлами форматов .cab и .xml. Содержимое открытого файла .cab можно просматривать средствами меню **Сервис**.

«Сведения о системе» – это корневой узел в дереве категорий программы. Когда он выделен, в области сведений отображаются данные общего характера о компьютере и его операционной системе. Здесь можно узнать название операционной системы, ее версию, изготовителя и местоположение системного каталога. Кроме того, можно сверить версию BIOS или EFI, тип процессора и объем памяти.

С помощью корневого узла можно:

- узнать версию и дату изготовления BIOS или EFI;
- определить каталог, в котором установлена операционная система;
- убедиться в том, что новая память установлена правильно (параметры Total Physical Memory и Available Physical Memory);
- проверить параметр Page File Space при наличии неполадок в работе памяти. Значение этого параметра соответствует размеру физического пространства на жестком диске, используемого операционной системой для увеличения виртуального размера ОЗУ;
- проверить состояние активизации продукта. Если операционная система активизирована, в области сведений отсутствуют какие-либо дополнительные данные.

8.3.1 Управление программой «Сведения о системе» из командной строки

Помимо средства «Сведения о системе», доступном в окне «Центр справки и поддержки», для просмотра данных об управляемом компьютере можно использовать команду msinfo32.

8.3.2 Запуск программы

Чтобы запустить системное средство:

1. Запускается программа «**Сведения о системе**».
2. В меню **Сервис** выбирается команда, соответствующая необходимому средству.
3. Чтобы запустить программу «Сведения о системе», необходимо нажать кнопку **Пуск** и выбрать команду **Справка и поддержка**. Нажать кнопку **Поддержка** на панели инструментов, затем щелкните ссылку **Расширенные сведения о системе** в группе **Средства и ссылки** в левой части окна. В правой части окна щелкнуть ссылку **Просмотр дополнительных сведений о системе**.
4. Для получения сведений о конкретном средстве щелкнуть ссылку «См. также» или нажать кнопку **Справка** (если она имеется в окне программы).
5. При обращении в службу технической поддержки с целью устранения неполадок в системе может потребоваться запуск данных средств.

Лекция 9. Службы планирования и развития

9.1. Службы планирования

9.1.1 Планировщик заданий

Позволяет настраивать расписание автоматического выполнения задач на данном компьютере. Если не используется, то необходимо отключить. Зависит от службы «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Авто / Локальная система.

9.1.2 Поставщик поддержки безопасности NT LM

Поставщик поддержки безопасности NT LM – аутентификация на серверах NT и доступ к ресурсам домена. Актуален при наличии сети. От данной службы зависят **Telnet** . Тип запуска / Вход от имени – Вручную / Локальная система.

Если после отключения какой-либо службы в **Журнале просмотра** событий появляются красные отметки, как, например, после отключения «Службы COM записи компакт-дисков IMAPI», то их можно отключить следующим образом: Администрирование / Службы компонентов → Корень консоли → Службы компонентов → Компьютеры → Мой компьютер → Настройка DCOM → Microsoft IMAPI → Свойства → Расположение, убираем пометку «Запустить приложение на данном компьютере».

9.1.3 Уведомление о системных событиях

Протоколирует системные события, такие как регистрация в Windows, в сети и изменения в подаче электропитания. Уведомляет подписчиков из разряда «COM+ системное событие», рассылая оповещения. Следует оставлять без изменений. Зависит от «Системы событий COM+». Тип запуска / Вход от имени – Авто / Локальная система.

9.1.4 QoS RSVP

Обеспечивает рассылку оповещений в сети и управление локальным трафиком для QoS – программ и управляющих программ. Рекомендуется отключать. Простое отключение службы ни к чему не приведет – система по-прежнему будет резервировать 20 % от канала связи. Поэтому следует поступать следующим образом (под правами «Администратора»):

1) запускается оснастка **Групповая политика** (**Пуск → Выполнить → gpedit.msc**);

2) далее раздел **Конфигурация компьютера → Административные шаблоны → Сеть → Диспетчер пакетов QoS → Ограничить резервируемую пропускную способность**;

3) в открывшемся окне отметить пункт **Включен** и указать лимит канала в 0 %. Затем ОК – и выход из программы;

4) открываются свойства **Сетевого подключения**, где на закладке Сеть следует убедиться, что протокол **Планировщик пакетов QoS** подключен. Если его там нет, то необходимо добавить его (через кнопку **Установить**);

5) перезагружается компьютер.

