

Департамент образования вологодской области
бюджетное профессиональное образовательное учреждение
Вологодской области
«ВОЛОГОДСКИЙ СТРОИТЕЛЬНЫЙ КОЛЛЕДЖ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к практическим работам
по МДК 01.01. Эксплуатация информационной системы
ПМ.01. Эксплуатация и модификация информационных систем

Специальность 09.02.04 Информационные системы (по отраслям)

2017 г.

Рассмотрено на заседании предметной цикловой комиссии общепрофессиональных, специальных дисциплин и дипломного проектирования по специальностям 08.02.01 «Строительство и эксплуатация зданий и сооружений», 08.02.07 «Монтаж и эксплуатация внутренних сантехнических устройств, кондиционирования воздуха и вентиляции», 43.02.08 «Сервис домашнего и коммунального хозяйства».

Данные методические указания предназначены для студентов специальности 09.02.04 «Информационные системы (по отраслям)» БПОУ ВО «Вологодский строительный колледж» при выполнении практических работ по МДК 01.01. Эксплуатация информационной системы

Объем практических работ по МДК 01.01. Эксплуатация информационной системы составляет 60 часов.

Автор: Норина С.В., преподаватель БПОУ ВО «Вологодский строительный колледж»

СОДЕРЖАНИЕ

	стр
ПОЯСНИТЕЛЬНАЯ ЗАПИСКА	4
ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ ЗАНЯТИЙ	6
ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ:	7
Практическая работа №1. Анализ информационной среды предприятия	
Практическая работа №2. Анализ технической документации информационной системы.	
Практическая работа №3. . Анализ и разработка регламентов технического сопровождения информационной системы.	
Практическая работа №4. Выбор рационального состава аппаратно-программного обеспечения информационной системы.	
Практическая работа №5. Настройка серверного программного обеспечения	
Практическая работа №6. Установка клиентского программного обеспечения	
Практическая работа №7. Конфигурирование клиентского программного обеспечения	
Практическая работа №8«Настройка сети и поиск неисправностей в среде конкретных операционных систем»	
Практическая работа №9. . Настройка сети и поиск неисправностей в среде конкретных операционных систем.	
Практическая работа №10. «Организация удаленного доступа»	
Практическая работа №11. Организация удаленного доступа	
Практическая работа №12. Мониторинг и оптимизация корпоративных сетей.	
Практическая работа №13. Конфигурация учетной записи пользователя.	
Практическая работа №14. . Управление профилями пользователей.	
Практическая работа №15. Планирование стратегии управления доступом.	
Практическая работа №16. Реализация стратегии управления доступом	
Практическая работа №17 Мониторинг событий безопасности.	
Практическая работа №18. Организация управления совместными ресурсами	
Практическая работа №19. . Архивация и синхронизация данных.	
Практическая работа №20 Выполнение резервного копирования данных в различных информационных системах. Перенос файлов и параметров.	
Практическая работа №21. Выполнение резервного копирования данных в различных информационных системах. Копирование файлов вручную.	
Практическая работа №22.. Планирование действий на случай аварийных ситуаций	
Практическая работа №23. Отказоустойчивость информационной системы.	
Практическая работа №24. Организация технической поддержки отказоустойчивости информационной системы.	
Практическая работа №25. Диагностика и восстановление информационных систем.	
Практическая работа № 26. Защита информации и управление доступом в базе данных.	
Практическая работа № 27. Проектирование стратегий резервного копирования баз данных.	
Практическая работа №28. Мониторинг и обработка транзакций.	
Практическая работа № 29. Восстановление информации в базе данных.	
Практическая работа №30. Технология управления базами данных средствами языка SQL	

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

МДК 01.01. Эксплуатация информационной системы входит в состав профессионального модуля ПМ.01. Эксплуатация и модификация информационных систем в составе профессионального учебного цикла программы подготовки специалистов среднего звена по специальности **09.02.04**

Информационные системы (по отраслям)

В результате освоения ПМ.01 обучающийся должен **иметь практический опыт:**

- • инсталляции, настройки и сопровождения одной из информационных систем;
- выполнения регламентов по обновлению, техническому сопровождению и восстановлению данных информационной системы;
- сохранения и восстановления базы данных информационной системы;
- организации доступа пользователей к информационной системе в рамках компетенции конкретного пользователя;
- обеспечения сбора данных для анализа использования и функционирования информационной системы и участия в разработке проектной и отчетной документации;
- определения состава оборудования и программных средств разработки информационной системы;
- использования инструментальных средств программирования информационной системы;
- участия в экспериментальном тестировании информационной системы на этапе опытной эксплуатации и нахождения ошибок кодирования в разрабатываемых модулях информационной системы;
- разработки фрагментов документации по эксплуатации информационной системы;
- участия в оценке качества и экономической эффективности информационной системы;
- модификации отдельных модулей информационной системы;
- взаимодействия со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности;

уметь:

- • осуществлять сопровождение информационной системы, настройку для пользователя согласно технической документации;
- поддерживать документацию в актуальном состоянии;
- принимать решение о расширении функциональности информационной системы, о прекращении эксплуатации информационной системы или ее реинжиниринге;
- идентифицировать технические проблемы, возникающие в процессе эксплуатации системы;
- производить документирование на этапе сопровождения;
- осуществлять сохранение и восстановление базы данных информационной системы;
- составлять планы резервного копирования, определять интервал резервного копирования;
- организовывать разноуровневый доступ пользователей информационной системы в рамках своей компетенции;
- манипулировать данными с использованием языка запросов баз данных, определять ограничения целостности данных;
- выделять жизненные циклы проектирования компьютерных систем;
- использовать методы и критерии оценивания предметной области и методы определения стратегии развития бизнес-процессов организации;
- строить архитектурную схему организации;
- проводить анализ предметной области;
- осуществлять выбор модели построения информационной системы и программных средств;
- оформлять программную и техническую документацию, с использованием стандартов оформления программной документации;
- применять требования нормативных документов к основным видам продукции (услуг) и процессов;
- применять документацию систем качества;
- применять основные правила и документы системы сертификации Российской Федерации;

знать:

- • основные задачи сопровождения информационной системы;

- регламенты по обновлению и техническому сопровождению обслуживаемой информационной системы;
- типы тестирования;
- характеристики и атрибуты качества;
- методы обеспечения и контроля качества;
- терминологию и методы резервного копирования;
- отказы системы;
- восстановление информации в информационной системе;
- принципы организации равноуровневого доступа в информационных системах, политику безопасности в современных информационных системах;
- цели автоматизации организации;
- задачи и функции информационных систем;
- типы организационных структур;
- реинжиниринг бизнес-процессов;
- основные модели построения информационных систем, их структуру, особенности и области применения;
- особенности программных средств используемых в разработке информационных систем;
- методы и средства проектирования информационных систем;
- основные понятия системного анализа;
- национальную и международную систему стандартизации и сертификации и систему обеспечения качества продукции, методы контроля качества

В соответствии с учебным планом на изучение МДК 01.01. Эксплуатация информационной системы отводится 180 часов, в том числе 60 часов – практические занятия.

Целью практических занятий является формирование практических умений, необходимых в последующей учебной и профессиональной деятельности.

Содержание практических занятий по МДК 01.01. Эксплуатация информационной системы направлено на реализацию требований Федерального государственного образовательного стандарта по специальности 09.02.04 Информационные системы (по отраслям)

Практическое занятие включает следующие структурные элементы:

- 1) инструктаж, проводимый преподавателем,
- 2) самостоятельная деятельность обучающихся,
- 3) анализ и оценка выполненных работ.

Контроль и оценка результатов выполнения обучающимися работ, заданий на практических занятиях направлены на проверку освоения умений, практического опыта, развития общих и формирование профессиональных компетенций, определённых программой учебной дисциплины.

Оценки за выполнение заданий на практических занятиях выставляются по пятибалльной системе и учитываются как показатели текущей успеваемости обучающихся.

ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

№ п/п	Тема программы	Тема работы	Количество часов
1	Тема 1.	Анализ информационной среды предприятия	2
2	Проблемы эксплуатации информационной системы	Анализ технической документации информационной системы	2
3		Анализ и разработка регламентов технического сопровождения информационной системы	2
4		Выбор рационального состава аппаратно-программного обеспечения информационной системы	2
5	Тема 2. Организация и поддержка операционной среды информационной системы	Инсталляция серверного программного обеспечения	2
6		Настройка серверного программного обеспечения	2
7		Установка клиентского программного обеспечения	2
8		Конфигурирование клиентского программного обеспечения	
9	Тема 3. Организация и поддержка сетевой инфраструктуры информационной системы	Настройка сети и поиск неисправностей в среде конкретных операционных систем	2
10		Настройка сети в смешанных средах	2
11		Организация удаленного доступа	2
12		Мониторинг и оптимизация корпоративной сети	
13	Тема 4. Организация разноуровневого доступа в информационных системах	Конфигурирование учетных записей пользователей	2
14		Управление профилями	2
15		Планирование стратегии управления доступом	2
16		Реализация стратегии управления доступом	2
17		Мониторинг событий безопасности	2
18	Тема 5. Организация резервного копирования данных информационной системы	Организация управления совместными ресурсами	2
19		Архивация и синхронизация данных	2
20		Выполнение резервного копирования данных в различных информационных системах	2
21		Выполнение резервного копирования данных в различных информационных системах	2
22	Тема 6. Отказы и восстановления информационной системы	Планирование действий на случай аварийных ситуаций	2
23		Организация технической поддержки отказоустойчивости информационной системы	2
24		Организация технической поддержки отказоустойчивости информационной системы	2
25		Диагностика и восстановление информационной системы	2
26	Тема 7. Эксплуатация корпоративной базы данных	Защита информации и управление доступом в базе данных	2
27		Проектирование стратегии резервного копирования базы данных	2
28		Мониторинг и обработка транзакций	2
29		Восстановление информации в базе данных	2
30		Технологии управления базами данных средствами языка SQL	2

ПОРЯДОК ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа №1. Анализ информационной среды предприятия.

Цель работы: познакомиться с понятиями: деятельность, информационное обеспечение, информационная потребность, информационная система, автоматизированные информационные системы; научиться анализировать информационную среду какого-либо предприятия на своем и на наглядном примере.

Оборудование, технические и программные средства: персональный компьютер, операционная система Windows 7.

Теоретическая часть:

Информация в деятельности организации

Информация – 1) сведения (отображение) о событии или состоянии реальной действительности, позволяющие принимать решения, ведущие к достижению цели предметной деятельности; 2) сведения (отображение) о событии или состоянии реальной действительности, представленные в виде фактов или данных; 3) (с точки зрения принятия решений) данные, оказывающие влияние на поведение системы, используемые в процессе принятия решений или в связи с осуществлением тех или иных действий.

Экономическая информация – совокупность сведений о социально-экономических процессах, служащих для управления этими процессами и коллективами людей в производственной и непроизводственной сфере.

Деятельность – всякого рода практическая активность, направленная на достижение определенной цели, Данным понятием охватываются и материально-практические, и интеллектуальные, духовные операции; деятельностью является работа мысли в такой же мере, как и работа руки, процесс познания в такой же мере, как человеческое поведение. Содержание деятельности составляет целесообразное преобразование окружающего мира в интересах людей.

Предметная деятельность – деятельность, направленная на решение задач, определённых в положении или уставе организации.

Информационное обеспечение организации

Информационное обеспечение – полный набор показателей, документов, классификаторов и кодификаторов информации, файлов, баз данных, баз знаний, методов их использования в предметной деятельности, а также способы представления, накопления, хранения, преобразования, передачи информации, принятые в конкретной системе для удовлетворения информационных потребностей пользователей в нужной форме и в требуемое время.

Информационное обеспечение организации – регулярная деятельность по получению информационного продукта или оказанию информационных услуг.

Информационная потребность – 1) определенное состояние субъекта предметной деятельности, возникающее в связи с необходимостью получения данных, обеспечивающих принятие решений в предметной деятельности (эффективное функционирование организации); 2) осознанное понимание различия между индивидуальным знанием о предмете и знанием, накопленным обществом.

Информационная технология

Информационная технология – совокупность знаний о способах и приёмах труда по переработке информации, его материально-вещественных компонентах и способах их соединения для получения информационного продукта или оказания информационных услуг.

Сотрудник организации, имеющий потребность в наличии значимых для предметной деятельности сведений, должен осуществлять практическую активность по получению, обработке и использованию информации, т.е. по устранению информационной неопределенности.

Информационная процедура – набор однородных в функциональном отношении действий (операций), регулярно осуществляемых сотрудниками организации с целью:

Ø – перемещения информации в пространстве (сбор, распределение, передача, коммутация информационных потоков и т.п.);

Ø – преобразования её во времени (ввод, вывод, хранение, обработка информации и т.п.) инвариантно к способу реализации процедуры и используемым ресурсом.

Информационный процесс – совокупность логически упорядоченных, взаимосвязанных и организованных информационных процедур (функций), ведущая к достижению цели информационного обеспечения предметной деятельности.

Информационная система

Информационная система – система, в которой протекают информационные процессы, составляющие полный жизненный цикл информации: генерация, преобразование, передача, прием, хранение, обработка (использование), уничтожение.

Миссия информационных систем – информационное обеспечение предметной деятельности организации.

Характеристики и свойства информационных систем

Величина и сложность. Современные системы любой природы, как правило, являются большими и сложными системами.

Сложной системой большого масштаба называют систему, состоящую из большого числа взаимосвязанных и взаимодействующих между собой элементов и способную выполнять сложную функцию.

Воздействие случайных факторов. Характерной и весьма существенной особенностью является подверженность информационных систем влиянию случайных факторов, причем не только таких, как, например, отказы, сбои или ошибки технических устройств персонала или пользователей, но и таких, как злоумышленные действия людей, которые являются не только случайными, но и вообще непредсказуемыми или в лучшем случае трудно предсказуемыми.

Участие в информационных процессах человека. Особенность состоит в том, что конечным пользователем информационных систем всегда являются сотрудники организации. Персонал организации имеет свои интересы и цели, которые необходимо учитывать при информационном обеспечении (наличие свободы воли).

Уникальность. Каждое состояние информационной системы уникально и требует при информационном обеспечении учета всех ее особенностей и, следовательно, индивидуального применения различных воздействий.

Динамичность. Информационные системы с течением времени меняют свою структуру и состояние элементов.

Распределённость означает пространственное расположение отдельных компонент системы.

Состояние информационной системы – совокупность системно взаимосвязанных организационно-технических, процедурных, информационных и правовых структурных решений.

Дадим определения введенных понятий. Фиксированную организацию состава, количества, архитектуры (взаимосвязи) комплекса технических средств и систем, а также технического персонала и личного состава, непосредственно участвующего в выполнении информационных процедур, можно определить как состояние техникоорганизационной структуры информационной системы или как организационно-техническое структурное решение.

Фиксированную организацию состава, последовательности информационных процедур можно определить как состояние процедурной структуры информационной системы или как процедурное структурное решение.

Под правовой базой информационной технологии будем понимать состав нормативных документов, регулирующих информационное обеспечение в части функционирования информационной системы. Это могут быть: общие положения, функциональные обязанности личного состава, инструкции и наставления по приемам, способам и методам выполнения процедур и работе на технических средствах и др.

Автоматизированные информационные системы

Общая характеристика АИС

1. АИС – совокупность информации, экономико-математических методов и моделей, технических, программных, технологических средств и специалистов, предназначенная для обработки информации и принятия управленческих решений.

2. АИС – взаимосвязанная совокупность данных, оборудования, программных средств, персонала, стандартов, процедур, предназначенных для сбора, обработки, распределения, хранения, выдачи информации в соответствии с требованиями, вытекающими из целей организации.

Функциональные и обеспечивающие подсистемы

Автоматизированная информационная система имеет функциональную и обеспечивающую подсистемы.

Функциональная подсистема обеспечивает выполнение задач и назначение информационной системы. Обычно в информационной системе функциональная часть разбивается на подсистемы по функциональным признакам:

- уровень предметной деятельности, например управления (высший, средний, низший);
- вид управляемого ресурса (материальные, трудовые, финансовые и т.п.);
- сфера применения (банковские, фондового рынка и т.п.);
- функции управления и период управления.

Обеспечивающая подсистема включает «информационное, техническое, математическое, программное, методическое, организационное и лингвистическое обеспечение.

Практическая часть

Для описания информационной системы конкретной организации, рассмотрим организацию «ИП Абакумова О.Н АЗС №80». Организация занимается продажей горюче-смазочных материалов (ГСМ) с целью получения прибыли. В данном случае субъектом деятельности является организация, а объектом – потребитель ГСМ, т.е. покупатель.

Информационное обеспечение организации составляют различные документы (начиная от учредительных документов, договоров аренды и т.п. и заканчивая отчетами кассиров-операционистов).

Организация также обладает информационной потребностью. Например, операторы, занимающиеся отпуском ГСМ потребителям, должны быть информированы о качестве, производителе отпускаемой продукции. Чтобы в случае необходимости сообщить об этой информации покупателю. Также в организации должны иметься документы о реализуемой продукции (сертификаты соответствия, паспорта качества и т.п.), которые могут быть предъявлены покупателю, чтобы он мог лично удостовериться в качестве приобретаемой продукции.

Сотрудники организации имеют потребность в значимых сведениях для осуществления практической деятельности. Они осуществляют различные однородные операции с информацией, имеющейся в их распоряжении. Так операторы АЗС ведут учет о поступлении ГСМ. При поступлении ГСМ на АЗС оператор должен выписывать накладные в двух экземплярах, один из которых передается водителю, осуществившему перевозку ГСМ, а второй передается в бухгалтерию для составления отчетности по приходу материалов. Операторы также ведут журнал по приходу ГСМ и делают отметки в сменном отчете о поступивших ГСМ. Также оператору вместе с поступившими ГСМ передаются сертификаты соответствия и паспорта качества о данном продукте. Еще одна процедура осуществляемая операторами – это учет реализованных ГСМ. Каждый оператор по окончании своей смены пишет сменный отчет, в котором указывается количество реализованных нефтепродуктов, выручка, данные о поступивших нефтепродуктах. Сменные отчеты в конце месяца сдаются в бухгалтерию для проверки.

Задание: проанализировать информационную среду своего предприятия, учитывая все аспекты и параметры.

Бухгалтерские информационные системы (БУИС)

Бухгалтерская информационная система (БУИС) создается в целях получения информации, необходимой для управления производственной и хозяйственной деятельностью предприятия. БУИС служит связующим звеном между хозяйственной деятельностью и людьми, принимающими решения (рис. 1.1). В ней осуществляются сбор, регистрация данных о хозяйственной деятельности на предприятии, их обработка, хранение, передача пользователям для анализа и принятия решений. Таким образом, данные о хозяйственной деятельности являются входом в БУИС, а полезная информация для лиц, принимающих решения, - выходом из нее. Главная цель функционирования БУИС на предприятии - обеспечить руководство предприятия финансовой информацией для принятия обоснованных решений при выборе альтернативных вариантов использования ресурсов.



Рис. 1.1. Схема управления предприятием в условиях использования БУИС

Бухгалтерская система является наиболее важной из экономических систем, так как выполняет ведущую роль в управлении потоком информации о состоянии объекта управления и направлении ее во все подразделения предприятия, а также заинтересованным лицам вне-его. Прежде всего, она предоставляет количественные данные, необходимые для выполнения таких функций управления производственной и коммерческой деятельностью предприятия, как планирование, контроль и анализ.

Главными пользователями бухгалтерской информации являются руководство и менеджеры служб предприятия. На основе этой информации определяются чистая прибыль предприятия за последний отчетный период, соответствие нормы прибыли ожидаемой величине, наличие денежных ресурсов, соотношение чистых активов и уставного капитала, наиболее прибыльные направления деятельности, себестоимость производимой продукции. Бухгалтерская информация помогает руководителям не только понять и проанализировать итоги, но и прогнозировать результаты деятельности предприятия при принятии различных решений.

Существуют и внешние пользователи бухгалтерской информации. Это акционеры, инвесторы, кредиторы, покупатели, клиенты, аудиторы и инспектора налоговых служб. Акционерам и инвесторам важно знать, насколько эффективно и прибыльно используется собственный капитал владельцев предприятия, нужны ли ему новые инвестиции или их объем следует уменьшить, может ли фирма в будущем оставаться прибыльной и при каких условиях. Кредиторов интересуют вопросы о способности предприятия своевременно выплачивать проценты за кредит и в срок расплатиться с долгами. В этой связи бухгалтерская информация все в большей степени становится связанной с технико-экономическим обоснованием и с бизнес планированием при привлечении инвестиций. Государственные службы интересуются полнотой и правильностью определения прибыли и исчисления налогов, соблюдением антимонопольного и валютного законодательства.

Особенности функционирования БУИС на крупных предприятиях

Проблема автоматизации бухгалтерского учета на крупных предприятиях остается одной из актуальных и сложных в современных условиях. Это связано, прежде всего, с необходимостью сбора и переработки значительных объемов информации и своевременной выдачи результатов для их анализа и принята управленческих решений.

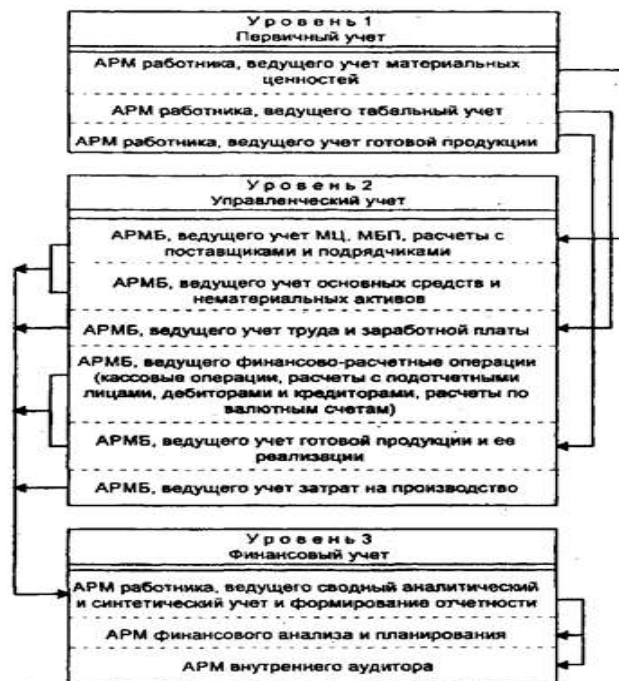


Рис. 1.2. Уровни учета

Для решения задачи повышения эффективности управления предприятием БУИС крупного предприятия должна обеспечивать:

- автоматизированное решение всего комплекса задач бухгалтерского учета, планирования, анализа финансово-хозяйственной деятельности предприятия, а также внутреннего аудита;
- получение оперативной, постоянно меняющейся информации о текущем состоянии дел на предприятии;
- возможность консолидированного управления и получения консолидированных финансовых отчетов.

Крупные предприятия могут иметь филиалы или удаленные склады. Кроме того, финансы такого предприятия могут принадлежать группе собственников. Поэтому актуальным является наличие в такой системе удаленных рабочих мест с возможностью осуществлять обмен данными для оперативного управления из центра.

На крупном предприятии обработка учетной информации с помощью БУИС ведется на трех уровнях учета:

1. первичном (сбор, регистрация, накопление, хранение информации и передача ее для дальнейшей обработки),
2. управленческом (сметы, нормативы, калькуляции)
3. финансовом (обобщение, синтез информации).

На каждом уровне в соответствии с методологией сбора, регистрации и обработки учетной информации создаются АРМ экономистов, бухгалтеров, финансистов и аналитиков, взаимодействующие между собой.

Применение АРМ для обработки данных непосредственно на рабочих местах специалистов различных уровней учета обеспечивает минимальное использование бумажных носителей, достоверность и полноту информации.

Особенности функционирования БУИС на предприятиях малого и среднего бизнеса

Существует несколько подходов к автоматизации бухгалтерского учета при создании БУИС на предприятиях малого и среднего бизнеса. Это связано с тем, что небольшие предприятия с простой и слаборазвитой структурой не требуют ведения управленческого учета как отдельной подсистемы.

При первом подходе создается система, автоматизирующая только финансовый учет. Такую БУИС относят к классу мини бухгалтерий. Как правило, бухгалтерский учет в этой системе ведется одним человеком - бухгалтером.

При втором подходе кроме финансового учета частично автоматизируется управленческий учет. В этом случае бухгалтерский учет ведут два человека

(бухгалтер и его помощник) либо на одном рабочем месте путем разграничения доступа, либо на двух рабочих местах.

Автоматизация финансового и управленческого учета достигается при третьем подходе. В такой системе при значительных объемах обрабатываемой информации используется многопользовательский режим. Несколько компьютеров объединяются в локальную сеть, а каждый из компьютеров рассматривается как отдельное рабочее место бухгалтера.

Выбор подхода зависит от типа предприятия и его размеров. В отличие от крупных предприятий на небольших предприятиях основное внимание уделяется ведению финансового учета, который по трудоемкости и значимости занимает главное место. Он направлен на обобщение и синтез учетной информации.

Ведение же учета по отдельным участкам, например таким, как учет труда и заработной платы, учет готовой продукции и ее реализации, учет основных средств и нематериальных активов, учет материальных ценностей, сводный учет и др., осуществляется посредством применения отдельных программных модулей (блоков).

Основная роль бухгалтера в этих условиях сводится к правильности оформления хозяйственных операций, принятию решений, анализу и контролю правильности формирования отчетной документации. Работа бухгалтера становится более рациональной, ПК превращается в главный инструмент его деятельности.

Программный комплекс для автоматизации бухгалтерского учета на малых и средних предприятиях представлен на рис 1.3.



Рис. 1.3. Структура программного комплекса автоматизации бухгалтерского учета на малых и средних предприятиях

В заключении обзора принципов функционирования БУИС перечислим некоторые рекомендации, которыми имеет смысл руководствоваться при выборе системы автоматизации бухгалтерского учета.

1. функциональное соответствие выбираемого пакета системе управления и бухучета на предприятии. Программа должна обеспечивать автоматизацию всех принятых на фирме процедур. Если это невозможно (например, в силу каких-то исторических причин на предприятии до сих пор применяются устаревшие, плохо формализуемые правила), следует убедиться в том, что можно будет быстро и без лишних хлопот привести свои методы управления в соответствие алгоритмам, заложенным в основу программного комплекса.

В первую очередь следует обратить внимание на специализированные «отраслевые» пакеты. Хотя, в общем, и в целом бухучет - вещь универсальная, но его отдельные разделы могут сильно зависеть от специфики деятельности предприятия.

2. Класс пакета. Все пакеты можно разделить на три класса - комплексы АРМ, интегрированные бухгалтерские пакеты и мини бухгалтерии. Небольшому предприятию ни к чему приобретать комплекс АРМ, в то время как автоматизация бухучета крупного завода с помощью мини бухгалтерии практически невозможна. Чтобы точнее определить, подходит ли предлагаемое

программное обеспечение (ПО) Вашей организации, следует изучить список клиентов, уже выбравших этот продукт, - по аналогии станет понятно, «ваша» эта программа или нет.

3. Взаимосвязанность всех модулей комплекса. Вся актуальная информация должна вводиться единожды и обрабатываться различными способами. Такое свойство системы называется «отсутствием повторного ввода данных».