Зависит от «Драйвера протокола TCP/IP», «Среды сетевой поддержки AFD» и «Удаленного вызова процедур (RPC)». Тип запуска / Вход от имени – Вручную / Локальная система.

9.2 Службы развития

9.2.1 Рабочие станции

Обеспечивают поддержку сетевых подключений и связь. Тип запуска определяется наличием сети. От данной службы зависят следующие компоненты: «Локатор удаленного вызова процедур (RPC)», «Обозреватель компьютеров», «Оповещатель», «Сетевой вход в систему», «Служба сообщений» и «Фоновая интеллектуальная служба передачи». Тип запуска / Вход от имени – Авто / Локальная система.

9.2.2 Удаленный вызов процедур (RPC)

Обеспечивает сопоставление конечных точек и иных служб RPC. От этой службы зависит более 39 компонентов, поэтому лучше не рисковать – оставлять службу как «Авто». Тип запуска / Вход от имени – Авто / Локальная система.

9.2.3 Удаленный реестр

Позволяет удаленным пользователям изменять параметры реестра на локальном компьютере. Если эта служба остановлена, то реестр может быть изменен только локальными пользователями, работающими на этом компьютере. Зависит от компонента «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Вручную / Локальная служба.

9.2.4 Узел универсальных PnP- устройств

Поддерживает универсальные PnP-устройства узла. Следует оставлять «Вручную». Зависит от компонента «Служба обнаружения SSDP». Тип запуска / Вход от имени – Вручную / Локальная служба

9.2.5 Управление приложениями

Обеспечивает службы установки программного обеспечения, такие, например, как назначение, публикация и удаление. Лучше оставлять без изменений, поскольку могут появиться проблемы с установкой и удалением программ, у которых установщик отличается от MSI. Тип запуска / Вход от имени – Вручную / Локальная система.

9.2.6 Telnet

Позволяет удаленному пользователю входить в систему и запускать программы, поддерживает различных клиентов TCP/IP Telnet, включая компьютеры с операционными системами UNIX и Windows. Если эта служба остановлена, то удаленный пользователь не сможет запускать программы. Лучше отключить. Зависит от служб «Драйвер протокола TCP/IP», «Поставщик поддержки безопасности NT LM» и «Удаленный вызов процедур (RPC)». Тип запуска /Вход от имени – Вручную /Локальная система.

9.2.7 Windows Audio

Управление звуковыми устройствами для Windows-программ. Если эта служба остановлена, звуковые устройства и эффекты не будут работать должным образом. Лучше оставлять без изменений. Зависит от служб «Plug and Play» и «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Авто / Локальная система.

9.2.8 Windows Installer

Устанавливает, удаляет или восстанавливает программное обеспечение в соответствии с инструкциями файлов MSI. Лучше оставлять – «Вручную». Зависит от службы «Удаленный вызов процедур (RPC)». Тип запуска / Вход от имени – Вручную / Локальная система.

9.2.9 Автоматическое обновление

Включает загрузку и установку критических обновлений Windows . Если эта служба выключена, то обновление операционной системы может выполняться вручную с сервера Windows Update. Рекомендуется отключить. Тип запуска / Вход от имени – Авто / Локальная система.

9.3. Службы планирования синхронизации автономных элементов

9.3.1 Запуск мастера расписания синхронизации

1. Запустить диспетчер синхронизации.

2. Нажать кнопку **Установка** и выбрать вкладку **Назначено**.

3. Нажать кнопку **Добавить** для запуска мастера расписания синхронизации, упрощающего процесс планирования.