Необходимо помнить, что при автоматизации предприятия «по кускам» есть большая вероятность возникновения ошибок на том или ином этапе. Поэтому, выбирая ПО, проследите, является ли оно частью комплексной системы или, по крайней мере, обеспечивает экспорт проводок в существующую бухгалтерскую программу. Хотя первоначальная автоматизация предприятия - дело, в общем-то, нелегкое, но замена пакета, переставшего удовлетворять вашим требованиям, - просто мучение.

4. Удобство пользовательского интерфейса. Этот критерий хотя и является субъективным, но очень важен. Поэтому рекомендуется сначала познакомиться с демонстрационной версией продукта, чтобы понять, насколько программа удобна именно для вас и легко ли будет ее освоить.

Следует обратить внимание на скорость ввода информации по первичным документам, вид экранных форм для этого ввода (насколько он приближен к первичным бланкам кассовых ордеров, платежных поручений, счетов и т.д.), возможность оперативного доступа к справочникам, корректировки и пополнения их содержимого и т.д.

5. Гибкость программы. Уже имеются бухгалтерские комплексы, адаптированные практически к любым, даже самым непредвиденным капризам нашего законодательства. Купив такое «гибкое» ПО, можно его использовать в течение нескольких лет, даже после исчезновения разработчика с рынка.

6. Наличие гарантийных обязательств и комплекс услуг, предоставляемых фирмой-разработчиком и ее дилерами. Программ без ошибок просто не бывает, а потому важно не столько их отсутствие, сколько скорость исправления (кстати, стоит поинтересоваться о ней у клиентов выбранной вами фирмы). Если разработчики отказываются от внедрения системы или обучения работе с ней, мотивируя это тем, что и так все ясно, то трудностей на первом этапе внедрения пакета вам не миновать. Стоит проверить и скорость реакции создателей продукта на ваши вопросы по горячей линии (если она имеется).

7. Самый последний критерий выбора - цена продукта. Почему последний? В первую очередь, следует руководствоваться всеми вышеперечисленными принципами, а уже потом выбирать продукт наиболее доступный по цене среди равных по возможностям

Внеаудиторная работа:

1. Сформулировать цели работы.
2. Оформить работу, написать выводы.

Практическая работа 2. Анализ технической документации информационной системы.

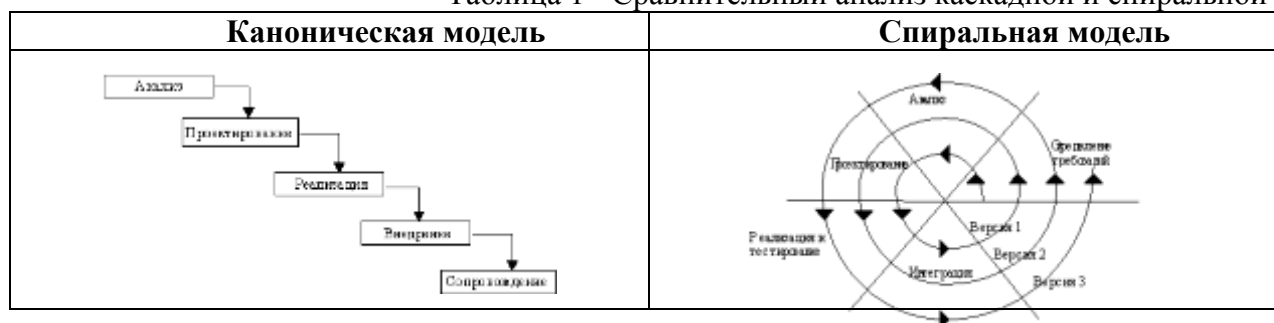
Цель работы: сформировать навыки анализа технической документации, сформировать умения по анализу и составлению технической документации информационных систем.

Оборудование, технические и программные средства: персональный компьютер, тетрадь, письменные принадлежности.

1. Модели жизненного цикла

Существует несколько моделей жизненного цикла. Под моделью обычно понимается структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении жизненного цикла. Из существующих в настоящее время моделей наиболее распространены две: каскадная и спиральная.

Таблица 1 - Сравнительный анализ каскадной и спиральной моделей

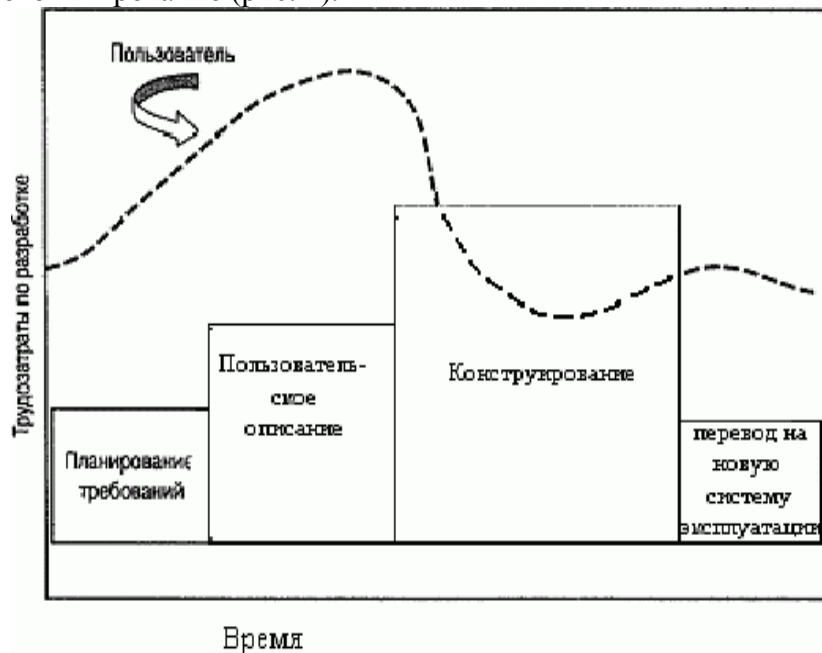


<p>Основная характеристика: Разбиение всей разработки на этапы, причем переход с одного этапа на следующий происходит только после того, как будет полностью завершена работа на текущем. Каждый этап завершается выпуском полного комплекта документации, достаточной для того, чтобы разработка могла быть продолжена другой командой разработчиков.</p> <p>Применение "водопадного" процесса эффективно для систем, для которых в самом начале разработки можно достаточно точно и полно сформулировать все требования, с тем чтобы предоставить разработчикам свободу реализовать их как можно лучше с технической точки зрения.</p>	<p>Разработка системы по данной методологии происходит итерациями, и после прохождения каждого витка спирали пользователь получает очередную версию системы. После получения заказчиком каждой версии уточняются цели и характеристики проекта, определяется его качество и планируются работы следующего витка спирали.</p> <p>Модель сочетает в себе возможности модели прототипирования и водопадной модели. Неполное завершение работ на каждом этапе позволяет переходить на следующий этап, не дожидаясь полного завершения работы на текущем. При итеративном способе разработки недостающую работу можно будет выполнить на следующей итерации. Главная задача — как можно быстрее показать пользователям системы работоспособный продукт, тем самым активизируя процесс уточнения и дополнения требований. Одним из возможных подходов к разработке ПО является методология быстрой разработки приложений RAD (Rapid Application Development).</p>
--	---

2. Метод прототипирования

Прототипирование – это процесс построения рабочей модели системы. Прототипирование имеет множество различных вариантов. Тем не менее все методы основаны на двух типах: быстрое прототипирование и эволюционное прототипирование.

Быстрое прототипирование (рис. 1).

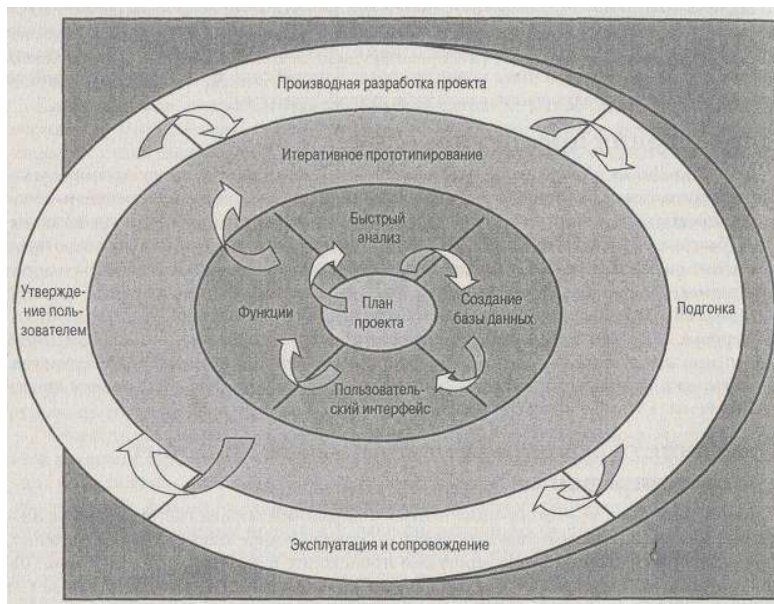


При быстром прототипировании предполагается, что мы создаем макет, который на каком-то этапе будет оставлен («выброшен») и не станет частью готовой системы.

Такое прототипирование выполняется в кратчайшие сроки, поскольку в данном случае тратятся время и ресурсы на код, который не будет в дальнейшем использован.

Основная технология в данном виде разработки – RAD-технологии.

Эволюционное прототипирование (рис. 2).



Эволюционное прототипирование (англ. evolutionary prototyping) ставит своей целью последовательно создавать макеты системы, которые будут все ближе и ближе к реальному продукту.

Такой подход имеет то преимущество, что на каждом шаге мы располагаем работающей системой, пусть и не обладающей всей нужной функциональностью, но улучшающейся с каждой итерацией. При этом, не тратятся ресурсы на код, который будет «выброшен».

Эволюционный подход к прототипированию может быть выбран, исходя из предположения, что все необходимые требования к моменту начала разработки неизвестны, и будут определяться по мере создания программы; тогда на каждом этапе мы реализуем лишь те требования, которые известны и ясны.

3. RAD-технологии

RAD-технология не является универсальной, то есть ее применение целесообразно не всегда. Например, в проектах, где требования к программному продукту четко определены и не должны меняться, вовлечение заказчика в процесс разработки не требуется и более эффективной может быть иерархическая разработка (каскадный метод). То же касается проектов, ПО, сложность которых определяется необходимостью реализации сложных алгоритмов, а роль и объем пользовательского интерфейса невелик.



Рисунок 3 - Сравнение RAD-технологии и каскадной модели

4. Принципы RAD-технологий

Принципы RAD технологии направлены на обеспечение трех основных ее преимуществ – высокой скорости разработки, низкой стоимости и высокого качества. Достигнуть высокого качества программного продукта весьма непросто и одна из главных причин возникающих трудностей заключается в том, что разработчик и заказчик видят предмет разработки ПО по-разному.

- Инструментарий должен быть нацелен на минимизацию времени разработки.
- Создание прототипа для уточнения требований заказчика.

- Цикличность разработки: каждая новая версия продукта основывается на оценке результата работы предыдущей версии заказчиком.
- Минимизация времени разработки версии, за счёт переноса уже готовых модулей и добавления функциональности в новую версию.
- Команда разработчиков должна тесно сотрудничать, каждый участник должен быть готов выполнять несколько обязанностей.
- Управление проектом должно минимизировать длительность цикла разработки.

5. Фазы разработки RAD-технологий

- **Планирование** - совокупность требований, полученных при системном планировании и анализе процедуры разработки жизненного цикла. На этом этапе пользователи, менеджеры и IT-специалисты обсуждают задачи проекта, его объём, системные требования, а также сложности, которые могут возникнуть при разработке. Фаза завершается согласованием ключевых моментов с RAD-группой и получением от руководителей проекта разрешения на продолжение.

- **Пользовательское проектирование** - на протяжении данного этапа пользователи, взаимодействуя с системными аналитиками, разрабатывают модели и прототипы, которые включают в себя все необходимые системные функции. Для перевода пользовательских прототипов в рабочие модели RAD-группа обычно использует технику объединенной разработки приложений (JAD) и CASE-инструменты. Пользовательское проектирование оказывается длительным интерактивным процессом, который позволяет пользователям понять, изменить и, в конечном счете, выбрать рабочую модель, отвечающую их требованиям.

- **Конструирование** - этап, в котором основная задача заключается в разработке программ и приложений. Пользователи продолжают принимать участие и по-прежнему могут предлагать изменения или улучшения в виде разработанных ими докладов. В их задачи входит программирование и разработка приложений, написание кода, интеграция модулей и системное тестирование.

- **Переключение** - включает в себя операции по конверсии данных, тестирование, переход на новую систему и тренировку пользователей. Сравнивая с традиционными методами разработки ПО, весь процесс оказывается сжатым по времени. Как результат, новая система оказывается быстрее построенной, доставленной до заказчика и установленной на рабочих местах.



Рисунок 4 - Фазы разработки RAD-технологий

6. Преимущества RAD-технологий

Технология быстрой разработки приложений (RAD) позволяет обеспечить:

- быстроту продвижения программного продукта на рынок;
- интерфейс, устраивающий пользователя;
- легкую адаптируемость проекта к изменяющимся требованиям;
- простоту развития функциональности системы.



Рисунок 5 - Преимущества RAD-технологий

7. Документация на разработку ИС методом прототипирования

По данному методу используют стандарты проекта, т.к. документации по данному методу нет. Следовательно, разработчики сами определяют правила и требования к разработке.

- 1) Проанализировать представленные модели.
- 2) Составить свой анализ технической документации

Внеаудиторная работа:

- 1) Сформулировать цели работы.
- 2) Оформить работу, написать выводы.

Практическая работа №3. Анализ и разработка регламентов технического сопровождения информационной системы.

Цель работы: сформировать навыки разработки регламента технического сопровождения, сформировать умения по анализу регламента технического сопровождения, на примере представленного, разработке своего регламента.

Оборудование, технические и программные средства: персональный компьютер, операционная система Windows 7.

Задание:

1. Прочитать и проанализировать регламент технического сопровождения, представленный в работе.
2. Написать свой регламент технического сопровождения информационной системы.
3. Сделать выводы.

Регламент технического сопровождения

1. Предмет регулирования
2. Объем и условия технического сопровождения
3. Обновление Программного продукта
4. Техническая поддержка
5. Установка Программного продукта на сервер
6. Конфигурирование и доработка Программных продуктов
7. Использование Программных продуктов для решения прикладных задач

1. Предмет регулирования

1.1. Настоящий Регламент определяет порядок и условия технического сопровождения Программных продуктов и регулирует отношения между компанией «ISPsystem» и Пользователем Программного продукта.

1.2. Положения настоящего Регламента, касающиеся отношений с Партнером компании «ISPsystem» (Партнером), носят информационный характер: отношения Партнера с его контрагентами, в частности сублицензиатами, регулируются соответствующими соглашениями между Партнером и этими лицами.

1.3. Настоящий Регламент является частью публичной оферты компании «ISPsystem», другая часть которой представляет собой предложение о заключении лицензионного договора о

предоставлении права использования Программного продукта и также размещена на Интернет-сайте компании «ISPsystem» по адресу /ru/software/terms_of_licensing

1.4. Настоящий Регламент также подлежит применению в соответствующей части в случае, если право использования Программного продукта было приобретено у Партнера компании «ISPsystem» на основании заключенного с ним сублицензионного договора и была заказана «стандартная» лицензия – в этом случае положения настоящего Регламента подлежат применению к отношениям между компанией «ISPsystem» и лицом, с которым Партнером был заключен сублицензионный договор.

2. Объем и условия технического сопровождения

2.1. Техническое сопровождение Программного продукта включает в себя:

- доработку Программного продукта в целях устранения выявленных ошибок, расширения функциональных возможностей Программного продукта и т.д., результатом которой является выпуск обновлений Программного продукта;
- обеспечение технических условий для загрузки Пользователями Программного продукта выпущенных обновлений;
- техническую поддержку (консультации по вопросам установки, настройки и использования Программного продукта);
- установку Программного продукта на сервер;
- дополнительные работы и услуги.

2.2. В зависимости от того, как был осуществлен заказ лицензии – напрямую у компании «ISPsystem» или у Партнера – объем и условия технического сопровождения Программного продукта могут отличаться.

2.3. В случае модификации Программного продукта, включая его адаптацию (внесение изменений, осуществляемых исключительно в целях функционирования Программного продукта на конкретных технических средствах Пользователя или под управлением конкретных программ Пользователя), в результате которой был изменен объектный код Программного продукта, компания «ISPsystem» вправе отказаться от исполнения своих обязательств в части технического сопровождения Программного продукта без возмещения возможных убытков и не возобновлять техническое сопровождение Программного продукта до восстановления Пользователем его исходного состояния. После восстановления Пользователем исходного состояния Программного продукта компания «ISPsystem» не вправе отказаться от исполнения своих обязательств по техническому сопровождению Программного продукта по указанному в настоящем пункте основанию.

2.4. Объем и условия технического сопровождения при заказе лицензии напрямую у компании «ISPsystem»

Во всех случаях, когда заказ лицензии осуществляется напрямую у компании «ISPsystem» техническое сопровождение Программного продукта предоставляется в полном объеме, включая техническую поддержку и установку Программного продукта на сервер, осуществляемые специалистами компании «ISPsystem» (дополнительные работы и услуги оплачиваются отдельно).

2.5. Объем и условия технического сопровождения при заказе лицензии у Партнера

2.5.1. При заказе лицензии у Партнера объем и условия технического сопровождения в части технической поддержки (консультаций по вопросам установки, настройки и использования Программного продукта) и установки Программного продукта на сервер определяются соглашением с Партнером и зависят от вида лицензии, заказанной у Партнера («триал», «стандартная» или «партнерская» лицензия).

«СТАНДАРТНЫЕ» лицензии

При заказе «стандартной» лицензии техническая поддержка и установка Программного продукта на сервер осуществляется специалистами компании «ISPsystem» без дополнительной оплаты, как если бы лицензия была заказана напрямую у компании «ISPsystem».

«ПАРТНЕРСКИЕ» и «ТРИАЛ» лицензии

При заказе «партнерской» лицензии, а также при заказе «триал» лицензии у Партнера, компания «ISPsystem» не осуществляет техническую поддержку и установку Программного продукта на сервер. Техническая поддержка и установка Программного продукта на сервер могут осуществляться специалистами Партнера на условиях, определяемых соглашением с Партнером.

2.5.2. Партнером могут выполняться дополнительные работы и оказываться дополнительные услуги, связанные с техническим сопровождением Программного продукта, в том числе не предусмотренные настоящим Регламентом.

2.5.3. В рамках партнерского сотрудничества компания «ISPsystem» осуществляет консультирование специалистов Партнеров по вопросам установки, настройки и использования Программного продукта, однако не несет ответственности перед контрагентами Партнера за качество работ и услуг, выполняемых (оказываемых) Партнером в рамках осуществляемого им технического сопровождения Программного продукта, за содержание предоставляемых Партнером справочных материалов, равно как и за любые иные действия Партнера и предоставляемую им информацию.

3. Обновление Программных продуктов

3.1. Компания «ISPsystem» периодически выпускает обновления Программных продуктов, установка которых позволяет устранить выявленные ошибки в работе Программных продуктов, расширить их функциональные возможности и т.д.

3.2. Загрузка и установка обновлений для Программных продуктов осуществляется автоматически, при условии, что сервер, на котором установлен Программный продукт, подключен к информационно-телекоммуникационной сети Интернет, имеет публичный IP адрес и действующий Ключ активации (Ключ активации, срок действия которого не истек на момент обновления Программного продукта).

3.3. Обновления доступны для загрузки в течение всего срока использования Программного продукта, выбранного при заказе лицензии.

3.4. Доступ к обновлениям предоставляется вне зависимости от вида лицензии и способа ее заказа.

3.5. За доступ к обновлениям плата не взимается.

3.6. Компания «ISPsystem» гарантирует, что ей будут приложены все разумные и коммерчески обоснованные усилия, направленные на устранение выявляемых ошибок в работе Программных продуктов, и результаты произведенных доработок будут доступны для загрузки в виде обновлений или патчей. Однако компания «ISPsystem» не принимает на себя персональных обязательств перед Пользователем или контрагентом Партнера по устранению ошибок в работе Программного продукта, который им используется или планируется к использованию.

4. Техническая поддержка

4.1. Техническая поддержка представляет собой консультирование Пользователя (контрагента Партнера) по вопросам установки, настройки и использования Программного продукта для решения конкретных прикладных задач.

4.2. Техническая поддержка не включает в себя диагностику неисправностей в работе сервера, на котором установлен Программный продукт, в том числе неисправностей, которые, по мнению Пользователя (контрагента Партнера), связаны с некорректной работой Программного продукта.

4.3. Техническая поддержка осуществляется специалистами компании «ISPsystem» в случае заказа лицензии напрямую у компании «ISPsystem». При заказе «партнерской» лицензии, а также в случае заказа «триал» лицензии у Партнера, в зависимости от условий соглашения с Партнером, техническая поддержка осуществляется специалистами Партнера, либо Программный продукт предоставляется без технической поддержки.

Компания «ISPsystem» настоятельно рекомендует перед заказом лицензии у Партнера уточнить вопросы, связанные с предоставлением технической поддержки, ознакомившись с соответствующей информацией, размещенной на Интернет-сайте Партнера, а при необходимости – обратиться за разъяснениями к представителям данного Партнера.

4.4. Техническая поддержка, осуществляемая специалистами компании «ISPsystem», предоставляется в течение всего срока использования Программного продукта, выбранного при заказе лицензии, за исключением случаев, когда была заказана т.н. «вечная» лицензия.

В случае заказа «вечной» лицензии техническая поддержка предоставляется в течение первых 3 (трех) месяцев с начала использования Программного продукта. Для целей настоящего пункта началом использования Программного продукта является либо загрузка первого из Ключей активации, не считая Ключей активации, предоставляемых при заказе «триал» лицензии (если заказу «вечной» лицензии предшествовал заказ «триал» лицензии), либо отправка первого запроса в службу технической поддержки относительно этого продукта.

4.5. В случае заказа «триал» лицензии напрямую у компании «ISPsystem» техническая поддержка осуществляется специалистами компании «ISPsystem» в течение всего разрешенного срока безвозмездного использования Программного продукта (в течение всего срока действия «триал» лицензии). Однако в течение этого срока Пользователю предоставляется возможность получить консультацию по вопросам установки, настройки и использования выбранного им Программного продукта, для которого им была заказана «триал» лицензия, не более 10 (десяти) раз с общим временем консультирования не более 3 (трех) часов. При этом повторное обращение по вопросу, в связи с которым уже была предоставлена консультация, учитывается как отдельное обращение.

4.6. В тех случаях, когда техническая поддержка осуществляется специалистами компании «ISPsystem», консультации по вопросам установки, настройки и использования Программного продукта предоставляются без дополнительной оплаты.

4.7. Вне зависимости от вида и способа заказа лицензии Пользователь, контрагент Партнера, а также любое иное лицо, заинтересованное в получении информации о Программных продуктах, может в любое время обратиться к специалистам компании «ISPsystem» через форум, размещенный на Интернет-сайте компании «ISPsystem» по адресу <http://forum.ispsystem.com/ru/index.php>

Компания «ISPsystem» гарантирует, что все вопросы, размещенные на данном форуме, будут рассмотрены и изучены специалистами компании «ISPsystem», однако не принимает на себя персональных обязательств перед Пользователем, контрагентом Партнера или иными участниками форума по предоставлению им консультаций по задаваемым на форуме вопросам.

5. Установка Программного продукта на сервер

5.1. В тех случаях, когда заказ лицензии был осуществлен напрямую у компании «ISPsystem», либо заказ лицензии был осуществлен у Партнера, но была заказана «стандартная» лицензия, специалистами компании «ISPsystem» может быть произведена установка Программного продукта на сервер.

В том случае, когда заказ лицензии был осуществлен у Партнера, и была заказана «партнерская» или «триал» лицензия, установка Программного продукта на сервер специалистами компании «ISPsystem» не производится, но может быть произведена специалистами Партнера на условиях заключаемого с ним соглашения.

5.2. Для установки Программного продукта на сервер специалистами компании «ISPsystem» Пользователь должен указать пароль root для доступа к серверу. Пользователь также должен воздержаться от любых действий, которые могут препятствовать установке, а при необходимости – оказать специалистам компании «ISPsystem» необходимое содействие.

5.3. При установке Программного продукта на сервер, производимой специалистами компании «ISPsystem», также устанавливается необходимое прикладное программное обеспечение: Apache, php и т.д. При этом устанавливается только то прикладное программное обеспечение, которое необходимо для функционирования Программного продукта и присутствует в репозитории пакетов операционной системы, установленной на сервере. При наличии альтернативы выбор конкретного программного обеспечения, устанавливаемого на сервер, осуществляется по усмотрению специалистов компании «ISPsystem».

5.4. В случае, когда установка Программного продукта на сервер осуществляется специалистами компании «ISPsystem», выполняемые при этом работы не подлежат дополнительной оплате.

6. Конфигурирование и доработка Программных продуктов

6.1. Партнер, Пользователь, равно как и любое иное лицо, вправе заниматься разработками, направленными на расширение функциональных возможностей Программных продуктов, изменение их дизайна и т.д., путем разработки самостоятельных и отдельно распространяемых (доводимых до всеобщего сведения и т.д.) элементов, таких как плагин (plug-in), тема (theme) и т.п.

6.2. Модификация Программных продуктов и последующее распространение (доведение до всеобщего сведения и т.д.) программ для ЭВМ, созданных на основе Программных продуктов, допускается только с согласия компании «ISPsystem».

7. Использование Программных продуктов для решения прикладных задач

Внеаудиторная работа:

- 1) Сформулировать цели работы.
- 2) Написать, что такое регламент технического сопровождения.

- 3) Перечислить из чего он состоит
- 5) Оформить работу, написать выводы.

Практическая работа №4. Выбор рационального состава аппаратно-программного обеспечения информационной системы.

Цель работы: сформировать навыки выбора рационального состава аппаратного обеспечения, программного обеспечения, сформировать умения по выбору состава аппаратного и программного обеспечения.

Оборудование, технические и программные средства: персональный компьютер.

Теоретическая часть.

Основные принципы выбора прикладного программного обеспечения:

После того, как решение о реорганизации бизнес-процессов на предприятии принято, немаловажным этапом является выбор прикладного программного обеспечения, которое будет призвано обслуживать и автоматизировать бизнес на предприятии. Многие компании используют следующий, в принципе вполне возможный вариант – они утверждают: «Мы имеем в штате программиста и он может запрограммировать все от самого начала, до самого конца на базовом языке C++ или Delphi». Конечно, такой подход имеет право на существование, поскольку найти сейчас дешевого программиста еще не составляет труда, но по мнению специалистов, он представляется бесперспективным, хотя бы по двум причинам:

- Во-первых, на «пристойное» стандартное программное обеспечение, существующее на рынке, затрачены многие человеко-годы, причем не только на написание самих программ, но и на их отладку.

- Во-вторых, программист может в любой момент уволиться и унести с собой все «Know-how», и систему в подобных случаях зачастую приходится переписывать практически «с нуля», в то время, как с приличным поставщиком ПО вы связаны определенным договором.

Более того, как показывает практика, основные недочеты «самопальных» систем выясняются порой уже на этапах их эксплуатации и ведут к разрушительным последствиям, поскольку исправление ошибок требует больших капиталов и трудовложений, а самое печальное, оказывается необходимым останавливать систему на неопределенный срок, что влечет за собой фактическое затормаживание бизнеса в ряде направлений, которые непосредственно контролировались с помощью системы, таких, например, как отгрузки или бухгалтерия.

Одной из подобных проблем, возникших в последнее время является наступление нового тысячелетия, в связи с чем на большом количестве предприятий, на которых установлены автоматизированные системы, неподдерживающие четырехзначное летоисчисление возникла необходимость в корне переписывать систему, или немедленно переходить к новой.

При выборе поставщика прикладного программного обеспечения, немаловажным фактором является его финансовая стабильность, потому как финансово нестабильный поставщик программно-прикладной составляющей ИС гораздо хуже, чем финансово нестабильный клиент. Последний омертвляет лишь оборотные средства, а первый, уйдя с рынка, омертвит капиталовложение, потому как исчезнет возможность модернизировать систему, и, в случае сбоя, ею придется заниматься незнакомым с ней специалистам.

Таким образом, можно сформировать ряд критериев, которыми следует руководствоваться при подборе системы ПО:

Первые два – почти тавтологичны:

- Система должна быть именно системой, т.е. изменение в одной ее части (скажем, изменения запасов на складе) должны автоматически изменить показатели в других ее разделах (скажем, в бухгалтерских проводках); это свойство системы принято называть интегрируемостью.

- Процедуры в автоматизированных системах должны быть действительно автоматизированы. Дело в том, что случается, что после внедрения системы, количество процедур не уменьшается, просто раньше они выполнялись к примеру на бумаге, а сейчас делается все то же самое, но на компьютере.

- Система должна обеспечивать реализацию бизнес-процессов и процедур, которые существуют либо должны существовать. (оптимальны для конкретного предприятия)

- Система должна давать руководителю возможность получать оперативную информацию в объеме, достаточном для принятия оперативных решений.

- Система должна быть легка в обучении и использовании (дружественна), чтобы рядовой сотрудник мог научиться выполнять свои обязанности при ее помощи за максимально короткое время.

- В системе должна быть заложена возможность без помощи программиста редактировать все необходимые отчеты и документы, менять их форму и создавать собственные форматы.

- В системе должны быть заложены процедуры контроля, сводящие ошибки к минимуму.

- Система должна давать возможность отследить, кто и когда внес изменения в том или ином файле и какая запись была до этих изменений.

- В системах среднего уровня и выше, должны присутствовать надежные программы защиты данных и функции распределения прав доступа.

Системы ПО на российском рынке бывают трех уровней. На **первом уровне** располагаются простые системы для малого и сверхмалого бизнеса, по цене от 50 до 5000 долларов. В этом сегменте доминируют российские продукты. Их очень много, в основном это программы, предназначенные для простых бухгалтерских функций. Они имеют ограничения по количеству операций, по возможности наращивания дополнительных мощностей, по защищенности данных и другим параметрам, но зато просты в использовании и дешевы.

Второй уровень составляют системы по цене 10-80 тыс. долларов и с сопоставимыми затратами на внедрение. Большинство из них – действительно интегрированные системы, поскольку дают возможность вести одновременно и управленческий и финансовый учет. Они не так похожи друг на друга, как системы первого уровня. Например в одной из них может присутствовать модуль, разработанный специально для металлургического завода, в другой – нет, но зато могут присутствовать другие важные частности. И поэтому здесь уже не столь важен сам продукт, как то, как он внедряется, и, следовательно, на предприятии должны присутствовать квалифицированные специалисты, хорошо знающие как и бизнес компании, так и специфику ПО. В этом сегменте больше продуктов западных, нежели отечественных. Выбирая западный продукт, первым делом стоит обращать внимание на то, как он привязан к российским реалиям: к законодательству, инфляции и т.п. Здесь стоит заметить, что европейские системы лучше отвечают этим требованиям, нежели американские, так как они были изначально замешены на присущем всему в Европе многообразию, в том числе и в стандартах учета, и поэтому более гибки.

В российских системах редко встречаются такие качества, как мультивалютность, соответствующая мировым стандартам и многоязычность, что может стать препятствием при работе с иностранными партнерами, инвесторами или клиентами.

Системы **третьего уровня** – это масштабные системы управления предприятием в целом по цене от 100 до 500 тыс. долларов (а иногда и дороже – все зависит от числа пользователей, от удаленности доступа, уровня базы данных и т.д.). В мире таких систем наберется не более десятка, в России систем такого уровня пока не создано вообще. Эти системы функционально различны: в одной может быть очень хорошо развит производственный модуль, в другой – финансовый. Одна больше подходит к нефтегазовому производству, другая к автомобилестроению. Сравнительный анализ систем такого уровня может вылиться в грандиозную работу, а для осуществления проекта внедрения, нужна целая команда из финансовых, управленческих и технических экспертов, имеющая достаточный опыт.

После того, как решение о выборе прикладного ПО на базе которого будет построена ИС принято, необходимо принять решение об аппаратной платформе. **Аппаратную платформу** следует выбирать проанализировав и определив перспективы развития предприятия, принимая во внимание масштаб выбранного ПО и то, планируется ли его наращивание в будущем, а также всевозможные количественные и качественные параметры, такие как количество автоматизированных рабочих мест, их функции, объемы информации, направленность ее потоков. Масштабы и мощность системы определяют уровень технического решения.

А к уровню и конкретному наполнению ИС уже могут быть применены стоимостные мерки. И следовательно, сущности, стоящие за малопонятными, но такими красивыми технологическими мерками, попадают под юрисдикцию закона по экономической целесообразности, в соответствии с которым приходится искать оптимальное решение, пройдя по острию ножа между неразумной с экономической точки зрения избыточностью и потерей капиталовложений в программно-техническую платформу.

Практическая часть.

1. Проанализировав теоретический материал, произвести выбор состава программного и аппаратного обеспечения информационной системы.
2. Составить комплекс программного и аппаратного обеспечения информационных систем.

Внеаудиторная работа:

1. Сформировать цели работы.
2. Оформить отчет.
3. Сделать выводы.

Практическая работа № 5

«Настройка серверного программного обеспечения»

Цели работы: *рассмотреть особенности серверного программного обеспечения, выявить недостатки и разработать пути совершенствования.*

Теоретическая часть:

Объектом исследования данной практической работы является программное обеспечение

Предметом - серверное программное обеспечение.

Для успешного применения технологии «клиент-сервер» должно использоваться соответствующее программное обеспечение, включающее клиентскую и серверную части. В частности, широко используемый пакет Microsoft Office представляет собой комплекс программ для клиентского компьютера. В его состав входят: текстовый процессор Word, табличный процессор Excel, система подготовки презентаций PowerPoint, система управления базами данных Access и программа управления информацией Outlook. В связи с успехом распространения этого пакета корпорация Microsoft решила собрать воедино комплекс программ для сервера - так появился пакет MS BackOffice.

В состав названного пакета входят следующие компоненты:

- Windows NT Server - сетевая операционная система;
- System Management Server - система администрирования сети;
- SQL Server - сервер управления базами данных;
- SNA Server - сервер для соединения с хост-компьютерами;
- Exchange Server - сервер системы электронной почты;
- Internet Information Server - сервер для работы с Internet.

Windows NT/2000 Server способна обеспечить совместное использование файлов, печатающих устройств, предоставить услуги по соединению с рабочими станциями (клиентскими компьютерами) и другой сервис.

Windows NT Server целесообразно использовать в случаях, когда предполагается наличие нескольких процессоров (обычно до четырех). Кроме того, Windows NT Server обеспечивает совместное использование ресурсов многими пользователями, возможность соединения с удаленными сетями через сервис удаленного доступа - RAS (Remote Access Service), а также через средства связи с сетями других фирм (Novell, Digital Pathworks и Apple).

System Management Server (SMS) позволяет сетевому администратору централизованно управлять всей сетью. При этом обеспечивается возможность администрирования каждого компьютера, подключенного к сети, включая установленное на нем программное обеспечение. SMS предоставляет следующий сервис:

1. управление инвентаризацией программного и аппаратного обеспечения;
2. автоматизация установки и распространения программного обеспечения, включая его обновление;
3. удаленное устранение неисправностей и предоставление полного контроля администратору за клавиатурой, мышью и экранами всех компьютеров в сети, работающих под управлением MS-DOS или Windows;
4. управление сетевыми приложениями.

SQL Server представляет собой систему управления реляционными базами данных, использующую принципы технологии «клиент-сервер». MS SQL Server поддерживает систему обработки транзакций, систему сохранения ссылочной целостности, механизм распределенных транзакций, тиражирование данных.

SNA Server обеспечивает возможность связи с IBM AS/400 и мэйнфреймами IBM (EC ЭВМ). Этот продукт позволяет нескольким настольным ПЭВМ, работающим под управлением MS-DOS, Windows, Windows NT, Macintosh, Unix или OS/2, «видеть» хост-компьютеры.

Exchange Server обеспечивает средства передачи и приема сообщений в информационной сети организации. Этот сервис включает электронную почту (E-mail) и обмен информационными сообщениями для рабочих групп. Microsoft Exchange Server построен на принципах технологии «клиент-сервер» и масштабируется в соответствии с возрастанием вычислительных возможностей сети.

Internet Information Server обеспечивает возможность создания Web-, FTP- и Gopher-серверов для сети Internet, поддерживает управление ими с помощью встроенной программы Internet Service Manager.

Архитектура компонента установки и поддержки серверного программного обеспечения

Серверное ПО - это комплекс программных продуктов обслуживающих клиентские запросы.

Для того, что бы добиться необходимых функциональных возможностей от сервера, требуется установить и настроить соответствующее ПО.

Компоненту установки и поддержки ПО для работы требуется наличие Windows 2000 Server, службы каталогов Active Directory, групповой политики и ОС Windows 2000 Professional. За подробной информацией об архитектуре групповой политики и ее объектах обратитесь к технической документации по групповой политике.

Компоненты Windows 2000 Server

клиент сервер инструмент администрирование установка

Этап подготовки программного обеспечения

Как правило, подготовительный этап не затрагивает серверы. Администраторы или разработчики обычно используют компьютеры, работающие под управлением ОС Windows 2000, для создания пакетов или переупаковки приложений с целью их последующей установки и поддержки.

Этап распространения программного обеспечения

Администраторы создают точки распространения ПО на серверах, работающих под управлением ОС Windows 2000 Server, и обеспечивают доступность программного обеспечения для развертывания из этих точек.

Для создания точки распространения ПО администраторы выполняют следующие действия:

- Создают необходимые сетевые папки
- Разрешают общий доступ пользователям к этим папкам
- Копируют программное обеспечение на созданные общие сетевые ресурсы
- Дают пользователям разрешение на чтение для общих сетевых ресурсов

Примечание: Многие программные продукты обладают возможностью административной установки, которая подготавливает приложение для установки из точки распространения ПО. Во время административной установки производится распаковка сжатых файлов, администратор получает возможность ввести регистрационный ключ, а также выполняются другие подготовительные действия. Например, для установки Microsoft Office 2000 в точку распространения ПО необходимо запустить программу установки из командной строки с параметром /a.

Назначение программного обеспечения компьютерам работает наилучшим образом в том случае, когда точка распространения ПО, расположенная на компьютере под управлением ОС Windows 2000 Server, находится в том же лесу службы каталогов Active Directory, что и целевой компьютер. Это обусловлено особенностями механизма проверки подлинности компьютера (объекта учетной записи компьютера). Дополнительные сведения о назначении программного обеспечения компьютеру Вы найдете ниже в разделе «Этап целевого назначения программного обеспечения».

Этап целевого назначения программного обеспечения

Область управления установкой программного обеспечения задается при помощи групповой политики - именно таким образом определяется, для каких пользователей будет производиться установка. Администраторы задействуют расширение Установка программ (Software Installation) для распространения программного обеспечения пользователям и компьютерам, которыми управляет объект групповой политики, связанный с доменом, сайтом или подразделением. Для этого администратору нужно запустить оснастку Групповая политика (Group Policy) и выбрать объект, которым необходимо управлять. Затем в узле Конфигурация пользователя (User Configuration) или в узле Конфигурация компьютера (Computer Configuration) нужно раскрыть узел Конфигурация программ (Software Settings) и установить требуемые параметры в расширении Установка программ

(Software Installation). Компонент установки и поддержки ПО в Windows 2000 позволяет администраторам назначать или публиковать программное обеспечение. Администраторы назначают программное обеспечение в тех случаях, когда оно необходимо пользователям для выполнения их рабочих обязанностей. Например, если все работники должны пользоваться электронной почтой, администратор может назначить им почтовую программу.

Примечание: Назначайте программное обеспечение в тех случаях, когда оно должно быть всегда установлено (или всегда доступно для установки) вне зависимости от действий пользователя. Если компьютером пользуются несколько сотрудников и все они работают с неким приложением, то такое приложение можно назначить компьютеру.

Администраторы могут публиковать программное обеспечение для пользователей, которым оно может пригодиться в работе. Например, администратор может опубликовать программный продукт для управления проектами, предоставляя возможность пользователям самостоятельно принять решение о его установке. Программное обеспечение можно публиковать только для пользователей, но не для компьютеров.

Администраторам необходимо подобрать работоспособную комбинацию с учетом того, что программное обеспечение можно назначать и публиковать, а его целевым назначением могут быть как пользователи, так и компьютеры.

Действия, которые нужно выполнить в расширении Установка программ (Software Installation) для назначения приложения по сути очень похожи на действия, выполняемые в этом расширении для публикации приложения. За подробной информацией об этих действиях обратитесь к разделам интерактивной справки Windows 2000 Server, посвященным расширению Установка программ, а также к Пошаговому руководству по установке и поддержке программного обеспечения Step-by-Step Guide to Software Installation and Maintenance (EN).

Администратор назначает или публикует программное обеспечение при помощи оснастки Групповая политика (Group Policy) и расширения Установка программ (Software Installation). Как правило, для этого необходимо выполнить все или некоторые действия, перечисленные ниже.

1. Откройте оснастку Active Directory - пользователи и компьютеры (Active Directory - Users and Computers) и перейдите в контейнер Active Directory (домен или подразделение), содержащий пользователей или компьютеры, для которых будет производиться управление программным обеспечением. Например, для того чтобы управлять приложениями подразделения под названием Accounts в домене reskit.com, Вам нужно в вышеуказанной оснастке дважды щелкнуть по пункту reskit.com и затем щелкнуть правой кнопкой мыши по подразделению Accounts.

2. Откройте оснастку Групповая политика (Group Policy) для создания нового объекта групповой политики или внесения изменений в уже существующий объект. Если продолжить рассмотрение примера из пункта 1, то для открытия оснастки Групповая политика Вам потребуется выполнить следующие действия. Щелкните правой кнопкой мыши по подразделению Accounts и выберите команду Свойства (Properties), а затем в открывшемся диалоговом окне Свойства: Accounts перейдите на вкладку Групповая политика (Group Policy). Для создания нового объекта групповой политики нажмите кнопку Создать (New), либо внесите изменения в существующий объект. Для этого выберите его из списка Ссылки на объекты групповой политики (Group Policy Object Links) и нажмите кнопку Изменить (Edit).

3. Для того чтобы открыть расширение Установка программ (Software Installation) в оснастке Групповая политика выберите один из двух узлов: Конфигурация пользователя (User Configuration) или Конфигурация пользователя (User Configuration). Дважды щелкните по узлу Конфигурация программ (Software Settings), а затем щелкните правой кнопкой мыши по узлу Установка программ (Software Installation). Например, для управления программным обеспечением пользователей в оснастке Групповая политика раскройте узел Конфигурация пользователя, дважды щелкните по узлу Конфигурация программ, щелкните правой кнопкой мыши по узлу Установка программ, и, наконец, выберите команду Создать (New) из контекстного меню.

4. Выберите пакет установщика Windows (MSI-файл), развертывание которого Вы хотите осуществить из точки распространения программного обеспечения.

5. Сконфигурируйте параметры управления программным продуктом (свяжите с ним файлы преобразования и укажите, какие приложения будет обновлять данный пакет).

6. Назначьте или опубликуйте программный продукт.

Расширение установки программ создает сценарий объявления приложения (файл с расширением .AAS - application advertisement script) и сохраняет его в указанном объекте групповой политики службы каталогов Active Directory. За дополнительной информацией об управлении объектами групповой политики и их хранении в Active Directory, а также о папке Sysvol, обратитесь к документу Введение в групповую политику Windows Server 2003 Introduction to Group Policy in Windows Server 2003 (EN).

Особенности эксплуатации различных видов серверного программного обеспечения

Сервером сети Интернет называется компьютер, на котором установлена специальная программа (она тоже называется сервером, web-сервером или http-сервером), которая отображает web-страницы по запросу клиентской машины, атак же выполняет множество других полезных функций, которых мы коснемся чуть позже. Когда ваш домашний компьютер связывается с сервером и получает от него все необходимые данные, например код web-страницы, он выступает в роли клиента, а всю систему в этом случае принято называть связкой клиент-сервер. На этот термин следует обратить особое внимание, поскольку в последствии мы часто будем сталкиваться с ним.

Системой клиент-сервер называют механизм передачи информации между удаленным компьютером, предоставляющим свои ресурсы в распоряжение пользователей, и пользовательским компьютером, эксплуатирующим эти ресурсы. В данном случае компьютер, открывающий доступ к собственным ресурсам, носит название сервера, а получающий такой доступ клиента.

Серверы могут быть разными, причем отличия заключаются, прежде всего, в операционной системе, под управлением которой они работают. В настоящее время на большинстве интернетовских узлов используют два типа серверных программ: либо Internet Information Server, рассчитанный на работу под Windows NT, либо Apache, предназначенный для платформ, совместимых со стандартом UNIX. Как правило, серверы работают на линиях с большой пропускной способностью, например, в сетях с оптоволоконными каналами связи, что по финансовым соображениям доступно лишь крупным предприятиям.

Помимо соответствующей программы настоящий сервер должен иметь собственный домен, то есть адрес DNS, отвечающий стандартам Domain Name System.

Таким образом, сервер это компьютер с установленным на нем специальным программным обеспечением, имеющий собственное доменное имя. Владелец и администратор сервера могут гибко менять необходимые настройки, разрешать или запрещать доступ к его ресурсам, подключать, настраивать и запускать ряд дополнительных программ и функций, таких как скрипты CGI или приложения SSI, то есть полностью конфигурировать его работу по мере необходимости.

Тематическое содержание серверов может варьироваться в широком диапазоне в зависимости от целей, ради которых они были созданы, возможностей или фантазии владельца и многих других условий. Объединяет их все, пожалуй, только одно: полноценный сервер должен представлять собой то, что среди пользователей Интернета принято называть термином информационный портал, то есть в идеальном случае он является достаточно большим виртуальным пространством, состоящим из множества различных тематических разделов меньшего размера, либо некоторого количества самостоятельных проектов.

Файл-серверы и принт - серверы управляют доступом соответственно к файлам и принтерам, на серверах приложений выполняются прикладные части клиент - серверных приложений, а так же находятся данные доступные клиентам. Например, чтобы упростить извлечение данных, серверы хранят большие объемы информации в структурированном виде. Эти серверы отличаются от файл - серверов и принт - серверов.

В принт - серверах, файл или данные целиком копируются на запрашиваемый компьютер. А в сервере приложений на запрашиваемый компьютер посылаются только результаты запроса. Приложение-клиент на удаленном компьютере получает доступ к данным, хранимым на сервере приложений. Однако вместо всей базы данных на ваш компьютер с сервера загружаются только результаты запроса. В расширенной сети использование серверов различных типов становится наиболее актуальным. Необходимо поэтому учитывать всевозможные нюансы, которые могут проявиться при разрастании сети, с тем чтобы изменение роли определенного сервера в дальнейшем не отразилось на работе всей сети. Основным аргументом при работе в сети на основе выделенного сервера является, как правило, защита данных.

В таких сетях, например как Windows NT Server, проблемами безопасности может заниматься один администратор. Поскольку жизненно важная информация расположена централизованно, то есть,

сосредоточена на одном или нескольких серверах, нетрудно обеспечить ее регулярное резервное копирование.

Благодаря избыточным системам данные на любом сервере могут дублироваться в реальном времени ,поэтому в случае повреждения основной области хранения данных информация не будет потеряна легко воспользоваться резервной копией.

Сети на основе сервера могут поддерживать тысячи пользователей.

Инструменты администрирования

Операционная система Windows Server 2003 предоставляет системному администратору широкий набор инструментов для решения задач управления. Основными из этих инструментов являются следующие:

* консоль управления (Microsoft Management Console, MMC);

* мастера (Wizards);

* утилиты командной строки.

Консоль управления MMC2 представляет собой унифицированную среду для выполнения административных задач. Администратор, имея в распоряжении такую среду, может помещать в неё одну или несколько утилит, называемых оснастками (snap-in), для решения текущей проблемы.

Консоль управления позволяет одинаково отображать любые оснастки и использовать для управления ими похожие приемы.

Таким образом, смысл применения консоли управления в том, чтобы сделать среду выполнения административных утилит единообразной и удобной.

С той же целью в Windows Server 2003 применяются мастера. Мастер представляет собой программу, которая проводит администратора по всем этапам решения какой-либо задачи. На каждом этапе возможен выбор одного или нескольких способов решения или параметров настройки. Часто также мастера предоставляют возможность выбора параметров по умолчанию.

Использование мастеров позволяет сократить время установки и настройки компонентов операционной системы или время решения другой административной задачи. Кроме того, параметры по умолчанию чаще всего обеспечивают вполне работоспособный режим, хотя, возможно, и не самый эффективный.

Утилиты командной строки являются самыми старыми инструментами администрирования, ведущими свою историю от первых операционных систем без графического интерфейса. В то время альтернативы утилитам командной строки не было. Сегодня большинство задач управления можно решить без использования утилит, однако многие администраторы считают, что утилиты командной строки удобнее графического интерфейса. Кроме того, такой вид утилит, как утилиты диагностики стека протоколов TCP/IP, не имеют стандартного графического аналога (эти утилиты рассматриваются во второй лекции).

Большинство административных задач возможно решить, используя любой из представленных инструментов - консоль управления, мастер или утилиту командной строки. Выбор инструмента обуславливается, в основном, личными предпочтениями системного администратора.

Практическая часть

Описание задачи

Фирма ООО «Инициатива» осуществляет деятельность, связанную со строительными работами и продажей строительных материалов. Цены на товары и услуги представлены на рис.2, данные о фирмах, заказы которых должно быть выполнены в сентябре 2005 г., - на рис.3.

1. Построить таблицы по приведенным ниже табличным данным (рис. 2, 3, 4).
2. Организовать межтабличные связи для автоматического заполнения граф: «Наименование фирм», «Наименование товара» и автоматически подсчет суммы заказов на каждой фирме-заказчика в выходных документах (рис. 4, 5).
3. Результаты вычислений представить в виде таблицы, содержащей итоговые суммы за месяц по каждой фирме-заказчику, по фирме ООО «Инициатива» и в графическом виде.
4. Рассчитать и заполнить форму заказов.

Код товара	Наименование товара	Характеристика товара	Единица измерения	Цена, руб.
1	Изготовление дверей	Материал фирмы, сосна, влажность 8%	кв. м	3000,00

2	Изготовление фундамента	Материал фирмы, бетон	куб. м	1200,00
3	Кровельные работы	Материал фирмы, оцинкованная сталь	кв. м	300,00
4	Пиломатериалы	Материал фирмы, дерева	куб. м	3000,00

Рис.2 Базовый прайс-лист

Код фирмы	Наименование фирмы	Адрес	Телефон	Контактная персона
1	Сервис	Кутузовский пр.,2	222-22-32	Сидоров В.В.
2	Проект-М	ул. Ботаническая, 3	331-09-65	Бородин К.П.
3	Факториал	ул. Тверская, 15	976-43-23	Власова И.А.
4	Приват	ул. Ордынка, 33	123-34-56	Столетова С.М.
5	Медик	ул. Грибоедова, 46	456-34-12	Кравченко А.И.

Рис.3 Список фирм-заказчиков

ООО «Инициатива» Заказ № _____ Дата выполнения _____ Наименование фирмы _____ Код фирмы _____ Наименование товара _____ Код товара _____ Количество _____ Сумма, руб. _____ ИТОГО: _____ Принял _____ Дата _____

Рис.4. Форма заказа

Описание алгоритма решения задачи

1. Запустить табличный процессор MS Excel.
 2. Создать книгу с именем «Инициатива».
 3. Лист 1 переименовать в лист с названием Товары.
 4. На рабочем листе Товары MS Excel создать таблицу базового прайс-листа.
 5. Заполнить таблицу базового прайс-листа исходными данными.
- Рис.4 Расположение таблицы «Базовый прайс-лист»
 На рабочем листе Товары MS Excel
6. Лист 2 переименовать в листе с названием Заказчики.
 7. На рабочем листе Заказчики MS Excel создать таблицу, в которой будет содержать список фирм заказчиков.
 8. Заполнить таблицу со списком фирм-заказчиков исходными данными.
- Рис.5 Расположение таблицы «Список фирм-заказчиков»
 На рабочем листе Заказчики MS Excel
9. Разработать структуру шаблона таблицы «Список заказов за месяц».

Колонка электронной таблицы	Наименование (реквизит)	Тип данных	Формат данных	
			длина	точность

A	Дата	дата	8	
B	Наименование фирмы	текстовый	50	
C	Код фирмы	числовой	5	
D	Код заказа	числовой	5	
E	Наименование товара	текстовый	50	
F	Код товара	числовой	5	
G	Количество	числовой	10	
Y	Сумма, руб.	числовой	20	2

Рис.6. Структура шаблона таблицы «Список заказов за месяц»

10. Лист 3 переименовать в лист с названием Список заказов.

11. На рабочем листе Список заказов MS Excel создать таблицу, в которой будет содержать список заказов за месяц.

12. Заполнить таблицу «Список заказов за месяц» исходными данными.

Рис.7 Расположение таблицы «Список заказов за месяц» на рабочем листе Список заказов MS Excel

13. Заполнить графу Наименование фирмы таблицы «Список заказов за месяц», находящейся на листе Список заказов следующим образом:

Занести в ячейку C3 формулу:

=ЕСЛИ(C3=»»;»»;ПРОСМОТР(C3;Заказчики!\$A\$3:\$A\$7;Заказчики!\$B\$3:\$B\$7)).

Размножить введенную в ячейку C3 формулу для остальных ячеек (с C4 по C11) данной графы.

Таким образом, будет выполнен цикл, управляющим параметром которого является номер строки.

14. Заполнить графу Наименование товара таблицы «Список заказов за месяц», находящейся на листе Список заказов следующим образом:

Занести в ячейку F3 формулу:

=ЕСЛИ(F3=»»;»»;ПРОСМОТР(F3;Товары!\$A\$3:\$a\$7;Товары!\$B\$3:\$B\$7)).

Размножить введенную в ячейку F3 формулу для остальных ячеек данной графы (с F4 по F11).