4. Для синхронизации отдельных файлов, папок или веб-страниц в проводнике Windows, окне «Мой компьютер» или Internet Explorer следует указать элемент, который необходимо синхронизировать, а затем в меню **Сервис** выбрать команду **Синхронизировать**.

5. Диспетчер синхронизации также можно запустить из командной строки. Нажать кнопку **Пуск**, выбрать команду **Выполнить** и ввсти **mobsync**, а затем нажать кнопку **OK**.

6. Для изменения или удаления имеющегося расписания синхронизации следует выбрать расписание на вкладке **Назначено**, а затем нажать кнопку **Изменить** или **Удалить**.

9.3.2 Синхронизация автономных элементов во время простоя компьютера

1. Запустить диспетчер синхронизации.

2. Нажать кнопку **Установка** и выбрать вкладку **При простое**.

3. В списке **При использовании данного сетевого подключения** выбрать нужное сетевое подключение.

4. В списке **Синхронизовать следующие отмеченные объекты** установите флажки рядом с автономными элементами, которые следует синхронизировать, например рядом с папкой на подключенном сетевом диске или Web-страницей, доступной в автономном режиме в обозревателе Internet Explorer.

5. Установить флажок **Синхронизовать выбранные объекты в ждущем режиме**.

- Для синхронизации отдельных файлов, папок или веб-страниц в проводнике Windows, окне «Мой компьютер» или Internet Explorer следует указать элемент, который необходимо синхронизировать, а затем в меню **Сервис** выбрать команду **Синхронизировать**.

- Диспетчер синхронизации также можно запустить из командной строки. Нажать кнопку **Пуск**, выбрать команду **Выполнить** и ввести **mobsync**, а затем нажать кнопку **ОК**.

- Для каждого сетевого подключения может быть задана своя настройка синхронизации.

- Для синхронизации автономных элементов при работе компьютера от батарей запустить **диспетчер синхронизации**. Нажать кнопку **Установка** в нижней части диалогового окна **Синхронизируемые объекты**. Откроется диалоговое окно **Параметры синхронизации**. Выбрать вкладку **При простое**. Убедитесь, что в верхнем поле отображается нужное сетевое подключение. Нажать кнопку **Другие**. Откроется диалоговое окно **Параметры синхронизации при простое**, содержащее параметры для настройки синхронизации, в том числе флажок, запрещающий синхронизацию при питании компьютера от батарей.

9.3.3 Планирование архивации

Чтобы запланировать архивацию:

1. Запустить приложение **Архивация**. По умолчанию программа архивации запускается в режиме мастера, если этот режим не отключен.

2. Нажать кнопку **Расширенный** в окне мастера архивации.

3. Перейти на вкладку **Архивация** и выбрать в меню **Задание** команду **Создать**.

4. Выбрать файлы и папки для архивации, установив флажки в списке **Установите флажки для всех объектов, которые вы хотите заархивировать**.

5. Выбрать в списке **Размещение архива** пункт **Файл** или накопитель на магнитной ленте и сохранить список выбранных файлов и папок, выбрав в меню **Задание** команду **Сохранить выделенные**.

6. В поле **Носитель архива или имя файла** ввести путь и имя файла архива или выбрать ленту.

7. Задать параметры архивации – тип архива и тип журнала, выбрав в меню **Сервис** команду **Параметры**. После этого нажать кнопку **ОК**.

8. Нажать кнопку **Запуск** и внести изменения в диалоговом окне **Сведения о задании архивации**.

9. Чтобы задать дополнительные параметры архивации, например проверку данных или аппаратное сжатие, нажать кнопку **Дополнительно**. Завершив задание дополнительных параметров, нажать кнопку **ОК**.

10. В диалоговом окне **Сведения о задании архивации** нажать кнопку **Расписание**.

11. В диалоговом окне **Указание учетной записи** ввести имя и пароль пользователя, учетная запись которого будет использована при выполнении данного запланированного задания архивации.