15. Заполнить графу Сумма, руб. таблицы «Список заказов за месяц», находящейся на листе Список Заказов, следующим образом:

Занести в ячейку I3 формулу:

=ПРОСМОТР(G3;Товары!\$A\$3:\$A\$6;Товары!\$E\$3:\$E\$6)*H3.

Размножить введенную в ячейку I3 формулу для остальных ячеек (с I4 по I11) данной графы.

16. В таблице «Список заказов за месяц» вставить автоматические промежуточные (для каждой фирмы) и общие итоги в списке по полю Сумма, руб.

Рис. 8. Список заказов, выполненных фирмой ООО»Инициатива»

В сентябре 2005 г.

17. Лист 4 переименовать в лист с названием Форма заказа.

18. На рабочем листе Формат заказа MS Excel создать форму заказа.

19. Путем создания межтабличных связей заполнить созданную форму полученными данными из таблицы «Список заказов за месяц» (рис. 11).

20. Лист 5 переименовать в лист с названием График.

21. На рабочем листе График MS Excel создать сводную таблицу.

Путем создания межтабличных связей автоматически заполнить графы Наименование фирмы и Всего, руб. полученными данными из таблицы «Список заказов за месяц» (рис. 9).

Рис. 9 Форма заказа фирмы «Проект-М»

Результаты вычислений представить графически (рис. 10)

Рис. 10. Сводная таблица и графическое представление результатов вычислений

Практическая работа №6 «Установка клиентского программного обеспечения»

Цели работы: познакомиться с понятиями клиентское обеспечение, клиентское приложение, со структурой различных клиентских приложений; научиться устанавливать клиентское программное обеспечение на ПК

1. Теоретическая часть

Клиентские приложения

Клиентской называется часть приложения, с которой напрямую взаимодействует конечный пользователь. Это может быть либо приобретенное компанией серийное коммерческое программное обеспечение, либо прикладная программа, разработанная внутри компании с помощью инструментальных средств третьих фирм.

Наличие клиентских приложений способствует упрощению работы конечного пользователя базы данных. От него скрыты объекты базы данных, содержащие реальную информацию, программный код, а также происходящие внутри нее события. Современные технологии делают работу с прикладными программами для конечного пользователя более интуитивной: они дают ему возможность сосредоточиться на выполнении своих прямых обязанностей и, тем самым, способствуют повышению производительности его труда.

Стратегия клиентских приложений

Доступ с любого компьютера предприятия к информации, поступающей от производственного технологического процесса, от любой подсистемы становится необходимостью. Одним из основных компонентов АСУТП (автоматизированная система управления технологическим процессом), способным поставлять технологическую информацию, является приложение SCADA (Supervisory Control and Data Acquisition). А различного типа клиентские приложения могут предоставлять соответствующие производственному процессу в огромном объеме данные в приемлемом для пользователя виде

Традиционно SCADA-системы выполняют следующие функции:

- сбор данных с контроллерного уровня, в том числе на основе стандартных протоколов DDE, OPC;
- отображение данных с использованием графических анимированных объектов (простых и сложных);
- обработка данных с использованием встроенных языков программирования.
- алармирование данных;
- архивирование, хранение данных.

Самым простым и распространенным клиентским приложением являются клиенты в локальной сети. Клиент-серверная организация SCADA-систем предполагает наряду с серверными конфигурациями применение клиентских компонентов двух типов: с возможностью передачи управляющих воздействий с клиентского приложения и чисто мониторинговые приложения. Такие клиентские компоненты SCADA-систем традиционно объединяются с серверными приложениями с помощью протоколов локальных сетей (TCP/IP, NetBEUI). Однако развивающиеся технологии Internet/Intranet не оставили безучастными разработчиков SCADA-систем, баз данных реального времени и т.п. программных продуктов и привели к появлению следующих типов клиентских приложений:

- клиентские приложения в режиме сервер/терминал;
 - бедные и богатые Internet/Intranet-клиенты.
- Основой рассматриваемых решений для клиентских приложений являются новые технологии Microsoft, реализованные в структуре Windows DNA (Distributed Internet Architecture). Поэтому знакомство с ними предлагается начать с краткого изложения особенностей этой структуры.

Структура Windows DNA

Структура Windows DNA это, в первую очередь, реализация трехуровневой модели приложения, включающей следующие уровни (Приложение 2):

- уровень представления;
- уровень бизнес-логики;
- уровень доступа к данным.

Кроме технологий, привязанных к уровням, применяются технологии, представляющие общие сервисы, а также склеивающие технологии. В программном обеспечении Microsoft роль склеивающих технологий играют архитектуры COM и COM+. Архитектура компонентных объектов COM (Component Object Model) это объектно-ориентированная технология. Приложение с компонентной организацией конструируется из COM-объектов, используя готовые наборы этих объектов.

Слои Windows DNA. Технологии Microsoft и относящийся к ним инструментарий предназначены для разработки и реализации трехуровневых приложений.

Уровень представления

На этом уровне есть два обширных вида клиентов, называемых бедными (thin) и богатыми (rich) клиентами. В отличие от толстого (fat) клиента богатый клиент в большей степени ссылается на используемые при создании пользовательского интерфейса технологии, чем на то, какое количество кода выполняется на стороне клиента. Богатые клиенты похожи на обычные приложения Win32, но являются клиентской частью трехуровневого приложения.

Бедные клиенты не одинаково бедны. Примером бедного клиента служит давно известный терминал. Компания Microsoft предложила технологию Windows Terminal Server, в которой приложение Windows работает на центральном сервере и передает графический интерфейс пользователю-клиенту. При этом требуется дорогостоящий сервер и широкая полоса пропускания между клиентом и сервером. Чаще всего понятие бедный клиент обозначает приложение, работающее на Web-сервере и передающее пользовательский интерфейс с помощью HTML-страниц на Web-браузер.

Далее появилась идея обогащения Web-приложений различными компонентами, которые могут использоваться браузером, управляющие элементы ActiveX, апплеты Java и т.д. Различной оснащенности бедные клиенты предлагаются и компаниями-поставщиками SCADA-систем.

Уровень бизнес-логики

Этому уровню свойственны три сервиса: сервисы компонентов (COM), сервер очередей сообщений Microsoft Message Queue (MSMQ) и сервер Internet Information Server (IIS). Сервер IIS это полнофункциональный Web-сервер Microsoft, интегрированный в Windows 2000 Server. Сервер IIS является сервером приложений, поддерживающим бедных клиентов, которые подключаются к нему через протокол HTTP.

Microsoft Transaction Server и COM+. Фундаментальной структурной концепцией, которая обеспечивает разработку сложных многопользовательских приложений для работы с данными, является транзакция. Главное свойство транзакции атомарность. Именно концепция транзакции обеспечивает выполнение ряда операций получения данных из разных СУБД и позволяет рассматривать их как единую операцию (Приложение 3). Message Queue асинхронная однонаправленная связь, ориентированная на сообщения. Протоколы DCOM и HTTP являются синхронными. Они возвращают результат, и до получения ответа от сервера работа клиента блокируется. Асинхронность MSMQ означает, что вызов сервиса осуществляется помещением сообщения в очередь. При этом возврат управления клиенту происходит немедленно (и возврат свидетельствует о постановке в очередь) и клиент продолжает работать (нет блокировки).

Уровень доступа к данным

Фундаментальной технологией доступа к данным является OLE DB гибкий низкоуровневый интерфейс COM.

Структура Windows DNA, особенно уровня представления данных, является основой клиентских приложений, предлагаемых поставщиками SCADA-систем.

Новая реализация клиентского приложения в режиме сервер/терминал

С появлением Windows NT/2000 Terminal Services вновь стала возможна организация клиентских сессий, когда каждый клиент функционирует независимо от других. В этом случае каждый пользователь получает свой ресурс: память, время центрального процессора, доступ к дискам сервера и приложениям. Когда клиент запускается, терминальный сервер его регистрирует, предоставляя доступ к ресурсам сервера. ОС Windows создает также виртуальный дисплей, который затем передается клиенту и отображается на локальном мониторе. Операции ввода, активизируемые клиентом с клавиатуры и мыши также обслуживаются сервером. Добавление новых клиентов сводится к встраиванию нового терминала.

Для организации взаимодействия между сервером и клиентом используются стандартные протоколы Microsoft RDP (Remote Desktop Protocol) и Citrix ICA (Independent Computing Architecture), что допускает реализацию клиентов в виде супер-тонких бездисковых рабочих станций на платформах Linux/CE, от Windows 3.11.95.98 до рабочих станций Windows NT или 2000.

Используя новые архитектурные возможности, компании-разработчики SCADA-систем имеют возможность предложить терминальные сервисы, поддерживающие выполнение SCADA-приложений в режиме сессии. Так компания Wonderware уже поставляет Terminal Services (терминальные сервисы) для SCADA-системы InTouch версии 7.1, что позволяет установить

исполняющую систему InTouch один раз на центральном сервере и затем запускать InTouch-приложения много раз. Клиентские узлы необходимо подключать в режиме терминальной сессии InTouch. Бедный клиент может быть в этом случае терминалом персонального компьютера или встроенным терминальным устройством с вышеперечисленными операционными системами (Приложение 4).

Терминальные пользователи имеют доступ к данным, графическим мнемосхемам с возможностью обмена информации в реальном времени без необходимости установки InTouch на локальном клиентском компьютере. Применение терминал-серверной модели позволяет создавать более экономичные решения за счет того, что приложение устанавливается и поддерживается инженерами только на сервере, при этом можно использовать клиентские узлы на различных платформах. Следует заметить, что на клиентских узлах может просматривать как одно и то же приложение, так и разные приложения.

Установка клиентского программного обеспечения

1. Подготовка компьютера перед установкой

Убедитесь, что конфигурация компьютера отвечает минимальным требованиям ПО.

Проверить наличия свободного места на жёстком диске, если его не хватает, освободить.

Отключить антивирусные программы.

Остановить выполнение посторонних программ.

Установка различного ПО может существенно различаться, но чаще всего установка приложения сводится к стандартному набору действий в которых вам помогает мастер установки.

В случае если программа уже была когда то проинсталлирована на ПК мастер установки спросит, что делать со старой версией удалить, заменить или восстановить.

После этого можно будет указать путь установки программы и завершить установку выполнив все действия указанные мастером.

Завершающим этапом установки, чаще всего, становится регистрация программного продукта.

Поддержка программного обеспечения

Пакеты исправлений и заплатки

Время от времени производители программного обеспечения выпускают исправления к своим программным продуктам. Как правило, исправления корректируют выявленную проблему, а затраты на их тестирование могут варьироваться в зависимости от программного продукта.

Протестировав исправление и приняв решение о его развертывании, администратор копирует необходимые файлы в точку распространения ПО, производя замену старых файлов. Производители программного обеспечения распространяют обновления либо в виде нового пакета установщика, либо в качестве исправления установщика. В случае поставки нового пакета установщика администратор просто заменяет пакет, размещенный в точке распространения ПО. Если же поставляется исправление установщика, администратор следует указаниям производителя программного продукта по применению MSP-файла к существующему пакету, содержащему приложение.

После обновления файлов в точке распространения ПО администратор открывает расширение Установка программ (Software Installation) в объекте групповой политики, который управляет существующим программным обеспечением, и щелкает правой кнопкой мыши по исправляемому приложению для вызова контекстного меню. Он выбирает команду Развернуть приложение заново (Redeploy application), обеспечивающую копирование исправленных файлов при следующем применении групповой политики к тем пользователям, которые уже установили данное приложение.

Пакеты обновления

Между пакетами обновления и исправлениями нет больших отличий. Как правило, в состав пакета обновления входят несколько уже протестированных исправлений. Пакеты обновления распространяются реже, чем исправления, но чаще, чем полные обновления программного продукта. Рекомендуется распространять пакет обновления в качестве исправления, если он содержит небольшое количество файлов. Распространение пакета с большим количеством файлов и управление им рекомендуется рассматривать в качестве полного обновления программного продукта.

В любом случае, следуйте инструкциям производителя заплатки и тестируйте ее в лаборатории или на небольшой группе пользователей, прежде чем осуществлять распространение заплатки для всех пользователей и компьютеров, управляемых заданным объектом групповой политики.

Пакеты обновлений подготовлены с учетом возможности их управления при помощи компонента установки и поддержки ПО, который является частью технологии IntelliMirror.

Обновления

Обновление подразумевает замену значительного числа файлов. Поскольку производятся большие изменения в программном продукте, обновление получает другой номер версии.

Производитель предоставляет новую версию в пакете установщика ПО, с заложенной в него информацией о том, какие более ранние версии он может обновлять. В пакете также должен содержаться сценарий процесса обновления, в котором описано, какие файлы должны быть заменены, удалены и добавлены.

Процесс обновления начинается с размещения файлов программного продукта (пакетов установщика ПО и файлов преобразования для них) в точке распространения ПО. Затем администратор назначает или публикует новую версию в расширении Установка программ (Software Installation). При этом администратор задает преемственную связь между версиями, если это необходимо. Если пакету установщика ПО с новой версией известно об обновляемом приложении, расширение Установка программ автоматически устанавливает преемственную связь между версиями.

Администраторам необходимо определиться с тем, будет обновление обязательным (немедленно вступит в силу для всех пользователей, работающих с текущей версией) или необязательным (пользователи смогут установить новую версию, когда сочтут это нужным).

Практическая часть

Общая характеристика задачи

Задание:

1. Создать таблицы, по приведенным данным. Рис.1-3
2. Произвести необходимый расчет.
3. Заполнить таблицу (рис. 3) числовыми данными, выполнив консолидацию по расположению данных.
4. По данным таблицы на рис. 3 построить гистограмму.

№ лицевого счета	ФИО	Сумма причитающейся пенсии. Руб.	Удержание по исполнительным документам. руб.	Выплачено пенсионеру, руб.
И1212	Иванова А.А.	900	125	
А1245	Антонов С.С.	1200	200	
П1268	Петров И.И.	560	25	
Д1378	Дубровицкий И.С.	456		
С1577	Сидорчук А.В	304	100	

Рис. 1 Табличные данные документа «Свод лицевых счетов» за январь 2006г.

№ лицевого счета	ФИО	Сумма причитающейся пенсии. Руб.	Удержание по исполнительным документам. руб.	Выплачено пенсионеру, руб.
И1212	Иванова А.А.	950	130	
А1245	Антонов С.С.	1250	210	
П1268	Петров И.И.	610	30	
Д1378	Дубровицкий И.С.	506	5	
С1577	Сидорчук А.В	374	100	

Рис. 2 Табличные данные документа «Свод лицевых счетов» за февраль 2006 г.

№ лицевого счета	ФИО	Сумма причитающейся пенсии. Руб.	Удержание по исполнительным документам. руб.	Выплачено пенсионеру, руб.
И1212	Иванова А.А.			
А1245	Антонов С.С.			
П1268	Петров И.И.			
Д1378	Дубровицкий И.С.			
С1577	Сидорчук А.В			

Рис. 3 Табличные данные документа «Свод лицевых счетов» за январь и февраль 2006 г.

Описание алгоритма решения задачи

1. Создал новый документ в Excel.
2. Лист первый переименоуем в «январь». Названия листа прописываем не полностью так как в названии можно прописать ограниченное количество символов.
3. Лист второй переименоуем в «февраль».
4. Лист третий переименоуем в «январь и февраль».
5. На листе «январь» сформируем таблицу «Свод лицевых счетов» за январь 2006г. по образцу.
6. Заполним графу «Выплачено пенсионеру, руб.». Формулу (=C2:C6-D2:D6) укажем для ячеек E2:E6
- На листе «февраль» сформируем таблицу «Свод лицевых счетов» за февраль 2006г. по образцу.
7. Заполним графу «Выплачено пенсионеру, руб.». Формулу =(=C2:C6-D2:D6) укажем для ячеек E2:E6. Получим таблицу:
8. На листе «январь и февраль» сформируем таблицу «Свод лицевых счетов» за январь и февраль 2006 г. по образцу.
9. Заполним таблицу с помощью автоматической консолидации:
 - 9.1. Выделим ячейку В1.
 - 9.2. Выберем в меню **Данные - Консолидация**, появится диалоговое окно **Консолидация**, в выпадающем списке **Функция** выставлено **Сумма**, т.е. выбранные данные будут суммироваться щелчком мышью в поле **Ссылка**,
 - 9.3. Щелкнем по ярлычку листа **Январь**,
 - 9.4. Выделим диапазон В1:Е6 - Вокруг блока Бегущая пунктирная рамка,
 - 9.5. Щелкните кнопку **Добавить** - адрес диапазона окажется в поле **Список диапазонов:**.
 - 9.6. Аналогично добавим диапазоны Февраль!\$B\$1:\$E\$6.
- Список диапазонов консолидации сформирован.
- 9.7. Установим в блоке **Использовать в качестве имен** флажки и в **Подписи верхней строки**, и в **Значение левого столбца**.
- 9.8. Эти флажки нужно установить, потому что информация в таблице будет идентифицироваться по названиям строк и столбцов.
- 9.9. Установим флажок **Создавать связи с исходными данными** щелчком **ОК**.
10. Выполним подгонку ширины столбцов. Столбец С пустой, столбцы С, D, E переместились в столбцы D, E, F. Слева появились символы структуры. Раскроем второй уровень структуры. В столбце С имена текущей рабочей книги (можно консолидировать данные и из разных рабочих книг), а в столбцах D, E, F мы увидим, из каких исходных данных сложились **итоговые данные**.
11. Создадим гистограмму по таблице «Свод лицевых счетов» за январь и февраль 2006 г. Раскроем первый уровень структуры. Выделим необходимые ячейки **В1:F16**. Через меню **Вставка** выберем **Диаграмма** из предложенного списка выберем гистограмму. В параметрах диаграммы прописываем необходимые значения. Получаем готовую гистограмму.

Практическая работа №7**Конфигурирование клиентского программного обеспечения**

Схема сети приведена на [рис. 6.19](#). С помощью настроек ПК, представленных на рисунке, мы указываем хосту, что он должен получать IP адрес, адрес основного шлюза и адрес DNS сервера от DHCP сервера.

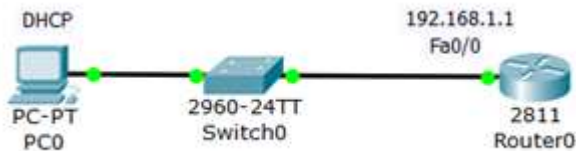


Рис. 6.19. Схема сети

Произведем настройку R0:

Router (config)#ip dhcp pool TST создаем пул IP адресов для DHCP сервера с именем TST

Router (dhcp-config)#network 192.168.1.0 255.255.255.0 указываем из какой сети мы будем раздавать IP адреса (первый параметр - адрес данной сети, а второй параметр ее маска)

Router (dhcp-config)#default-router 192.168.1.1 указываем адрес основного шлюза, который будет рассылать в сообщениях DHCP

Router (dhcp-config)#dns-server 5.5.5.5 указываем адрес DNS сервера, который так же будет рассылаться хостам в сообщениях DHCP

Router (dhcp-config)#exit

Router (config)#ip dhcp excluded-address 192.168.1.1 этот хост исключен из пула, то есть, ни один из хостов сети не получит от DHCP сервера этот адрес.

Полный листинг этих команд приведен на [рис. 6.20](#).

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp pool tst
Router(dhcp-config)#network 192.168.1.1 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 5.5.5.5
Router(dhcp-config)#exit

Router(config)#ip dhcp excluded-address 192.168.1.1
Router(config)#
  
```

Рис. 6.20. Команды для конфигурирования R0

Проверим результат получения динамических параметров для PC0 ([рис. 6.21](#)).



Рис. 6.21. DHCP работает

Проверим работоспособность DHCP сервера на хосте PC0 командой **ipconfig /all** ([рис. 6.22](#)).

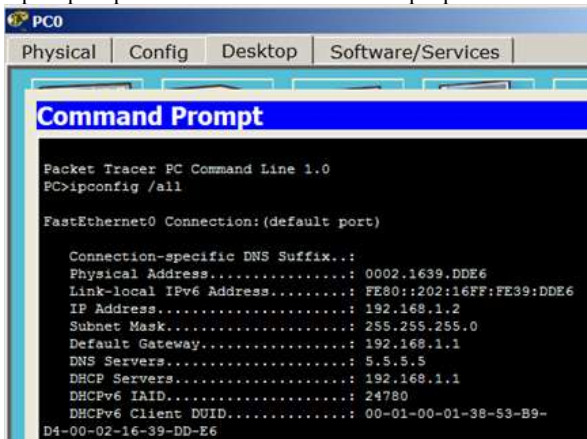
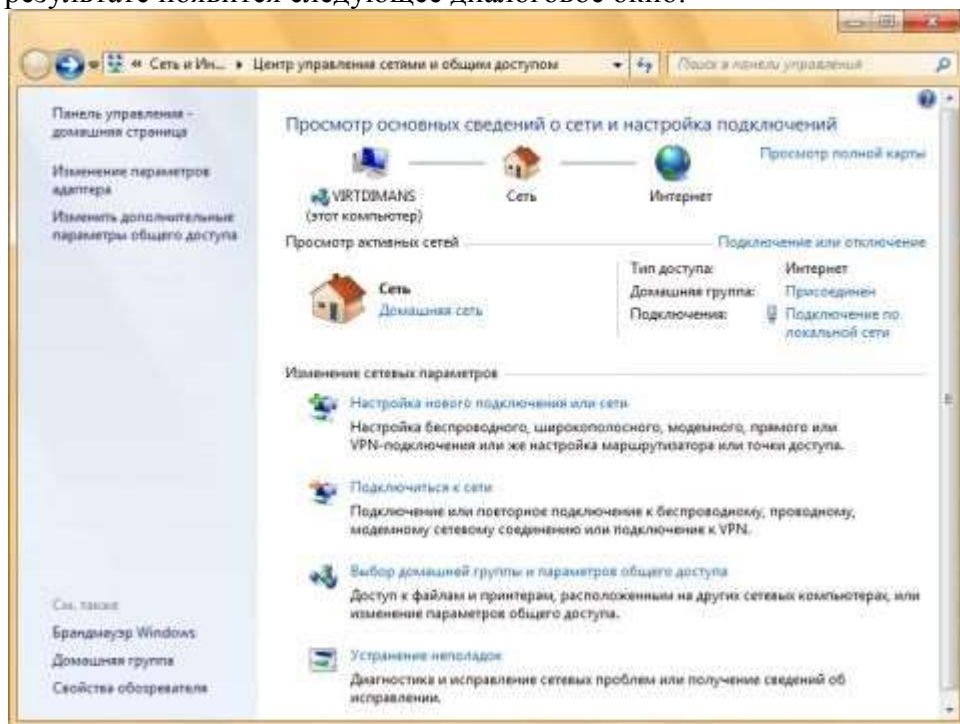


Рис. 6.22. Хост получил настройки от DHCP сервера
Хост успешно получил IP адрес, адрес шлюза и адрес DNS сервера от DHCP сервера R0.

Практическая работа №8 «Настройка сети и поиск неисправностей в среде конкретных операционных систем»

1. Прописать цели работы.
2. Прodelать пошагово все действия и записать их результат (Что делаем, что видим).
3. Сделать выводы.
4. Оформить работу.

1. Открыть Пуск\Панель управления\Центр управления сетями и общим доступом, в результате появится следующее диалоговое окно:



Понятие сетевого расположения

Перед началом работы с данным компонентом, следует разобраться с таким понятием как **сетевое расположение**. Этот параметр задается для компьютеров при первом подключении к сети и во время подключения автоматически настраивается брандмауэр и параметры безопасности для того типа сети, к которому производится подключение. В отличие от операционной системы [Windows Vista](#), где для всех сетевых подключений используется самый строгий профиль брандмауэра для сетевого размещения, операционная система Windows 7 поддерживает несколько активных профилей, что позволяет наиболее безопасно использовать несколько сетевых адаптеров, подключенных к различным сетям. Существует четыре типа сетевого расположения:

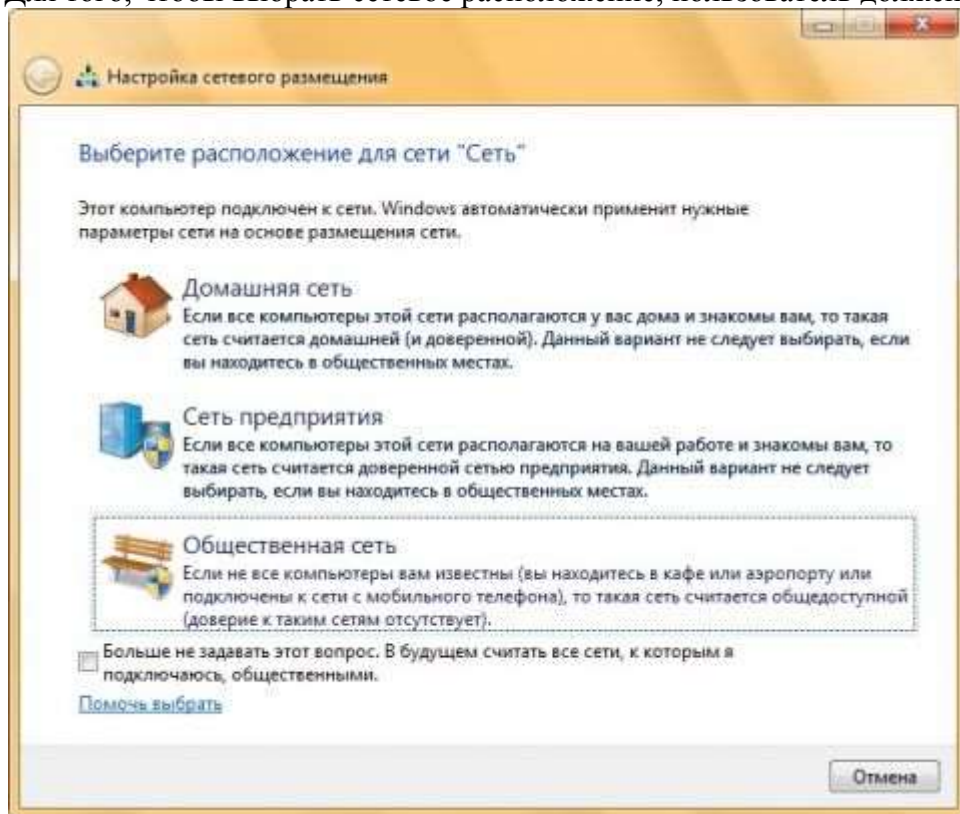
Домашняя сеть. Данное сетевое расположение предназначено для использования компьютера в домашних условиях или в таких сетях, где пользователи очень хорошо знают друг друга. Такие компьютеры могут создавать и присоединяться к домашним группам. Для домашних сетей автоматически включается обнаружение сети.

Сеть предприятия. Такое сетевое расположение используется в сети малого офиса (SOHO). Для этого сетевого расположения также включено обнаружение сети, но вы не можете ни создавать, ни присоединять компьютер к домашней группе.

Общественная сеть. Это сетевое расположение предназначено для использования компьютера в таких общественных местах, как кафе или аэропорты. Это наиболее строгое размещение, у которого по умолчанию отключены возможности присоединяться к домашней группе и сетевое обнаружение.

Доменная сеть. Если компьютер присоединён к домену Active Directory, то существующей сети будет автоматически назначен тип сетевого размещения «Домен». Доменный тип сетевого расположения аналогичен рабочей сети, за исключением того, что в домене конфигурация брандмауэра Windows, сетевого обнаружения, а также сетевой карты определяется групповой политикой.

Для того, чтобы выбрать сетевое расположение, пользователь должен открыть следующую вкладку:



Карта сети



Карта сети – это графическое представление расположения компьютеров и устройств, которое позволяет увидеть все устройства вашей локальной сети, а также схему их подключения друг к другу. В окне **«Центр управления сетями и общим доступом»** отображается только локальная часть сетевой карты, компоновка которой зависит от имеющихся сетевых подключений. Компьютер, на котором выполняется создание карты, отображается в левом верхнем углу. Другие компьютеры подсети отображаются слева. Такие устройства инфраструктуры, как коммутаторы, концентраторы и шлюзы в другие сети отображаются справа. Пример карты сети вы можете увидеть на следующей иллюстрации:

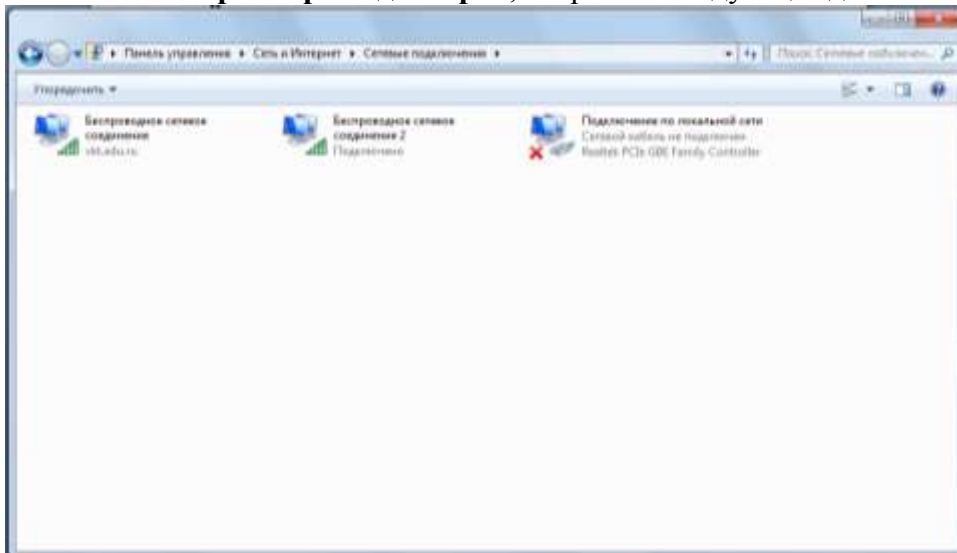


По умолчанию, карту сети можно просматривать только для расположений **«Домашняя сеть»** или **«Сеть предприятия»**. При попытке просмотра сетевой карты для расположений **«Доменная сеть»** или **«Общественная сеть»** вы увидите следующее сообщение:

Сетевые подключения

После установки драйвера для каждого сетевого адаптера, операционная система Windows пытается автоматически сконфигурировать сетевые подключения на локальном компьютере. Все доступные сетевые подключения отображаются в окне **«Сетевые подключения»**. Сетевое подключение представляет собой набор данных, необходимых для подключения компьютера к Интернету, локальной сети или любому другому компьютеру.

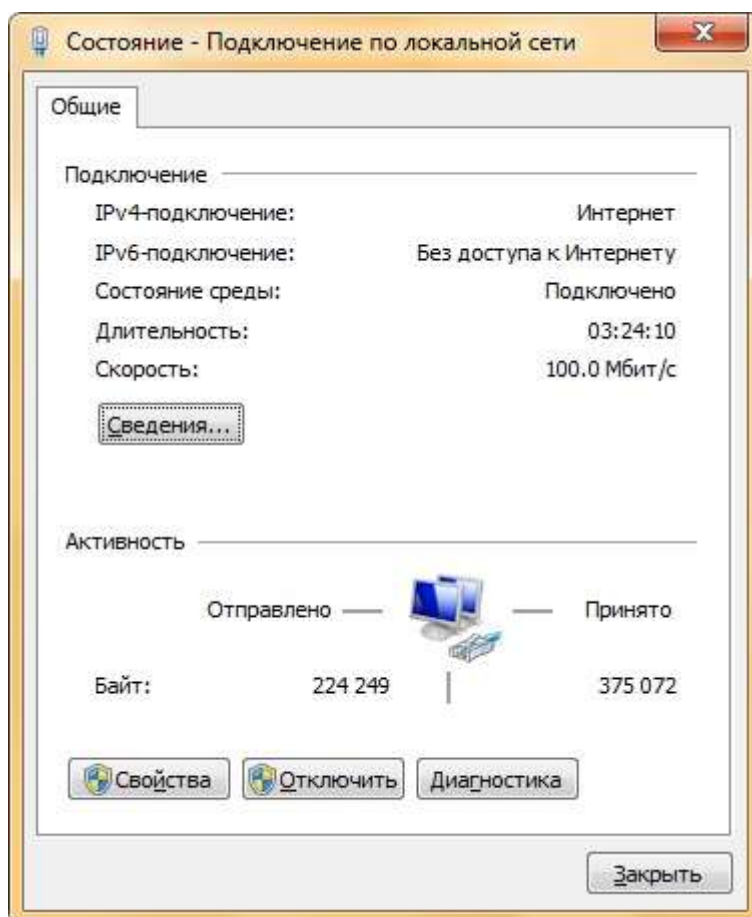
Откройте окно «**Центр управления сетями и общим доступом**» и перейдите по ссылке «**Изменение параметров адаптера**», откроется следующее диалоговое окно:



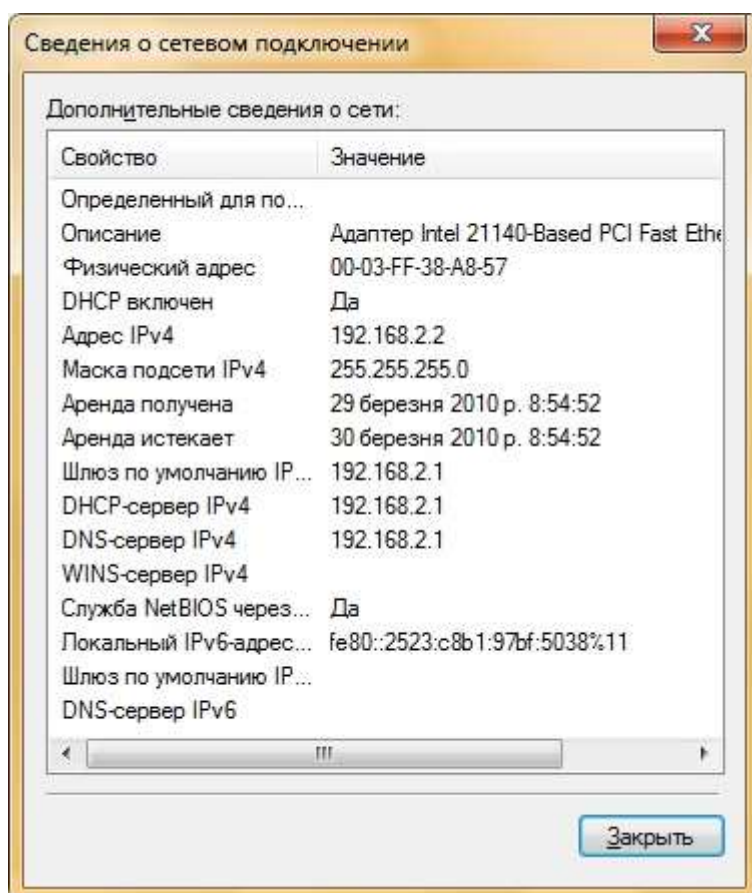
➤ Выписать наименование всех сетей.

При выборе любого сетевого подключения вы можете выполнить с ним следующие действия:

- **Переименование подключения.** Операционная система по умолчанию назначает всем сетевым подключениям имена «**Подключение по локальной сети**» или «**Подключение к беспроводной сети**» и номер подключения в том случае, если у вас существует более одного сетевого подключения. При желании, вы можете переименовать любое сетевое подключение одним из трех следующих способов:
 - Нажмите на клавишу **F2**, введите новое имя сетевого подключения, после чего нажмите на клавишу **Enter**;
 - Нажмите правой кнопкой мыши на переименовываемом сетевом подключении и из контекстного меню выберите команду «**Переименовать**». Введите новое имя сетевого подключения, после чего нажмите на клавишу **Enter**;
 - Выберите сетевое подключение и нажмите на кнопку «**Переименование подключения**», которая расположена на панели инструментов. После чего введите новое имя сетевого подключения и нажмите на клавишу **Enter**.
- **Состояние сети.** Используя данное окно, вы можете просмотреть любые данные о состоянии сетевого подключения и такие детали, как IP-адрес, MAC-адрес и прочее. Чтобы открыть диалоговое окно сведений о сетевом подключении, выполните следующие действия:
 1. Откройте диалоговое окно «**Состояние**» одним из следующих способов:
 - Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «**Состояние**»;
 - Выберите сетевое подключение и нажмите на кнопку «**Просмотр состояния подключения**», которая расположена на панели инструментов;
 - Выберите сетевое подключение и нажмите на клавишу **Enter**.

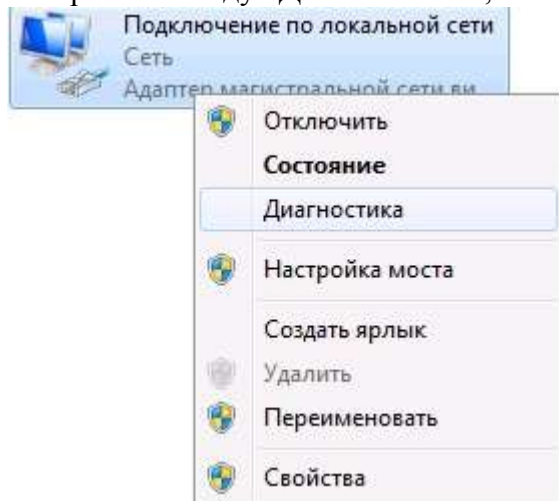


- Выписать общие сведения для своего подключения.
2. В окне «Состояние – подключение по локальной сети» нажмите на кнопку «Сведения». В диалоговом окне «Сведения о сетевом подключении», отображенном ниже, вы можете просмотреть подробные сведения о текущем сетевом подключении.



- Выписать свои сведения.

- Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «**Диагностика**», как показано на следующей иллюстрации:



- Выберите сетевое подключение и нажмите на кнопку «**Диагностика подключения**», которая расположена на панели инструментов.

В открывшемся диалоговом окне «**Диагностика сетей Windows**» для устранения неполадок следуйте действиям мастера.

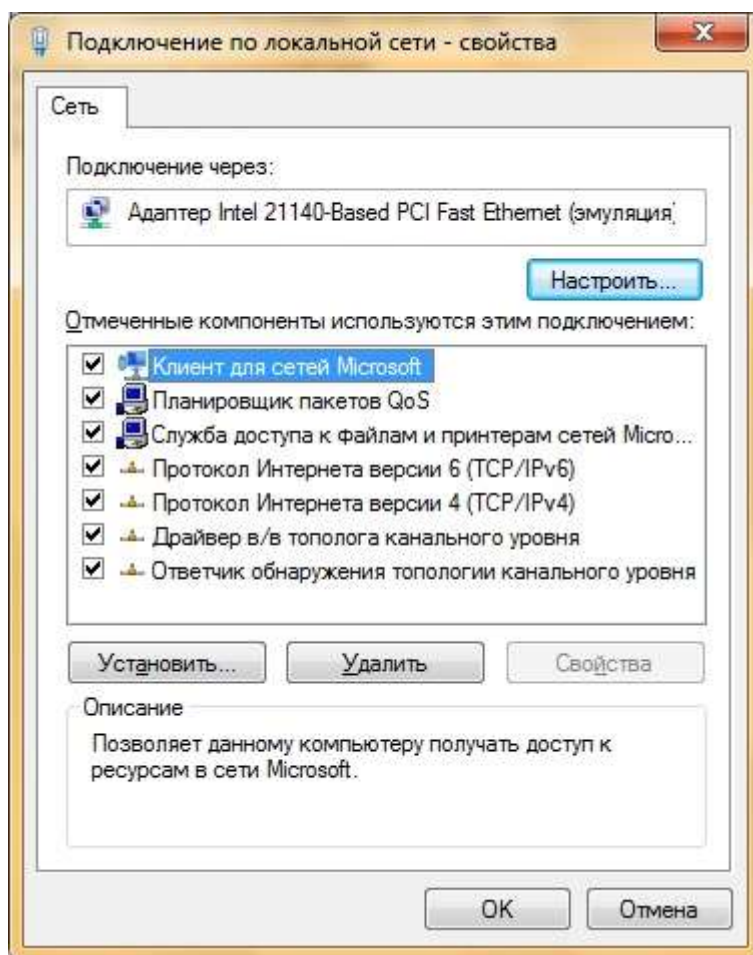
Отключение сетевого устройства. Иногда проблемы с сетевыми подключениями решаются посредством отключения сетевого адаптера компьютера от сети. Для того чтобы отключить сетевой адаптер выполните одно из следующих действий:

- Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «**Отключить**»;
- Выберите сетевое подключение и нажмите на кнопку «**Отключение сетевого устройства**», которая расположена на панели инструментов.

Настройка параметров подключения. Как таковые, сетевые подключения не позволяют осуществлять коммуникации. Осуществление коммуникаций обеспечивают сетевые клиенты, службы и протоколы, которые привязаны к созданным сетевым подключениям. Для того чтобы изменить настройки вашего сетевого подключения, вы можете воспользоваться средствами настройки параметров подключения. Для изменения компонентов и настроек сетевого подключения, выполните следующие действия:

- Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «**Свойства**»;
- Выберите сетевое подключение и нажмите на кнопку «**Настройка параметров подключения**», которая расположена на панели инструментов;
- Выберите сетевое подключение и воспользуйтесь комбинацией клавиш **Alt + Enter**.

Установленные возле компонентов флажки указывают, что эти компоненты привязаны к подключению. Диалоговое окно свойств сетевого подключения отображено ниже:



Практическая работа №9. Настройка сети и поиск неисправностей в среде конкретных операционных систем.

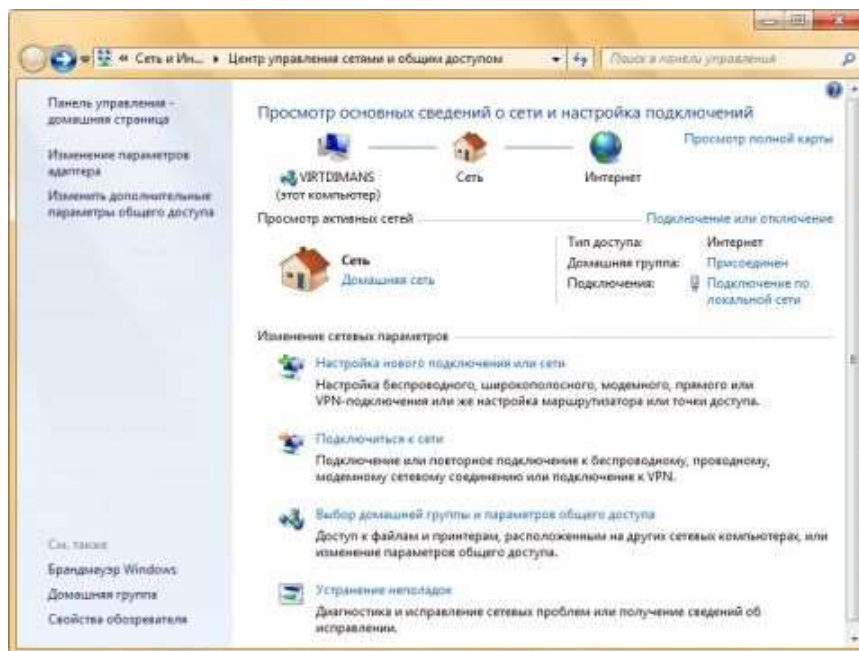
Цель работы: сформировать навыки настройки сети, сформировать умения по настраиванию сети и поиску неисправностей в них.

Реализуемые компетенции:

- ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
- ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
- ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.
- ПК 4.4. Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями.

Оборудование, технические и программные средства: персональный компьютер, операционная система Windows 7, Центр управления сетями и общим доступом.

1. Открыть Пуск\Панель управления\Центр управления сетями и общим доступом, в результате появится следующее диалоговое окно:



Понятие сетевого расположения. Перед началом работы с данным компонентом, следует разобраться с таким понятием как **сетевое расположение**. Этот параметр задается для компьютеров при первом подключении к сети и во время подключения автоматически настраивается брандмауэр и параметры безопасности для того типа сети, к которому производится подключение. В отличие от операционной системы [Windows Vista](#), где для всех сетевых подключений используется самый строгий профиль брандмауэра для сетевого размещения, операционная система Windows 7 поддерживает несколько активных профилей, что позволяет наиболее безопасно использовать несколько сетевых адаптеров, подключенных к различным сетям. Существует четыре типа сетевого расположения:

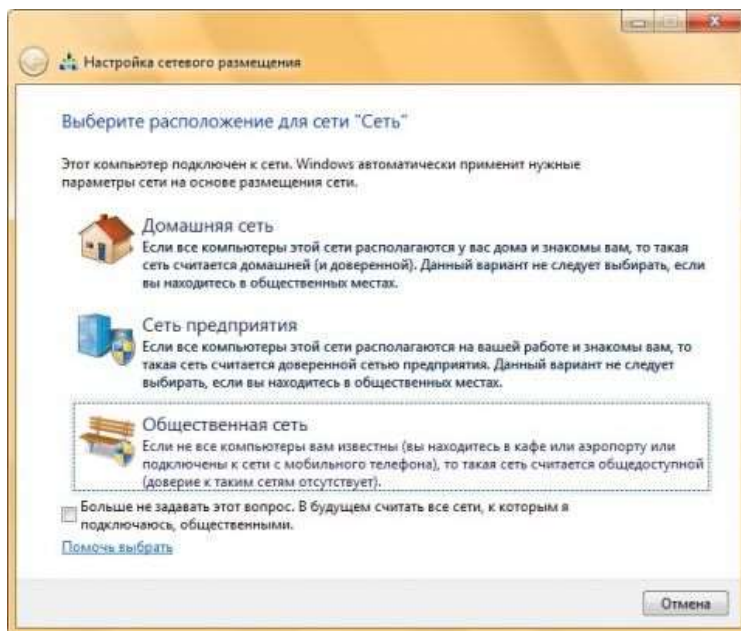
Домашняя сеть. Данное сетевое расположение предназначено для использования компьютера в домашних условиях или в таких сетях, где пользователи очень хорошо знают друг друга. Такие компьютеры могут создавать и присоединяться к домашним группам. Для домашних сетей автоматически включается обнаружение сети.

Сеть предприятия. Такое сетевое расположение используется в сети малого офиса (SOHO). Для этого сетевого расположения также включено обнаружение сети, но вы не можете ни создавать, ни присоединять компьютер к домашней группе.

Общественная сеть. Это сетевое расположение предназначено для использования компьютера в таких общественных местах, как кафе или аэропорты. Это наиболее строгое размещение, у которого по умолчанию отключены возможности присоединяться к домашней группе и сетевое обнаружение.

Доменная сеть. Если компьютер присоединён к домену Active Directory, то существующей сети будет автоматически назначен тип сетевого размещения «**Домен**». Доменный тип сетевого расположения аналогичен рабочей сети, за исключением того, что в домене конфигурация брандмауэра Windows, сетевого обнаружения, а также сетевой карты определяется групповой политикой.

Для того, чтобы выбрать сетевое расположение, пользователь должен открыть следующую вкладку:



Карта сети. Карта сети – это графическое представление расположения компьютеров и устройств, которое позволяет увидеть все устройства вашей локальной сети, а также схему их подключения друг к другу. В окне «**Центр управления сетями и общим доступом**» отображается только локальная часть сетевой карты, компоновка которой зависит от имеющихся сетевых подключений.

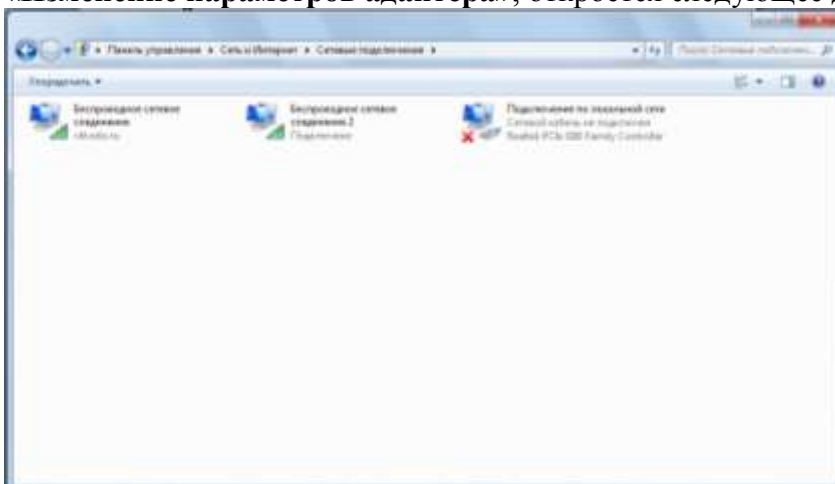
Компьютер, на котором выполняется создание карты, отображается в левом верхнем углу. Другие компьютеры подсети отображаются слева. Такие устройства инфраструктуры, как коммутаторы, концентраторы и шлюзы в другие сети отображаются справа. Пример карты сети вы можете увидеть на следующей иллюстрации:



По умолчанию, карту сети можно просматривать только для расположений «**Домашняя сеть**» или «**Сеть предприятия**». При попытке просмотра сетевой карты для расположений «**Доменная сеть**» или «**Общественная сеть**» вы увидите следующее сообщение:

Сетевые подключения. После установки драйвера для каждого сетевого адаптера, операционная система Windows пытается автоматически сконфигурировать сетевые подключения на локальном компьютере. Все доступные сетевые подключения отображаются в окне «**Сетевые подключения**». Сетевое подключение представляет собой набор данных, необходимых для подключения компьютера к Интернету, локальной сети или любому другому компьютеру.

Откройте окно «**Центр управления сетями и общим доступом**» и перейдите по ссылке «**Изменение параметров адаптера**», откроется следующее диалоговое окно:



➤ Выписать наименование всех сетей.

При выборе любого сетевого подключения вы можете выполнить с ним следующие действия:

- **Переименование подключения.** Операционная система по умолчанию назначает всем сетевым подключениям имена «Подключение по локальной сети» или «Подключение к беспроводной сети» и номер подключения в том случае, если у вас существует более одного сетевого подключения. При желании, вы можете переименовать любое сетевое подключение одним из трех следующих способов:

- Нажмите на клавишу **F2**, введите новое имя сетевого подключения, после чего нажмите на клавишу **Enter**;

- Нажмите правой кнопкой мыши на переименовываемом сетевом подключении и из контекстного меню выберите команду «**Переименовать**». Введите новое имя сетевого подключения, после чего нажмите на клавишу **Enter**;

- Выберите сетевое подключение и нажмите на кнопку «**Переименование подключения**», которая расположена на панели инструментов. После чего введите новое имя сетевого подключения и нажмите на клавишу **Enter**.

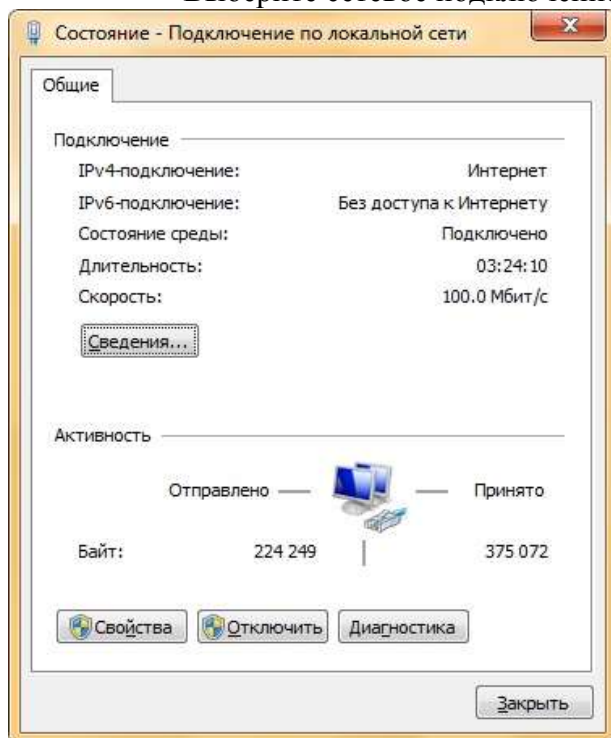
- **Состояние сети.** Используя данное окно, вы можете просмотреть любые данные о состоянии сетевого подключения и такие детали, как IP-адрес, MAC-адрес и прочее. Чтобы открыть диалоговое окно сведений о сетевом подключении, выполните следующие действия:

1. Откройте диалоговое окно «**Состояние**» одним из следующих способов:

- Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «**Состояние**»;

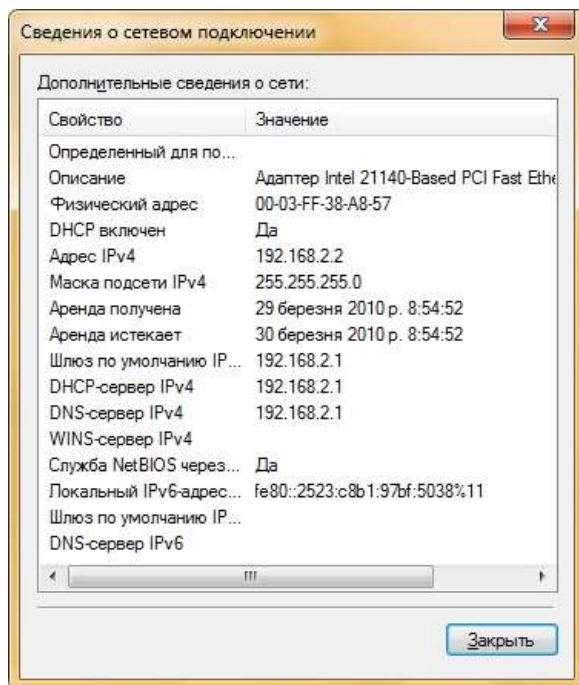
- Выберите сетевое подключение и нажмите на кнопку «**Просмотр состояния подключения**», которая расположена на панели инструментов;

- Выберите сетевое подключение и нажмите на клавишу **Enter**.



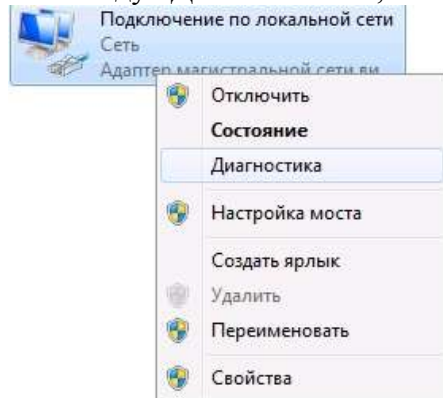
➤ Выписать общие сведения для своего подключения.

2. В окне «**Состояние – подключение по локальной сети**» нажмите на кнопку «**Сведения**». В диалоговом окне «**Сведения о сетевом подключении**», отображенном ниже, вы можете просмотреть подробные сведения о текущем сетевом подключении.



➤ Выписать свои сведения.

○ Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «**Диагностика**», как показано на следующей иллюстрации:



○ Выберите сетевое подключение и нажмите на кнопку «**Диагностика подключения**», которая расположена на панели инструментов.

В открывшемся диалоговом окне «**Диагностика сетей Windows**» для устранения неполадок следуйте действиям мастера.

Отключение сетевого устройства. Иногда проблемы с сетевыми подключениями решаются посредством отключения сетевого адаптера компьютера от сети. Для того чтобы отключить сетевой адаптер выполните одно из следующих действий:

○ Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «**Отключить**»;

○ Выберите сетевое подключение и нажмите на кнопку «**Отключение сетевого устройства**», которая расположена на панели инструментов.

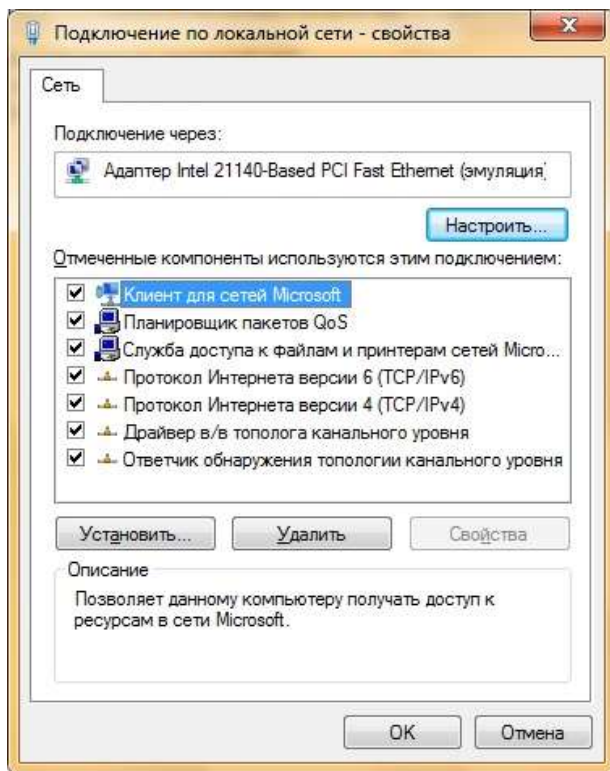
Настройка параметров подключения. Как таковые, сетевые подключения не позволяют осуществлять коммуникации. Осуществление коммуникаций обеспечивают сетевые клиенты, службы и протоколы, которые привязаны к созданным сетевым подключениям. Для того чтобы изменить настройки вашего сетевого подключения, вы можете воспользоваться средствами настройки параметров подключения. Для изменения компонентов и настроек сетевого подключения, выполните следующие действия:

○ Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «**Свойства**»;

○ Выберите сетевое подключение и нажмите на кнопку «**Настройка параметров подключения**», которая расположена на панели инструментов;

○ Выберите сетевое подключение и воспользуйтесь комбинацией клавиш **Alt + Enter**.

Установленные возле компонентов флажки указывают, что эти компоненты привязаны к подключению. Диалоговое окно свойств сетевого подключения отображено ниже:



Внеаудиторная работа:

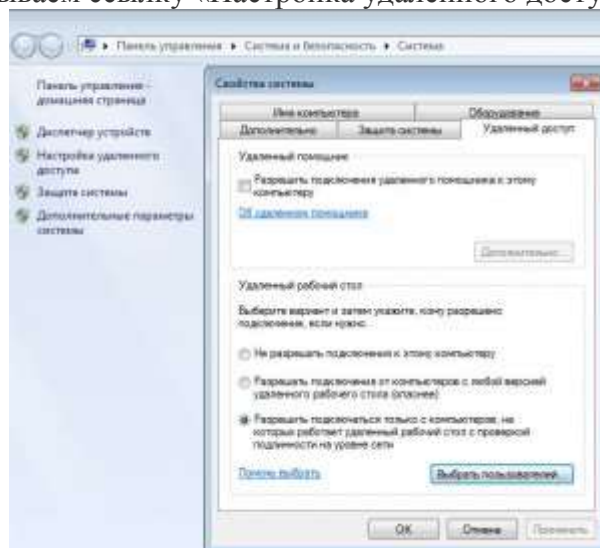
1. Прописать цели работы.
2. Составить отчет по практической работе.
3. Сделать выводы.

Практическая работа № 10 «Организация удаленного доступа»

- 1) Сформулировать цели работы.
- 2) Написать, что такое удаленный доступ.
- 3) Какими способами можно организовать удаленный доступ.
- 4) Проанализировать и посмотреть на компьютере организацию удаленного доступа к рабочему столу в Windows 7.
- 5) Сделать нужные скриншоты
- 6) Написать выводы

Настройка доступа к удаленному рабочему столу

Все достаточно просто. Открываем Панель управления -> Система и безопасность -> Система. Далее в левой колонке открываем ссылку «Настройка удаленного доступа»:



Настройка удаленного доступа

В разделе «Удаленный рабочий стол» необходимо выбрать тип подключения:

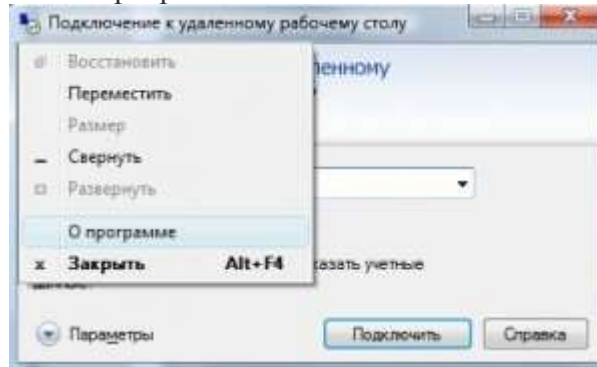
1. Разрешать подключение от компьютеров с любой версией удаленного рабочего стола (опаснее). Этот вариант подходит для подключения устаревших клиентов (версия протокола удаленного рабочего стола ниже 7.0), а также при подключении через Эксплорер (remote desktop web connection).
2. Разрешать подключаться только с компьютеров, на которых работает удаленный рабочий стол с проверкой подлинности на уровне сети. Этот вариант подходит для подключения клиентов с версией 7.0 протокола удаленного рабочего стола.

С помощью кнопки «Выбрать пользователей» можно указать учетные записи пользователей, которым разрешено подключаться к удаленному рабочему столу. Тот же самый эффект будет, если в ручную добавить учетные записи в группу «Пользователи удаленного рабочего стола». Обратите внимание, что пользователи входящие в группу администраторов уже имеют доступ к удаленному рабочему столу.

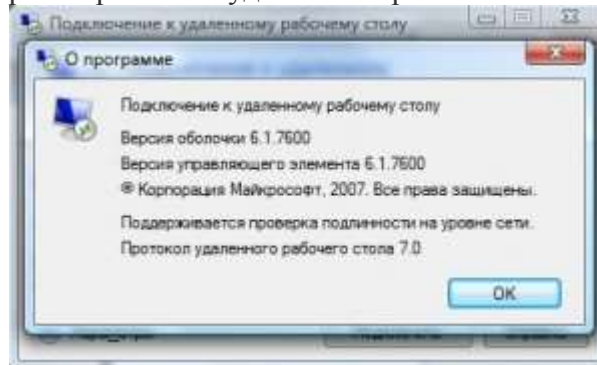
Также имейте в виду, что по умолчанию политика безопасности не разрешает вход в систему через сеть для учетных записей с пустым паролем. Поэтому **учетная запись должна быть защищена паролем** (в том числе и входящая в группу Администраторы), иначе подключиться не получится.

Подключение к удаленному рабочему столу с помощью стандартного клиента