9. В поле **Имя задания** диалогового окна **Параметры запланированного задания** ввести имя данного задания архивации и нажать кнопку **Свойства**, чтобы указать дату, время и частоту выполнения этого задания. По завершении нажмите кнопку **ОК**, затем еще раз нажать кнопку **ОК**:

- программа архивации позволяет архивировать данные с томов FAT16, FAT32 и NTFS. Данные, архивированные с тома NTFS Windows, рекомендуется восстанавливать

также на том NTFS Windows; в противном случае могут быть утеряны данные и свойства файлов и папок. Некоторые файловые системы могут поддерживать не все средства других файловых систем. Например, при восстановлении на томе FAT или томе NTFS Windows NT 4.0 данных, архивированных с тома NTFS Windows, будут утеряны разрешения, параметры шифрованной файловой системы (EFS), сведения о дисковых квотах, присоединенных дисках и внешних хранилищах.

- архивация файлов и папок может проводиться только администратором или оператором архива;

- чтобы запустить архивацию, следует нажать кнопку **Пуск** и выбрать команды **Программы**, **Стандартные**, **Служебные** и **Архивация данных**;

- если планируется архивация на ленту, лучше воспользоваться службой Съемные ЗУ, чтобы убедиться, что эта лента доступна в пуле носителей архивации;

- для возможности планирования заданий должна быть запущена служба планировщика заданий. Чтобы запустить ее, надо открыть окно командной строки и ввести **net start schedule**. Запуск, остановку и просмотр состояния служб можно также осуществлять в разделе «Службы» оснастки «Управление компьютером»;

- чтобы заархивировать данные состояния системы, включающие такие компоненты, как реестр и служба каталогов Active Directory, необходимо установить флажок **Состояние системы** в списке **Установите флажки для всех объектов, которые вы хотите заархивировать**;

- архивация данных состояния системы возможна только для локального компьютера. Данные состояния системы для удаленного компьютера архивировать нельзя;

- в диалоговом окне **Параметры запланированного задания** можно удалить запланированное задание архивации, нажав кнопку **Удалить**;

- после того, как задание запланировано, его параметры можно изменить, перейдя на вкладку **Запланированные задания** и щелкнув значок архива, отображающийся в календаре;

- операторы архива и администраторы могут архивировать и восстанавливать зашифрованные файлы и папки, не расшифровывая их.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

6.1.1. Перечень основной литературы

1. Власов, Ю. В. Администрирование сетей на платформе MS Windows Server : учеб. пособие / Ю.В. Власов, Т.И. Рицкова. - М. : Интернет-Университет Информационных Технологий, 2010. - 384 с. : ил. - (Основы информационных технологий). - Библиогр.: с. 383. - ISBN 978-5-94774-858-1.

2. Архитектура ЭВМ и систем : учебное пособие / Ю.Ю. Громов, О.Г. Иванова, М.Ю. Серегин и др. ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2012. - 200 с. - Библиогр. в кн; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=277352.

6.1.2. Перечень дополнительной литературы

1. Ригс, С. Администрирование PostgreSQL 9. Книга рецептов=PostgreSQL 9. Administration Cookbook : учебное пособие / С. Ригс, Х. Кросинг ; пер. с англ. Е.В. Самохвалов. - М. : ДМК Пресс, 2012. - 364 с. : ил., табл., схем. - ISBN 978-5-94074-750-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=260267

2. Максимов, Н. В. Архитектура ЭВМ и вычислительных систем : [учебник] / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М. : ФОРУМ, 2010. - 512 с. : ил. - (Профессиональное образование). - На учебнике гриф: Рек.МО. - Библиогр.: с. 463-464. - ISBN 978-5-91134-374-3

6.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по выполнению лабораторных работ по дисциплине «Администрирование информационных систем»
2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Администрирование информационных систем»

6.3. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1. Национальный Открытый Университет. Интуит. http://www.intuit.ru;
2. Федеральный портал «Российское образование. http://www.edu.ru;
3. Российская государственная библиотека. http://www.rsl.ru;
4. Институт Юнеско по информационным технологиям в образовании. http://ru.iite.unesco.org/publications.