Для начала определяем какая версия протокола поддерживается нашим клиентом. Для этого запускаем клиент (обычно он находится в меню Пуск -> Программы -> Стандартные -> Подключение к удаленному рабочему столу). Далее кликаем по пиктограмме в левом верхнем углу окна и в меню выбираем пункт «О программе»:



Версия протокола удаленного рабочего стола (1)



Версия протокола удаленного рабочего стола (2)

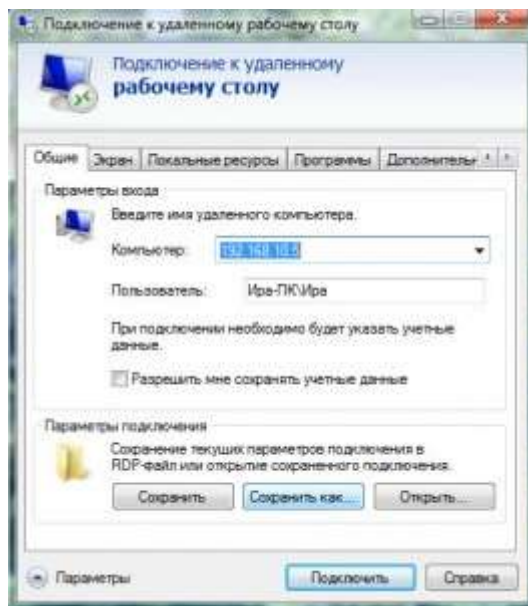
Внизу окна будет указана версия протокола.

Если версия протокола ниже 7.0, то необходимо обновить клиент, или понизить уровень безопасности в настройках сервера (до «Разрешать подключение от компьютеров с любой версией удаленного рабочего стола (опаснее)»). Клиент с поддержкой протокола 7.0 можно скачать здесь:

- Для XP
- Для Vista

Теперь запускаем клиент и настраиваем соединение. Для доступа к дополнительным настройкам нажимаем кнопку Параметры. В окне появятся дополнительные закладки.

Закладка Общие.



Дополнительные параметры. Закладка Общие.

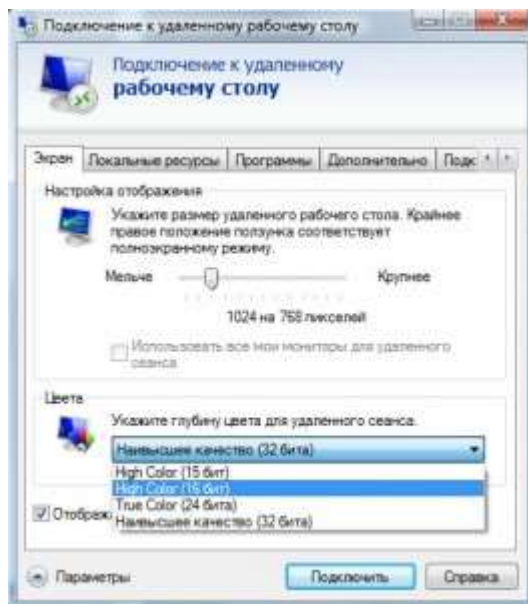
В поле Компьютер указываем ip-адрес или доменное имя компьютера к которому производится подключение.

В поле Пользователь указываем имя пользователя удаленного рабочего стола.

Опцию «Разрешить мне сохранять учетные данные» отмечаем только в том случае, если к компьютеру имеете доступ только вы (а лучше и вовсе оставить ее неотмеченной).

Чтобы сохранить параметры доступа, используем кнопку «Сохранить как».

Закладка Экран.

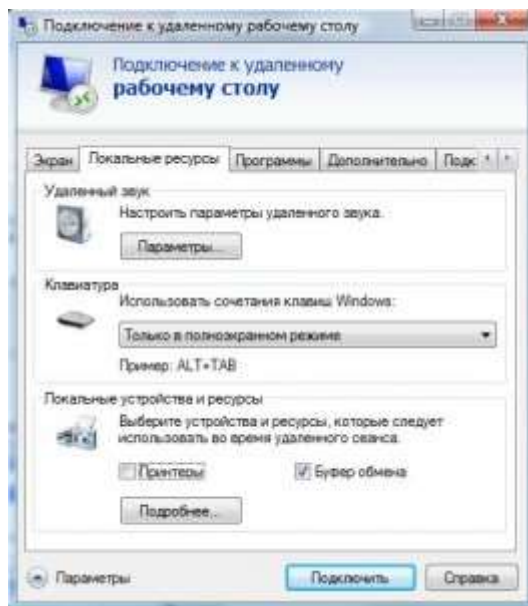


Дополнительные параметры. Закладка Экран.

В разделе «Настройка отображения» выбираем размер удаленного рабочего стола.

В разделе Цвета выбираем глубину цвета. Для медленных соединений рекомендуется устанавливать меньшую глубину.

Закладка «Локальные ресурсы».

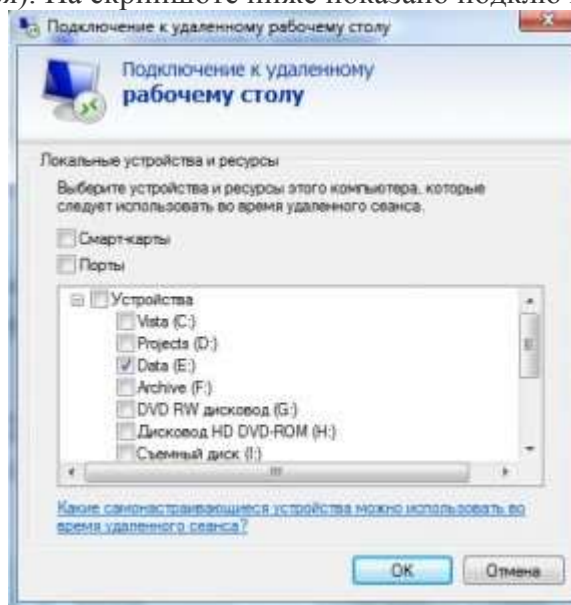


Дополнительные параметры. Закладка Локальные ресурсы.

Раздел «Удаленный звук». Здесь можно настроить где будет воспроизводиться звук (на локальном или удаленном компьютере).

Раздел Клавиатура. Здесь настраивается приоритет сочетаний клавиш между локальным и удаленным компьютером. Обратите внимание, что комбинация **CTRL+ALT+DEL** всегда будет вызывать действие на локальном компьютере. Вместо нее на удаленном компьютере используйте **CTRL+ALT+END**.

Раздел «Локальные устройства и ресурсы». Опция «буфер обмена» разрешает обмен данными между локальным и удаленным компьютером через буфер обмена. Опция Принтеры позволяет печатать на локальном принтере из удаленного рабочего стола. Кнопка Подробнее позволяет подключить к удаленному рабочему столу локальные диски, порты и «прочие устройства» (не знаю, что под этим подразумевается). На скриншоте ниже показано подключение локального диска E:

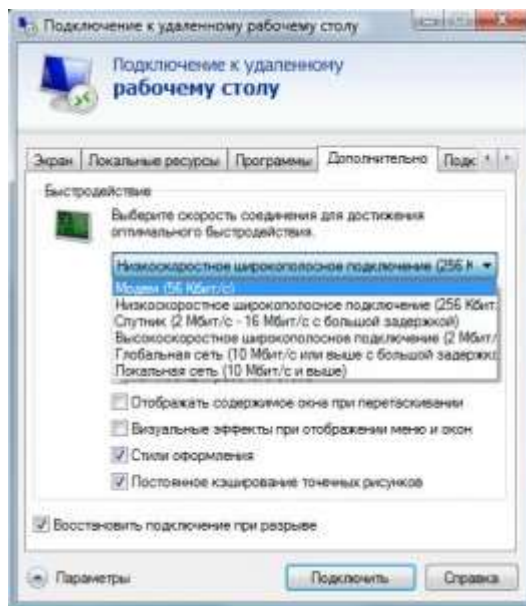


Подключение локального диска

В удаленном рабочем столе, подключенные диски отображаются в окне Компьютер.

Закладка Программы. Здесь можно указать программы (на удаленном компьютере), которые необходимо запустить сразу при входе в систему.

Закладка Дополнительно.



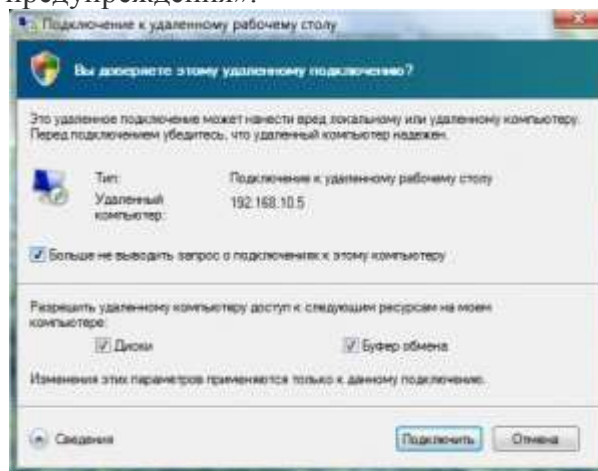
Дополнительные параметры. Закладка Дополнительно.

Здесь можно настроить производительность в зависимости от скорости канала.

Закладка Подключение. Все параметры оставляем без изменений.

После настройки всех опций переходим на закладку Общие и создаем ярлык с выбранными параметрами подключения (кнопка Сохранить как). После этого нажимаем кнопку Подключить.

Появится окно «последнего предупреждения»:



Последнее предупреждение

Вновь нажимаем Подключить, далее вводим пароль учетной записи и наконец попадаем в удаленный рабочий стол.

Практическая работа № 11. Организация удаленного доступа.

Цель работы: сформировать навыки организации удаленного доступа, сформировать умения по настройке удаленного доступа и его организации.

Реализуемые компетенции:

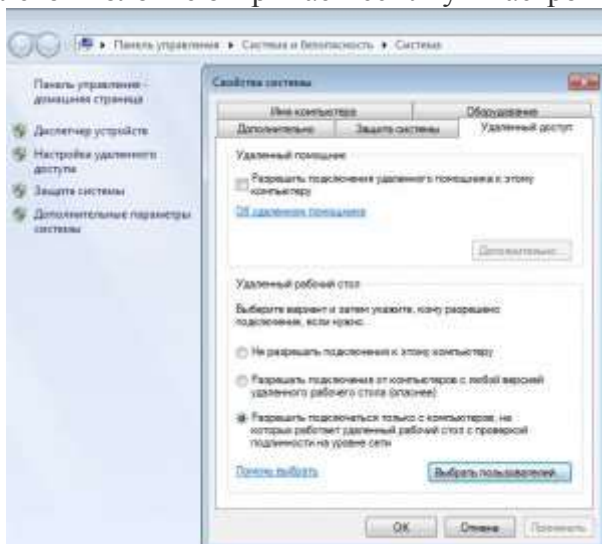
- ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
- ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
- ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.
- ПК 4.4. Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями.

Оборудование, технические и программные средства: персональный компьютер, операционная система Windows 7.

Задания:

Настройка доступа к удаленному рабочему столу

Все достаточно просто. Открываем Панель управления/ Система и безопасность / Система. Далее в левой колонке открываем ссылку «Настройка удаленного доступа»:



Настройка удаленного доступа

В разделе «Удаленный рабочий стол» необходимо выбрать тип подключения:

3. Разрешать подключение от компьютеров с любой версией удаленного рабочего стола (опаснее). Этот вариант подходит для подключения устаревших клиентов (версия протокола удаленного рабочего стола ниже 7.0), а также при подключении через Эксплорер (remote desktop web connection).

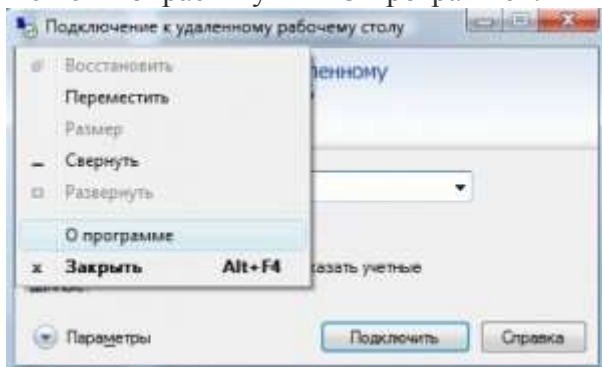
4. Разрешать подключаться только с компьютеров, на которых работает удаленный рабочий стол с проверкой подлинности на уровне сети. Этот вариант подходит для подключения клиентов с версией 7.0 протокола удаленного рабочего стола.

С помощью кнопки «Выбрать пользователей» можно указать учетные записи пользователей, которым разрешено подключаться к удаленному рабочему столу. Тот же самый эффект будет, если в ручную добавить учетные записи в группу «Пользователи удаленного рабочего стола». Обратите внимание, что пользователи входящие в группу администраторов уже имеют доступ к удаленному рабочему столу.

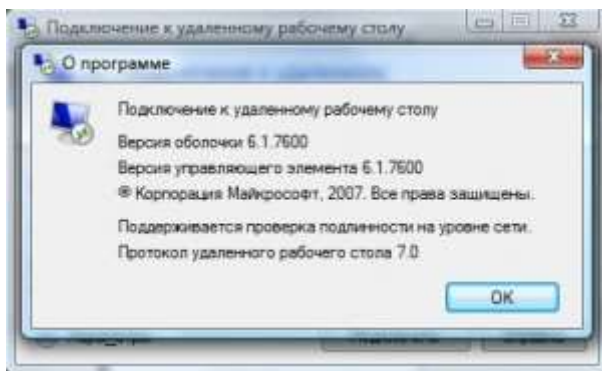
Также имейте в виду, что по умолчанию политика безопасности не разрешает вход в систему через сеть для учетных записей с пустым паролем. Поэтому **учетная запись должна быть защищена паролем** (в том числе и входящая в группу Администраторы), иначе подключиться не получится.

Подключение к удаленному рабочему столу с помощью стандартного клиента

Для начала определяемся какая версия протокола поддерживается нашим клиентом. Для этого запускаем клиент (обычно он находится в меню Пуск -> Программы -> Стандартные -> Подключение к удаленному рабочему столу). Далее кликаем по пиктограмме в левом верхнем углу окна и в меню выбираем пункт «О программе»:



Версия протокола удаленного рабочего стола (1)



Версия протокола удаленного рабочего стола (2)

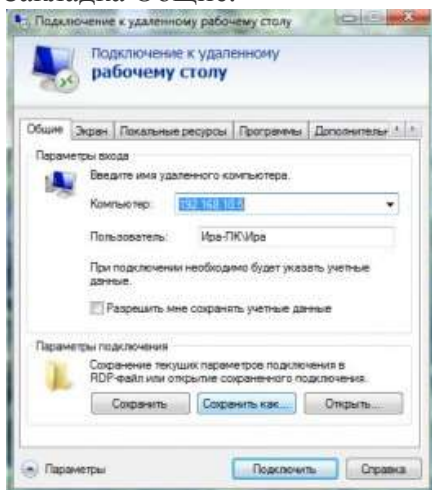
Внизу окна будет указана версия протокола.

Если версия протокола ниже 7.0, то необходимо обновить клиент, или понизить уровень безопасности в настройках сервера (до «Разрешать подключение от компьютеров с любой версией удаленного рабочего стола (опаснее)»). Клиент с поддержкой протокола 7.0 можно скачать здесь:

- Для XP
- Для Vista

Теперь запускаем клиент и настраиваем соединение. Для доступа к дополнительным настройкам нажимаем кнопку Параметры. В окне появятся дополнительные закладки.

Закладка Общие.



Дополнительные параметры. Закладка Общие.

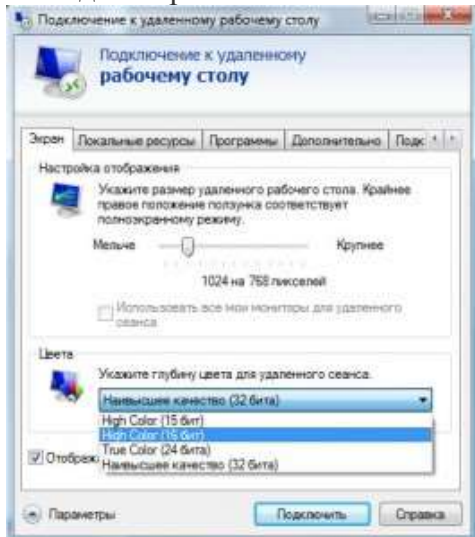
В поле Компьютер указываем ip-адрес или доменное имя компьютера к которому производится подключение.

В поле Пользователь указываем имя пользователя удаленного рабочего стола.

Опцию «Разрешить мне сохранять учетные данные» отмечаем только в том случае, если к компьютеру имеете доступ только вы (а лучше и вовсе оставить ее неотмеченной).

Чтобы сохранить параметры доступа, используем кнопку «Сохранить как».

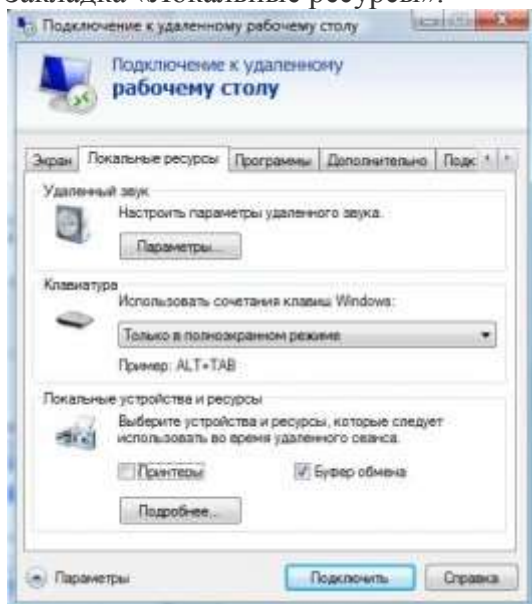
Закладка Экран.



Дополнительные параметры. Закладка Экран.

В разделе «Настройка отображения» выбираем размер удаленного рабочего стола. В разделе Цвета выбираем глубину цвета. Для медленных соединений рекомендуется устанавливать меньшую глубину.

Закладка «Локальные ресурсы».

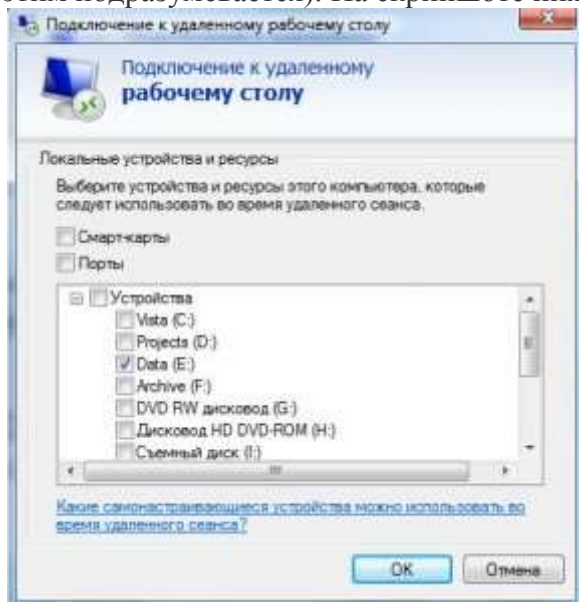


Дополнительные параметры. Закладка Локальные ресурсы.

Раздел «Удаленный звук». Здесь можно настроить где будет воспроизводиться звук (на локальном или удаленном компьютере).

Раздел Клавиатура. Здесь настраивается приоритет сочетаний клавиш между локальным и удаленным компьютером. Обратите внимание, что комбинация **CTRL+ALT+DEL** всегда будет вызывать действие на локальном компьютере. Вместо нее на удаленном компьютере используйте **CTRL+ALT+END**.

Раздел «Локальные устройства и ресурсы». Опция «буфер обмена» разрешает обмен данными между локальным и удаленным компьютером через буфер обмена. Опция Принтеры позволяет печатать на локальном принтере из удаленного рабочего стола. Кнопка Подробнее позволяет подключить к удаленному рабочему столу локальные диски, порты и «прочие устройства» (не знаю, что под этим подразумевается). На скриншоте ниже показано подключение локального диска E:

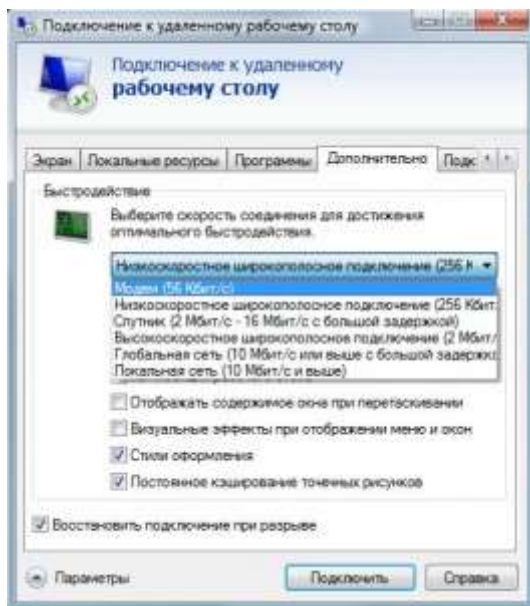


Подключение локального диска

В удаленном рабочем столе, подключенные диски отображаются в окне Компьютер.

Закладка Программы. Здесь можно указать программы (на удаленном компьютере), которые необходимо запустить сразу при входе в систему.

Закладка Дополнительно.

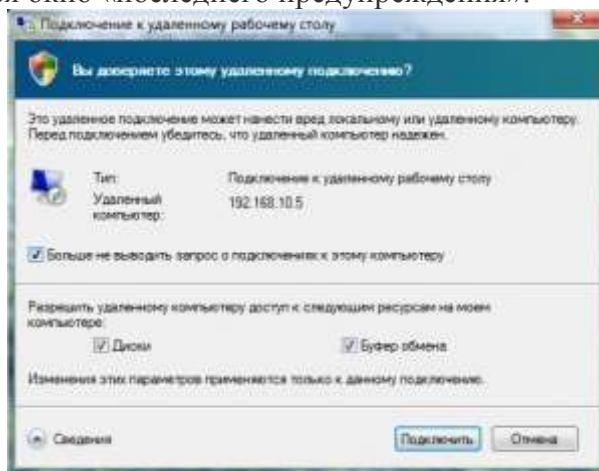


Дополнительные параметры. Закладка Дополнительно.

Здесь можно настроить производительность в зависимости от скорости канала.

Закладка Подключение. Все параметры оставляем без изменений.

После настройки всех опций переходим на закладку Общие и создаем ярлык с выбранными параметрами подключения (кнопка Сохранить как). После этого нажимаем кнопку Подключить. Появится окно «последнего предупреждения»:



Вновь нажимаем Подключить, далее вводим пароль учетной записи и наконец попадаем в удаленный рабочий стол.

Внеаудиторная работа:

- 1) Сформулировать цели работы.
- 2) Написать, что такое удаленный доступ.
- 3) Какими способами можно организовать удаленный доступ.
- 4) Проанализировать и посмотреть на компьютере организацию удаленного доступа к рабочему столу в Windows 7.
- 5) Оформить работу, написать выводы.

Практическая работа №12. Мониторинг и оптимизация корпоративных сетей.

Цель работы: сформировать навыки по выполнению мониторинга и оптимизации системы, сформировать умения по выполнению мониторинга и оптимизации системы.

Оборудование, технические и программные средства: персональный компьютер, операционная система Windows Server 2003.

Ход работы.

Для мониторинга и оптимизации работы компьютера в системах Windows Server 2003 имеется несколько инструментов, позволяющих администратору следить за работой любых компонентов системы и конфигурировать ее оптимальным образом.

Task Manager (Диспетчер задач).

Диспетчер задач служит для просмотра текущих данных о производительности системы. В этой утилите основными являются три индикатора: использование процессора, использование виртуальной памяти и запущенные процессы и программы.

Оснастка **Event Viewer** (Просмотр событий).

Оснастка Просмотр событий позволяет просматривать журналы событий, генерируемых приложениями, службой безопасности и системой.

Performance (Производительность).

Это обновленная оснастка систем Windows XP и Windows Server 2003, аналог утилиты **Performance Monitor** в Windows NT 4.0. Оснастка **Performance** включает в себя два компонента: **ActiveX-элемент System Monitor** и оснастку **Performance Logs and Alerts** (Оповещения и журналы безопасности).

Графические средства **System Monitor** позволяют визуально отслеживать изменение производительности системы. С помощью **System Monitor** можно одновременно просматривать данные с нескольких компьютеров в виде динамических диаграмм, на которых отображается текущее состояние системы и показания счетчиков.

Оснастка **Performance Logs and Alerts** позволяет создавать отчеты на основе текущих данных производительности или информации из журналов. При превышении счетчиками заданного значения или уменьшения нижеуказанного уровня данная оснастка посредством службы сообщений (**Messenger**) посылает оповещения пользователю.

Windows Server 2003 присутствует традиционное для линейки Windows NT 4.0 средство мониторинга производительности – Диспетчер задач (**Task Manager**), который представляет информацию о программах и процессах, запущенных на компьютере, и отображает наиболее общие показатели производительности процессов.

Диспетчер задач можно использовать для отслеживания ключевых индикаторов производительности компьютера, он позволяет определять статус запущенных программ и завершать приложения, которые перестали отвечать на запросы системы. С помощью диспетчера задач можно отслеживать активность запущенных процессов по 25 параметрам и просматривать графики использования процессора и памяти.

В Windows Server 2003 диспетчер задач содержит пять вкладок/индикаторов, среди которых две новых (по сравнению с Windows 2000) – **Networking** (Сеть) и **Users** (Пользователи). Ниже перечислены эти вкладки и указано их назначение.

- **Applications** (Приложения) – показывает статус приложений, запущенных на компьютере.
- **Processes** (Процессы) – содержит информацию о процессах, запущенных на компьютере.
- **Performance** (Быстродействие) – отображает динамическое состояние производительности компьютера, включая степень использования памяти и процессора.
- **Networking** (Сеть) – показывает степень загрузки сети. Индикатор отображается только при наличии на компьютере сетевой карты.
- **Users** (Пользователи) – содержит список зарегистрированных пользователей. Эти пользователи могут регистрироваться локально (с консоли) или являться клиентами служб **Terminal Services**, подключенных с использованием технологий **Terminal Server**, **Remote Access** или **Remote Assistant**.

Запуск диспетчера задач

Для запуска диспетчера задач можно выбрать один из следующих методов.

- Нажать комбинацию клавиш **CTRL + SHIFT + Esc**.
- Щелкнуть правой кнопкой мыши на свободном пространстве панели задач и выбрать в контекстном меню команду **Task Manager**.
- Нажать комбинацию клавиш **CTRL + ALT + Del** и нажать в появляющемся окне кнопку **Task Manager**.
- Вызвать команду **Run** (Выполнить) и ввести **taskmgr**.

Если диспетчер задач запущен, то в правой части панели задач в области оповещений (**system tray**) появляется индикатор загрузки процессора. Если подвести указатель мыши к этому индикатору, то будет показана степень загрузки процессора в процентах.

Окно диспетчера задач можно открыть двойным щелчком на значке индикатора загрузки на панели задач. Если вы не хотите, чтобы свернутое окно диспетчера оставалось на панели задач

среди других запущенных программ, то в окне диспетчера в меню **Options** (Параметры) установите флажок **Hide When Minimized** (Скрывать свернутое).

Для просмотра запущенных процессов и показателей их производительности выберите вкладку **Processes** (Процессы) в окне **Windows Task Manager** (рис. 7.1).

Таблица процессов содержит все процессы, запущенные в собственном адресном пространстве, включая все приложения и системные сервисы. (В Windows 2000 список отображаемых по умолчанию столбцов немного отличается.) Если требуется просматривать также 16-разрядные процессы, то в меню **Options** (Параметры) установите флажок **Show 16-bit tasks** (Отображать 16-разрядные задачи).



Рис. 7.1. Вкладка Processes в окне диспетчера задач

Обратите внимание на флажок **Show processes from all users** (Отображать процессы для всех пользователей) – когда он установлен, отображаются также все процессы, запущенные пользователями, зарегистрировавшимися на компьютере с удаленных систем.

С помощью команды **Select Columns** (Выбрать столбцы) меню **View** (Вид) можно добавить на экран новые столбцы показателей. В открывшемся диалоговом окне **Select Columns** установите флажки рядом с теми показателями, которые должны быть отображены в таблице.

В табл. 7.1 кратко описаны основные столбцы таблицы и соответствующие им счетчики.

Базовый приоритет задается, как правило, кодом приложения. С помощью диспетчера задач можно изменить базовый приоритет процесса. Внесенное изменение будет действительно только в течение времени работы процесса.

При следующем запуске процесс будет выполняться с базовым значением приоритета. Для изменения приоритета процесса выделите имя процесса на вкладке **Processes** и щелкните на нем правой кнопкой мыши. Затем в контекстном меню выберите пункт **Set Priority** (Приоритет) и укажите новый уровень приоритета (рис. 7.2).

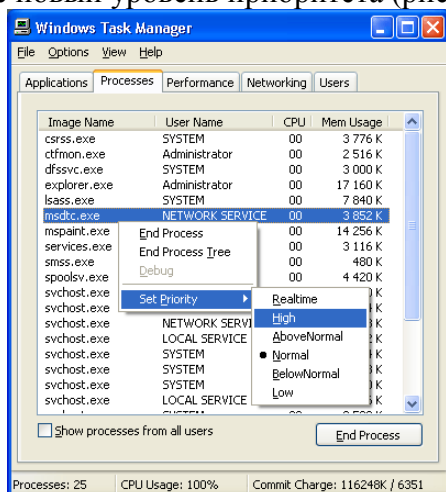


Рис. 7.2. Изменение базового приоритета процесса в диспетчере задач

Выбор процессора

В диспетчере задач можно назначить выполнение Определенного процесса одному или нескольким процессорам. Для этого на вкладке **Processes** щелкните правой кнопкой мыши на названии процессора, укажите пункт **Set Affinity** (Установить связь) и затем выберите один или несколько процессоров.

Опция **Set Affinity** доступна только в том случае, если на компьютере установлено более одного процессора.

Скорость обновления

Вы можете регулировать скорость, с которой обновляются показания счетчиков в диспетчере задач. Это позволяет снизить процент использования ресурсов, но при этом данные могут оказаться слишком приближенными. Для выполнения принудительного обновления выберите команду **Refresh Now** (Обновить) меню **View** (Вид) или нажмите клавишу **F5**.

В диспетчере задач можно задать разности скорости обновления показаний.

- **High** (Высокая) – обновление проводится каждые полсекунды.
- **Normal** (Обычная) – обновление выполняется каждую секунду.
- **Low** (Низкая) – показания обновляются каждые 4 секунды.
- **Paused** (Приостановить) – автоматическое обновление не производится. Для запуска обновления нажмите клавишу **F5**.

Для отслеживания загрузки системы откройте вкладку **Performance** (Быстродействие)

(рис. 7.3).

Для вывода на экран числового значения (в процентах) процессорного времени, в течение которого процессор работал в режиме ядра, выберите команду **Show Kernel Times** (Вывод времени ядра) в меню **View** (Вид). Данное значение равно периоду времени, в течение которого приложения пользовались сервисами операционной системы. Остальную часть времени процессор работал в режиме пользователя, выполняя потоки в режиме работы приложений.

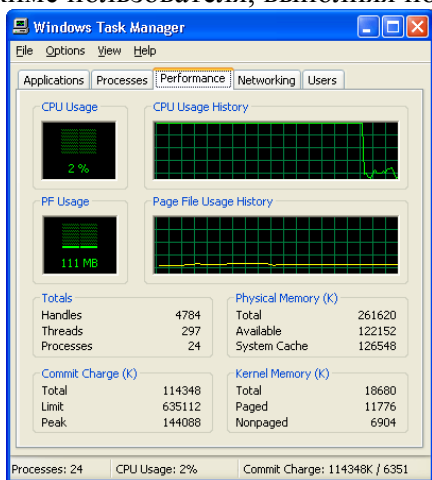
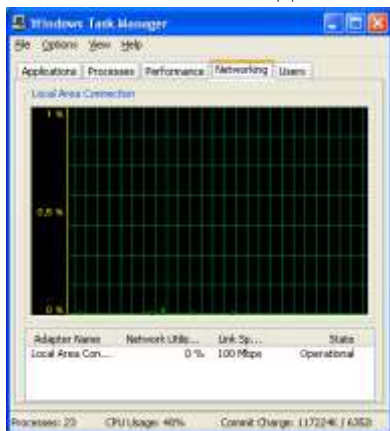


Рис. 7.3. Вкладка Performance

- Пользователи многопроцессорных систем могут выбрать команду **CPU History** (Загрузка ЦП) меню **View**, чтобы вывести график занятости для каждого процессора.
- На вкладке **Networking** (Сеть) можно в виде графика видеть объем информации, передаваемой компьютером по сети в каждый момент времени. Если на компьютере установлены несколько сетевых адаптеров, на вкладке **Networking** будет представлена общая кривая, показывающая объем трафика, передаваемого через все сетевые соединения компьютера (рис. 7.4).
- Команда **View > Network Adapter History** (Вид > Журнал сетевого адаптера)



позволяет отдельно отображать на графике число полученных (**Bytes Received** (Получено байт)) и/или отправленных байт (**Bytes Sent** (Отправлено байт)) для сетевого адаптера.

Рис. 7.4. Вкладка Networking в окне диспетчера задач

- На вкладке **Users** (Пользователи) отображаются имена всех пользователей, зарегистрированных в данный момент на компьютере локально или удаленно (при использовании возможностей служб терминалов).
- Рис. 7.5 иллюстрирует ситуацию, когда один пользователь (**administrator**) зарегистрирован локально, а другой (**alex**) – с удаленного компьютера **NETDC1**.

- На вкладке **Users** (Пользователи) вы можете отключить "лишних" пользователей (кнопка **Disconnect** (Отключить)) или "разрегистрировать" их в системе (кнопка **Logoff** (Выйти из системы)). Для этого, однако, нужно иметь права администратора системы.

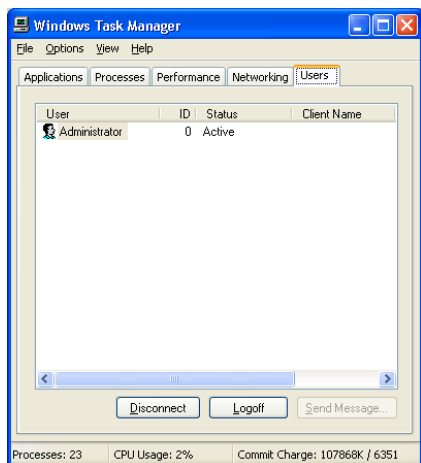


Рис. 7.5. Вкладка Users позволяет увидеть, кто зарегистрирован на компьютере

В операционных системах Windows событием называется любое значительное "происшествие" в работе системы или приложения, о котором следует уведомить пользователей. В случае возникновения критических событий, таких как переполнение диска сервера или неполадки с электропитанием, на экран монитора будет выведено соответствующее сообщение. Остальные события, которые не требуют немедленных действий от пользователя, регистрируются в системных журналах. Служба регистрации событий в системных журналах активизируется автоматически при каждом запуске системы Windows Server 2003.

В системе Windows Server 2003 для просмотра системных журналов можно использовать оснастку **Event Viewer** (Просмотр событий) (группа **Administrative Tools** (Администрирование) на панели управления). Эту оснастку можно также запустить из окна оснастки **Computer Management** (Управление компьютером).

На рис. 7.6 показан пример окна оснастки Event Viewer для контроллера домена.

Сортировка событий

Для определения порядка сортировки событий в журнале щелкните заголовок того столбца, по которому следует отсортировать события. Для отмены установленного порядка сортировки щелкните данный заголовок еще раз.

Порядок сортировки по времени регистрации события можно установить с помощью меню **View** (Вид). Возможны два режима сортировки: **Oldest First** (От старых к новым) или **Newest First** (От новых к старым – опция по умолчанию).

При архивировании журнала порядок сортировки не сохраняется.

Обновление журналов

Выберите в окне оснастки на панели обзора журнал, который требуется обновить. Затем в меню **Action** (Действие) укажите пункт **Refresh** (Обновить).

Следует учитывать, что команда **Refresh** недоступна для архивированных журналов, поскольку данные файлы уже не могут быть обновлены.

Когда вы открываете журнал, оснастка отображает текущую информацию журнала. Во время просмотра журнала информация не обновляется, если не делать это принудительно, по команде **Refresh**. Если журнал не отображается в текущем окне, то информация автоматически обновляется.

Поиск событий

Для поиска события в журнале в меню **View** (Вид) выберите команду **Find** (Найти). В открывшемся окне (которое аналогично окну фильтра, показанному на рис. 7.8) можно установить следующие параметры поиска: по типу события (**Type**), по источнику события (**Source**), по категории (**Category**), коду события (**Event ID**), пользователю (**User**), компьютеру (**Computer**) или описанию (**Description**).

Для начала поиска нажмите кнопку **Find Next** (Найти далее). Для восстановления критериев поиска по умолчанию нажмите кнопку **Restore Defaults** (Восстановить умолчания).

Создание нового вида журнала

Вы можете создать дополнительный вид какого-либо журнала, позволяющий просматривать, скажем, события с определенными параметрами. Для этого:

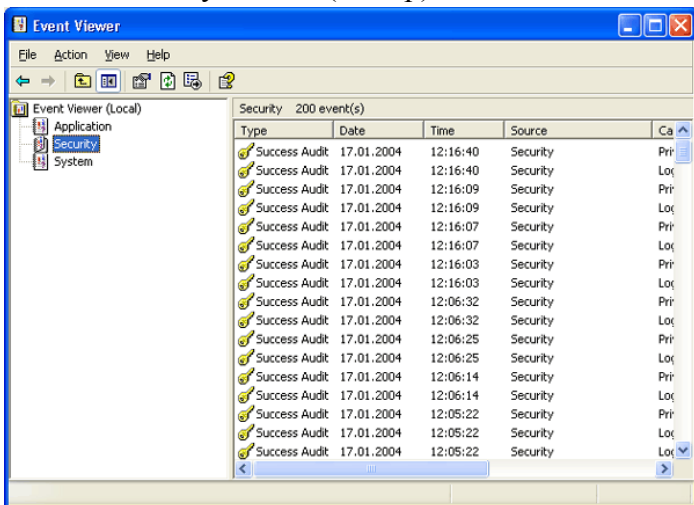
1. Откройте необходимый журнал и в меню **Action** (Действие) выберите пункт **New Log View** (Создать вид журнала).
2. Вызовите для нового журнала контекстное меню и выберите команду **Rename** (Переименовать).
3. Задайте нужный вид журнала (столбцы, фильтр, способ сортировки).

Управление и настройка дополнительных журналов, добавленных в дерево консоли, производится так же, как и журналов по умолчанию.

Просмотр событий на другом компьютере

Для просмотра событий на другом компьютере достаточно в окне оснастки **Event Viewer** подключиться к этому компьютеру:

1. В окне оснастки выберите корневой узел и в меню **Action** выполните команду **Connect to another computer**.
2. Укажите имя удаленного компьютера или найдите его в каталоге, нажав кнопку **Browse**(Обзор).



3. Нажмите кнопку **OK**.

Рис. 7.6. Окно оснастки Event Viewer

Оснастку **Event Viewer** можно также открыть с помощью команды **Start** > **Programs** > **Administrative Tools** > **Event Viewer** (Пуск > Программы > Администрирование > Просмотр событий).

С помощью оснастки **Event Viewer** можно просматривать три типа стандартных (основных) журналов.

- **Журнал приложений** (Application log) – фиксирует события, зарегистрированные приложениями. Например, текстовый редактор может зарегистрировать в данном журнале ошибку при

открытии файла.

- **Журнал системы** (System log) – записывает события, которые регистрируются системными компонентами Windows Server 2003. Например, в системный журнал записываются такие события, как сбой в процессе загрузки драйвера или другого системного компонента при запуске системы.

- **Журнал безопасности** (Security log) – содержит записи, связанные с системой безопасности. С помощью этого журнала можно отслеживать изменения в системе безопасности и идентифицировать бреши в защите. В данном журнале можно регистрировать попытки входа в систему. Для просмотра журнала необходимо иметь права администратора. По умолчанию регистрация событий в журнале безопасности отключена.

Помимо стандартных, на компьютере – в первую очередь на контроллере домена – могут быть и другие журналы, создаваемые различными службами (например, Active Directory, DNS, File Replication Service и т. д.). Работа с такими журналами ничем не отличается от процедур просмотра стандартных журналов.

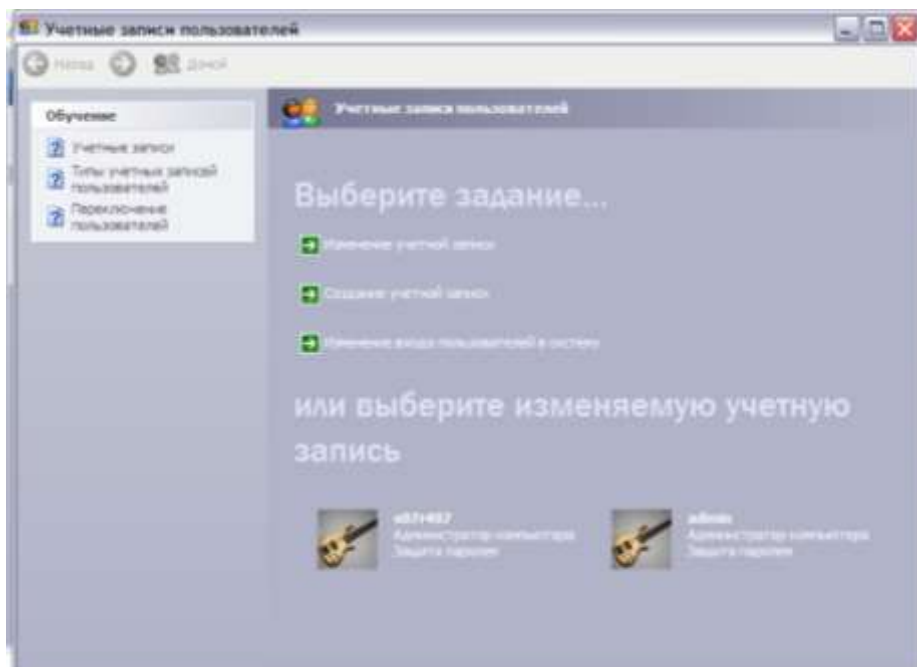
Журнал системы безопасности может просматривать только пользователь с правами системного администратора. По умолчанию регистрация событий в данном журнале отключена. Для запуска регистрации необходимо установить политику аудита.

Практическая работа №13. Конфигурация учетной записи пользователя.

Цель работы: сформировать навыки конфигурирования учетной записи, сформировать умения по настройке учетной записи и работе с учетной записью.

Оборудование, технические и программные средства: персональный компьютер, операционная система Windows 7.

1. Зайдите в Пуск>Настройка>Панель Управления. Здесь кликните «Учетные Записи Пользователей».



2. Выберите элемент «Создать новую учетную запись». Вы будете перенаправлены к мастеру установки, позволяющему ввести имя для учетной записи вручную. Введите нужное имя, кликните «Далее».
3. У вас появится два варианта: Предоставить этой учетной записи доступ с правами администратора или сохранить права рядового пользователя. Учетная запись рядового пользователя позволяет вам изменять основные установки рабочего стола, создавать и изменять ваш пароль, просматривать ваши файлы, но при этом у вас не будет полного доступа ко всем ресурсам системы и к возможности производить изменения.
4. С учетной записью администратора вы получаете все вышеперечисленные права. Вы сможете производить изменения по всей системе, создавать или изменять другие учетные записи, устанавливая все программы и получать полный доступ ко всем файлам системы. Выберите нужную вам опцию и кликните «Создать учетную запись.»
5. Теперь, когда вы создали учетную запись, вы при необходимости можете внести в нее изменения: Изменения рисунка вашей учетной записи, создания или изменения вашего пароля, изменения типа учетной записи (между пользовательской и наделенной функциями администратора) или удаления учетной записи. Все это производится из апплета Учетные Записи Пользователей.
6. Отсюда вы также можете включить учетную запись «Гость», которая предназначена в основном для обеспечения минимального доступа к ресурсам компьютера по сети.

На закладке «Общие» можно указать полное имя и описание учетной записи, а также настроить некоторые свойства пароля учетной записи.

Просмотреть свойства, где находятся, за что отвечают.

Свойства:

Потребовать смену пользователя при следующем входе в систему

Если эта галочка установлена, то при следующем входе в систему Windows попросит пользователя сменить пароль.

Это свойство предполагается применять следующим образом: системный администратор создает новую учетную запись с каким-нибудь стандартным простым паролем, например «12345». Затем пользователь при входе в Windows под этой новой учетной записью меняет пароль на свой собственный.

В результате должно получиться, что пароль пользователя знает только сам пользователь, при этом рекомендуется использовать пароль не меньше 6-8 символов, содержащий буквы в верхнем и нижнем регистре, цифры, спецсимволы.

Это свойство рассчитано на сознательных пользователей, которые понимают важность защиты информации и стараются обеспечивать высокий уровень безопасности.

Запретить смену пароля пользователем

Эта галочка при установке запрещает пользователю самостоятельно менять пароль. Это свойство надо использовать, если пользователи неосознательные и хотят изменить сложный пароль, выданный системным администратором, на простой пароль.

Срок действия пароля не ограничен

Если эта галочка не установлена, то пользователю периодически надо менять пароль. Срок действия пароля по умолчанию, если не ошибаюсь – 42 дня. Если срок действия пароля истек, то запись блокируется.

Отключить учетную запись

Эта галочка нужна при отключении учетной записи. Запись остается в Windows, но не работает. Это используется, например, когда пользователь уходит в отпуск, его запись отключается, и никто не сможет войти в ОС от имени этого пользователя, а после выхода на работу снова включается.

Заблокировать учетную запись

Эта галочка нужна для разблокирования записи. Пользователь ее может только убирать. Если учетная запись заблокирована по каким-либо причинам, то в этом поле появляется галочка, и для разблокирования записи ее надо снять.

Аналогичное описание полей этого окна можно почитать через встроенную подсказку. Для этого надо нажать значок «Вопросительный знак» в правом верхнем углу окна, курсор изменит вид на подсказывающий, затем подвести курсор к нужному полю и нажать еще раз. Должно появиться окно подсказки с описанием объекта.

Внеаудиторная работа:

1. Сформулировать цели работы.
2. Оформить работу, написать выводы.

Практическая работа № 14. Управление профилями пользователей.

Цель: Научиться создавать перемещаемый и преднастроенный перемещаемые профили пользователя, а также обязательный групповой профиль.

Теоретическое обоснование.

Профиль пользователя (*user profile*) — это набор папок и файлов данных, содержащих элементы среды рабочего стола конкретного пользователя. Профиль состоит из:

- ярлыков в меню **Пуск (Start)**, на рабочем столе и на панели быстрого запуска;
- документов на рабочем столе и, если не настроена переадресация, в папке **Мои документы (My Documents)**;

Совет Свойства папки **Мои документы (My Documents)** и политик перенаправления папок в групповой политике позволяют настраивать хранение папок **Мои документы** в сети. Таким образом, содержимое папки можно хранить на сервере, где ее можно архивировать и проверять на наличие вирусов. Кроме того, вы можете обеспечить пользователю доступ к своей папке, даже если он перейдет на другой компьютер в сети организации. Также папку **Мои документы** можно сделать доступной в автономном режиме, чтобы пользователи могли обращаться к своим файлам локально, без подключения к сети. • избранных страниц и файлов «cookie» в Internet Explorer; • сертификатов (если они внедрены в сети); • специальных файлов приложений, например пользовательского словаря, шаблонов и списка автотекста в Microsoft Office; • содержимого папки **Сетевое окружение (My Network Places)**; • параметров отображения рабочего стола, например его вида, фона и заставки. Эти важные элементы у каждого пользователя свои. Желательно, чтобы они не изменялись между входами в систему, были доступны, если пользователю потребуется войти в другую систему, и их можно было восстановить в случае, если система даст сбой и ее потребуется переустановить.

Локальные профили пользователей. По умолчанию профили пользователей хранятся локально в папке **Documents and Settings\Username** и работают следующим образом. • Когда пользователь входит в систему впервые, система создает для него профиль путем копирования профиля *Пользователь по умолчанию (Default User)*.

Имя для нового профиля формируется на основе имени для входа, указанного при первом входе в систему. • Все изменения рабочего стола пользователя и программной среды хранятся в локальном профиле пользователя. Для каждого пользователя существуют отдельные профили, поэтому все параметры индивидуальны. • Пользовательская среда расширена за счет профиля *Все пользователи (All Users)*, который может включать ярлыки на рабочем столе или в меню Пуск

(Start), адреса компьютеров в сети и даже данные приложений. Для создания среды пользователя элементы профиля *Все пользователи* (All Users) соединяются с профилем пользователя.

По умолчанию только члены группы *Администраторы* (Administrators) могут модифицировать профиль *Все пользователи* (All Users). • Профиль является локальным в полном смысле. Если пользователь входит в другую систему, документы и параметры, являющиеся частью его профиля, не перемещаются. Вместо этого, когда пользователь впервые входит в систему, она генерирует для него новый локальный профиль.

Перемещаемые профили пользователей. Если пользователь работает на нескольких компьютерах, вы можете настроить **перемещаемый профиль пользователя** (*roaming user profile, RUP*), чтобы гарантировать сохранность и неизменность его документов и параметров вне зависимости от того, в какую систему он входит. RUP хранит профили на сервере, а значит их можно архивировать, проверять на наличие вирусов и централизованно управлять ими. Даже в среде, где пользователи не перемещаются, RUP обеспечивает сохранность важной информации провидя. Если система пользователя дала сбой и ее необходимо переустановить, RUP гарантирует, что новая пользовательская среда будет идентичная предыдущей. Чтобы настроить RUP, создайте общую папку на сервере. В идеальном случае это должен быть файловый сервер, на котором часто проводится архивирование.

Примечание Настройте общий доступ так, чтобы всем (Everyone) был разрешен полный контроль над папкой (Full Control). Стандартные разрешения общего доступа в Windows Server 2003 позволяют только чтение (Read) папки, но этого недостаточно для настройки перемещаемого профиля. На вкладке **Профиль (Profile)** диалогового окна **Свойства (Properties)** пользователя введите **Путь к профилю (Profile Path)** в следующем формате:

\\<имя_сервера>\<имя_общего_ресурса >% Username%. Вместо переменной % Username% будет автоматически подставлено имя входа пользователя. Как видите, это очень просто. При следующем входе система найдет местоположение перемещаемого профиля.

Примечание Перемещаемый профиль пользователя — это всего лишь общая папка и путь к папке профиля пользователя в пределах этого общего ресурса, указанный в свойстве объекта пользователя. Перемещаемые профили никоим образом не являются свойством объекта компьютера.

Когда пользователь выходит из системы, его профиль выгружается на сервер профилей. Теперь пользователь может входить в эту или в любую другую систему в домене, и его документы и настройки, являющиеся частью RUP, всегда будут под рукой.

Примечание Windows Server 2003 представляет новую политику: *Разрешать использование только локальных профилей* (Only Allow Local User Profiles). Эта политика, связанная с ОП, содержащим учетные записи компьютеров, не позволяет использовать на данных компьютерах перемещаемые профили. Вместо этого пользователи работают с локальными профилями.

Когда пользователь с RUP впервые входит в новую систему, та не копирует профиль *Пользователь по умолчанию* (Default User), а загружает RUP из сетевого ресурса. Когда пользователь выходит из системы или входит в систему, на которой работал ранее, копируются только измененные файлы.

Синхронизация перемещаемого профиля.

В отличие от предыдущих версий, Windows 2000\XP и Windows Server 2003 не загружают и не выгружают весь профиль пользователя при входе и выходе, а синхронизируют его. Между локальной системой и сетевой папкой для хранения RUP перемещаются только измененные файлы. Это означает, что вход и выход из системы с использованием RUP выполняется существенно быстрее, чем в предыдущих версиях Windows. Организации, которые не внедряли RUP из-за опасения, что такие профили будут отрицательно влиять на процесс входа в систему и сетевой трафик, должны еще раз оценить ситуацию с учетом этого момента.

Создание преднастроенного профиля пользователя.

Для упорядочения и предварительной настройки рабочего стола и программной среды можно создавать настроенные профили пользователя, чтобы:

- создать продуктивную рабочую среду с простым доступом к необходимым сетевым ресурсам и приложениям;
- исключить доступ к ненужным ресурсам и приложениям;

- упростить работу службы поддержки по устранению неполадок благодаря более понятному и единообразному рабочему столу.

Для создания преднастроенного профиля пользователя не требуются никакие специальные средства. Просто войдите в систему и измените рабочий стол и настройки приложений по своему усмотрению. Лучше использовать для этого отдельную учетную запись, чтобы без необходимости не изменять собственный профиль. Создав профиль, войдите в систему с административными реквизитами. Из *Панели управления* раскройте окно **Система (System)**, перейдите на вкладку **Дополнительно (Advanced)** и в области **Профили пользователей (User Profiles)** щелкните **Параметры (Settings)**. Выберите созданный профиль и щелкните **Копировать (Copy To)**. Введите путь к профилю в стандартном формате записи пути (UNC):

`\\<имя_сервера>\<имя_общего_ресурса>\<имя_пользователя>`.

В области **Разрешить использование (Permitted To Use)** щелкните **Изменить (Change)**, чтобы выбрать пользователя, для которого вы настроили этот профиль. Таблица управления доступом (ACL) для папки профиля будет настроена так, чтобы разрешить доступ этому пользователю. Пример показан на рисунке 1. Щелкните **ОК** — профиль будет скопирован из сетевого ресурса.

Примечание Для копирования профиля необходимо быть членом группы *Администраторы (Administrators)*.

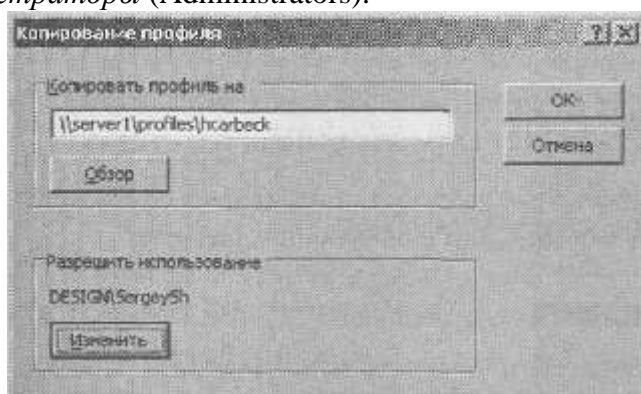


Рисунок 1. Копирование преднастроенного профиля пользователя на сетевой ресурс

Теперь раскройте свойства объекта пользователя и на вкладке **Профиль (Profile)** в поле **Путь к профилю (Profile Path)** введите тот же UNC-путь. И все! При следующем входе пользователя в домен этот профиль будет загружен и определит среду пользователя.

Совет Будьте осторожны при использовании преднастроенных (да и всех остальных) перемещаемых профилей, помните о потенциальных проблемах, связанных с различным аппаратным обеспечением систем, на которых может работать пользователь. Например, если ярлыки на рабочем столе организованы под разрешение XGA (1024x768), а пользователь входит в систему с видеоадаптером, который поддерживает только разрешение SVGA (800x600), возможно, некоторые ярлыки не отобразятся.

Также профили не всегда обладают межплатформенной совместимостью. Профиль, созданный для Windows 98, будет неправильно работать в системе Windows Server 2003.

Несоответствия будут возникать даже при перемещении между системами Windows Server 2003 и Windows XP или Windows 2000 Professional.

Создание преднастроенного группового профиля.

При помощи перемещаемых профилей можно создать стандартную среду рабочего стола для нескольких пользователей с одинаковыми должностными обязанностями. Этот процесс схож с процессом создания преднастроенного профиля для одного пользователя, но результирующий профиль будет доступен нескольким пользователям.

Создайте профиль, выполнив описанные выше действия. При копировании профиля на сервер укажите такой путь:

`\\<имя_сервера>\<имя_общего_ресурса>\<имя_группового_профиля>`.

Необходимо разрешить доступ всем пользователям, которые будут использовать этот профиль. Для этого в области **Разрешить использование (Permitted To Use)** щелкните **Изменить (Change)** и выберите группу, в которую входят все пользователи, или группу `BUILTIN\USERS`, которая включает всех пользователей домена. В действительности профиль будет применен только к тем пользователям, для объектов которых вы указали путь к этому профилю.

После того как профиль скопирован в сеть, необходимо настроить путь к нему для тех пользователей, которым он предназначен. Windows Server 2003 упрощает эту задачу — путь к профилю можно изменить одновременно для нескольких выбранных пользователей. Введите тот же UNC, который вы указали при копировании профиля в сеть, например:

\\<имя сервера>\<имя общего ресурса>\<имя группового профиля>.

Совет Путь к профилю настраивается как свойство одного или нескольких объектов пользователей. Он не назначается объекту группы. Хотя мы считаем, что профиль является групповым, не попадитесь в ловушку — не пытайтесь связать профиль с объектом самой группы.

И наконец, поскольку к групповому профилю получают доступ несколько пользователей, его необходимо сделать обязательным, как описано в следующем разделе.

Настройка обязательного профиля.

Обязательный профиль не позволяет пользователям изменять среду профиля. Точнее, обязательный профиль не сохраняет изменения от сеанса к сеансу. Хотя пользователь и может внести изменения, при следующем входе в систему его рабочий стол будет выглядеть так же, как раньше.

Обязательные профили удобны в ситуациях, когда вы хотите зафиксировать состояние рабочего стола. То есть в практическом смысле обязательные профили полезны, если, создавая групповые профили, вы не хотите, чтобы изменения, которые внесет один пользователь, повлияли на среду других пользователей.

Чтобы сделать профиль обязательным, просто переименуйте файл в корневой папке профиля. Интересно, что обязательные профили не настраиваются путем назначения разрешений. Файл, который вам требуется переименовать, — Ntuser.dat. Это скрытый файл, поэтому убедитесь, что в программе *Свойства папки* (Folder Options) из *Панели управления* вы включили параметр **Показывать скрытые файлы и папки (Show hidden files and folders)**, или запустите из командной строки программу attrib, чтобы снять атрибут **Скрытый (Hidden)**. Возможно, вам понадобится включить в *Проводнике Windows* отображение расширений файлов.

Найдите файл Ntuser.dat в профиле, который собираетесь сделать обязательным.

Переименуйте его в Ntuser.man. Профиль (перемещаемый или локальный) теперь является обязательным.

Ход работы.

Упражнение 1. Настройка объектов пользователей для входа на контроллер домена.

В реальной среде вы вряд ли захотите разрешить пользователям локально входить на контроллер домена, но в нашей тестовой среде с одной системой такая возможность необходима. Существует несколько способов задать необходимое разрешение, но самый простой — добавить группу *Пользователи домена* (Domain Users) в группу *Операторы печати* (Print Operators), которой разрешено входить в систему локально.

1. Откройте консоль *Active Directory* — *пользователи и компьютеры*.

2. В дереве выберите контейнер Builtin.

3. Раскройте окно свойств группы *Операторы печати* (Print Operators).

4. На вкладке **Члены группы (Members)** добавьте группу *Пользователи домена* (Domain Users).

Упражнение 2. Создание общего ресурса для профилей.

1. На диске C: создайте папку Profiles.

2. Правой кнопкой щелкните папку Profiles и выберите **Общий доступ и безопасность (Sharing and Security)**.

3. Перейдите на вкладку **Доступ (Sharing)**.

4. Откройте общий доступ к этой папке, оставив предложенное по умолчанию имя ресурса — Profiles.

5. Щелкните кнопку **Разрешения (Permissions)**.

6. Установите флажок **Полный доступ (Full Control)**.

7. Щелкните **ОК**.

Внимание! При создании общего ресурса Windows Server 2003 по умолчанию ограничивает к нему доступ. В большинстве организаций для общего ресурса включают разрешение **Полный доступ (Full Control)**, а особые разрешения применяют при помощи свойств на вкладке **Безопасность (Security)**. Впрочем, если администратор не защитил ресурс до того, как

открыть к нему общий доступ, Windows Server 2003 в целях безопасности допускает небольшую ошибку, назначая этому ресурсу доступ только для чтения.

Упражнение 3. Создание шаблона профиля пользователя.

1. Создайте учетную запись пользователя, которая будет применяться исключительно для создания шаблонов профилей, по следующим данным:

Поле	Введите
Имя (First Name)	Profile
Фамилия (Last Name)	Учетная запись (Account)
Имя входа пользователя (User Logon Name)	Profile
Имя входа пользователя (пред_ Windows 2000) [User Logon Name (Pre_ Windows 2000)]	Profile

2. Завершите сеанс на Server01.

3. Войдите в систему под учетной записью Profile.

4. Настройте рабочий стол, например создайте ярлыки для локальных или сетевых ресурсов, допустим, для системного диска C:.

5. Настройте рабочий стол при помощи приложения *Экран (Display)* из *Панели управления*.

На вкладке **Рабочий стол (Desktop)** диалогового окна **Свойства экрана (Display Properties)** можно изменить фон рабочего стола и, щелкнув **Настройка рабочего стола (Customize Desktop)**, добавить значки **Мои документы (My Documents)**, **Мой компьютер (My Computer)**, **Сетевое окружение (My Network Places)** и **Internet Explorer**.

6. Завершите сеанс учетной записи Profile.

Упражнение 4. Работа с преднастроенным профилем пользователя.

1. Войдите в систему как *Администратор (Administrator)*.

2. В *Панели управления* дважды щелкните **Система (System)**.

3. Перейдите на вкладку **Дополнительно (Advanced)**.

4. В области **Профили пользователей (User Profiles)** щелкните **Параметры (Settings)**.

Откроется диалоговое окно **Профили пользователей (User Profiles)**.

5. Выберите профиль, который вы настроили для учетной записи Profile.

6. Щелкните **Копировать (Copy To)**.

7. В поле **Копировать профиль на (Copy Profile To)** введите <\\server01\profiles\hcarbeck>.

8. В области **Разрешить использование (Permitted To Use)** щелкните **Изменить (Change)**.

9. Введите **Hank** и щелкните **ОК**.

10. Подтвердите значения, введенные в окне **Копирование профиля (Copy To)**, и щелкните **ОК**.

11. После того как профиль будет скопирован в сеть, щелкните **ОК** в окнах **Профили пользователей (User Profiles)** и **Свойства системы (System Properties)**.

12. Откройте папку C:\Profiles и убедитесь, что папка профиля Hcarbeck создана.

13. В дереве консоли *Active Directory — пользователи и компьютеры* выберите ОП Employees.

14. Откройте свойства объекта пользователя Hank Carbeck.

15. Перейдите на вкладку **Профиль (Profile)**.

16. В поле **Путь к профилю (Profile Path)** введите `\\server01\profiles\%username%`.

17. Щелкните **Применить (Apply)** и убедитесь, что вместо переменной `%Username%` было подставлено имя hcarbeck. Важно, чтобы путь к профилю соответствовал фактическому сетевому пути к папке профиля.

18. Щелкните **ОК**.

19. Проверьте, что преднастроенный перемещаемый профиль пользователя работает правильно. Для этого выйдите из системы и войдите под именем hank.carbeck@contoso.com. Вы должны увидеть изменения, которые внесли на рабочем столе под учетной записью Profile.

Упражнение 5. Работа с преднастроенным обязательным групповым профилем.

1. Войдите в систему как *Администратор* (Administrator).
2. В *Панели управления* дважды щелкните **Система (System)**.
3. Перейдите на вкладку **Дополнительно (Advanced)**.
4. В области **Профили пользователей (User Profiles)** щелкните **Параметры (Settings)**.
5. Выберите профиль, который вы настроили для учетной записи Profile.
6. Щелкните **Копировать (Copy To)**.
7. В поле **Копировать профиль на (Copy Profile To)** введите <\\server01\profiles\sales>.
8. В области **Разрешить использование (Permitted To Use)** щелкните **Изменить (Change)**.
9. Введите *Users* и щелкните **ОК**.
10. Подтвердите значения, введенные в окне **Копирование профиля (Copy To)**, и щелкните **ОК**.
11. После того как профиль будет скопирован в сеть, щелкните **ОК** в окнах **Профили пользователей (User Profiles)** и **Свойства системы (System Properties)**.
12. Откройте папку C:\Profiles и убедитесь, что папка профиля Sales создана.
13. В *Панели управления* раскройте **Свойства папки (Folder Options)** и проверьте, что на вкладке **Вид (View)** в области **Дополнительные параметры (Advanced Settings)** выбран параметр **Показывать скрытые файлы и папки (Show Hidden Files And Folders)**.
14. Раскройте папку C:\Profiles\Sales и переименуйте файл Ntuser.dat в Ntuser.man. Этот профиль станет обязательным.
15. В дереве консоли *Active Directory — пользователи и компьютеры* выберите ОП Employees.
16. Выберите в дереве следующие объекты (щелкните первый объект и, удерживая клавишу Ctrl, — остальные): Scott Bishop, Danielle Tiedt, Lorrin Smith_Bates.
17. В меню **Действие (Action)** выберите **Свойства (Properties)**.
18. Перейдите на вкладку **Профиль (Profile)** и установите флажок **Путь к профилю (Profile Path)**.
19. В поле **Путь к профилю (Profile Path)** введите <\\server01\profiles\sales>.
20. Щелкните **ОК**.
21. Проверьте, что преднастроенный перемещаемый профиль пользователя настроен правильно; для этого выйдите из системы и войдите под именем danielle.tiedt@contoso.com.
22. Удостоверьтесь, что профиль обязательный, изменив вид рабочего стола. Вы сможете внести изменения, но они не сохранятся для будущих сеансов.
23. Выйдите из системы и войдите как Danielle Tiedt. Так как профиль обязательный, вы не увидите изменений, сделанных на предыдущем шаге.
24. Выйдите из системы и войдите как Scott Bishop с именем пользователя scott.bishop@contoso.com. Должен появиться рабочий стол без изменений.

Контрольные вопросы:

1. Опишите, как формируется рабочий стол пользователя, если перемещаемые профили не применяются.
2. Расположите по порядку шаги, в результате которых создается преднастроенный перемещаемый профиль пользователя. Задействуйте все перечисленные шаги.
 - Настройка рабочего стола и среды пользователя.
 - Вход под именем пользователя с разрешениями, достаточными для изменения свойств учетной записи пользователя.
 - Копирование профиля в сеть.
 - Создание учетной записи пользователя таким образом, чтобы профиль можно было сформировать, не изменяя текущие профили остальных пользователей.
 - Вход в систему под учетной записью профиля.
 - Ввод UNC_пути к профилю на странице свойств **Профиль (Profile)** объекта пользователя.
 - Вход в систему в качестве локального администратора или администратора домена.
3. Как сделать профиль обязательным?
 - Настроить разрешения для папки на странице свойств **Безопасность (Security)**, чтобы запретить запись.

- Настроить разрешения для папки на странице свойств **Доступ (Sharing)**, чтобы разрешить только чтение.
- Изменить атрибуты папки с профилем, оставив лишь атрибут **Только чтение (Read Only)**
- Переименовать Ntuser.dat в Ntuser.man.

Практическая работа №15. Планирование стратегии управления доступом.

Цель работы: сформировать навыки планирования стратегий, сформировать умения по планированию стратегий управления доступом.

Оборудование, технические и программные средства: персональный компьютер, операционная система Windows 7.

Ход работы. Прочитайте теоретический материал, спланируйте свою стратегию по управлению доступом.

Принцип управления доступом

Если чрезмерно увеличить нагрузку в воздушном интерфейсе, то зона обслуживания ячейки уменьшается до значений ниже запланированных, и поэтому качество обслуживания имеющихся соединений не может быть гарантировано. Перед тем, как разрешить установление нового соединения, необходимо иметь управление доступом для того, чтобы проверить не повлечет ли разрешение на доступ к уменьшению запланированной зоны обслуживания или качества имеющихся соединений. Управление доступом позволяет принимать или не принимать запрос на установление радиоканала доступа в сети с радиодоступом. Алгоритм управления доступом выполняется, когда устанавливается или видоизменяется канал В. Функциональные возможности управления доступом размещаются в RNC, где можно получить информацию о нагрузке от нескольких ячеек. Алгоритм управления доступом оценивает увеличение нагрузки, к которому приведет установление канала В в радиосети. Оно должно оцениваться по отдельности для восходящего и нисходящего каналов. Запрашивающий канал В может быть допущен, если только управление доступом в восходящем и нисходящем канале позволяет это, в других случаях он не допускается из-за чрезмерных помех, которые будут вызваны в сети. Пределы для управления доступом устанавливаются при планировании радиосети.

Стратегия управления доступом, основанная на широкополосной мощности. В стратегии управления доступом, основанной на помехах, новый пользователь не допускается алгоритмом управления доступом в восходящем канале, если новый полученный полный уровень помех выше порогового значения.

На рис. 9.25 показано управление доступом, основанное на широкополосной мощности. Алгоритм управления доступом в восходящем канале оценивает увеличение нагрузки, используя каждый из нижеприведенных двух способов. В способах оценки увеличения мощности в восходящем канале учитывается кривая нагрузки в восходящем канале.

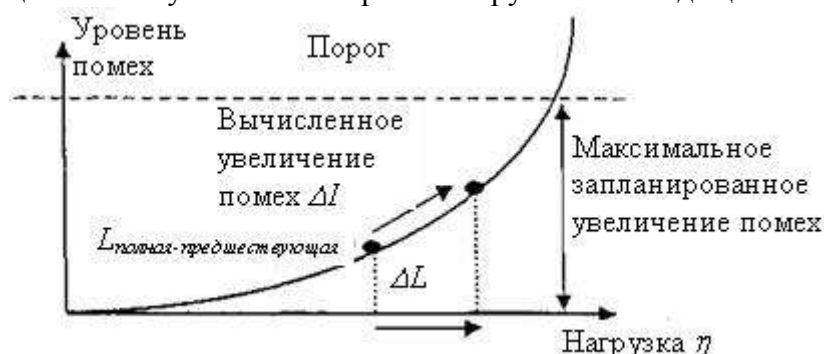


Рис. 9.25. Кривая нагрузки в восходящем канале и оценка увеличения нагрузки из-за появления нового пользователя

- **Мандатное управление доступом** (англ. *Mandatory access control, MAC*) — разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности. Также иногда переводится как **Принудительный контроль доступа**. Это способ, сочетающий защиту и ограничение прав, применяемый по отношению к компьютерным процессам, данным и системным устройствам и предназначенный для предотвращения их нежелательного использования.

Согласно требованиям ФСТЭК мандатное управление доступом или "метки доступа" являются ключевым отличием систем защиты Государственной Тайны РФ старших классов 1В и 1Б от младших классов защитных систем на классическом разделении прав по матрице доступа.

Пример: субъект «Пользователь № 2», имеющий допуск уровня «не секретно», не может получить доступ к объекту, имеющего метку «для служебного пользования». В то же время, субъект «Пользователь № 1» с допуском уровня «секретно» право доступа к объекту с меткой «для служебного пользования» имеет.

Особенности

Мандатная модель управления доступом, помимо дискреционной и ролевой, является основой реализации разграничительной политики доступа к ресурсам при защите информации ограниченного доступа. При этом данная модель доступа практически не используется «в чистом виде», обычно на практике она дополняется элементами других моделей доступа.

Для файловых систем, оно может расширять или заменять дискреционный контроль доступа и концепцию пользователей и групп.

Самое важное достоинство заключается в том, что пользователь не может полностью управлять доступом к ресурсам, которые он создаёт.

Политика безопасности системы, установленная администратором, полностью определяет доступ, и обычно пользователю не разрешается устанавливать более свободный доступ к его ресурсам чем тот, который установлен администратором пользователю. Системы с дискреционным контролем доступа разрешают пользователям полностью определять доступность их ресурсов, что означает, что они могут случайно или преднамеренно передать доступ неавторизованным пользователям.

Такая система запрещает пользователю или процессу, обладающему определённым уровнем доверия, получать доступ к информации, процессам или устройствам более защищённого уровня. Тем самым обеспечивается изоляция пользователей и процессов, как известных, так и неизвестных системе (неизвестная программа должна быть максимально лишена доверия, и её доступ к устройствам и файлам должен ограничиваться сильнее).

Очевидно, что система, которая обеспечивает разделение данных и операций в компьютере, должна быть построена таким образом, чтобы её нельзя было «обойти». Она также должна давать возможность оценивать полезность и эффективность используемых правил и быть защищённой от постороннего вмешательства.

- **Избирательное управление доступом** (англ. *discretionary access control*, DAC) — управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа. Также используются названия «дискреционное управление доступом», «контролируемое управление доступом» или «разграничительное управление доступом».

Субъект доступа «Пользователь № 1» имеет право доступа только к объекту доступа № 3, поэтому его запрос к объекту доступа № 2 отклоняется. Субъект «Пользователь № 2» имеет право доступа как к объекту доступа № 1, так и к объекту доступа № 2, поэтому его запросы к данным объектам не отклоняются.

Для каждой пары (субъект — объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т. д.), то есть тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу (объекту)^[1].

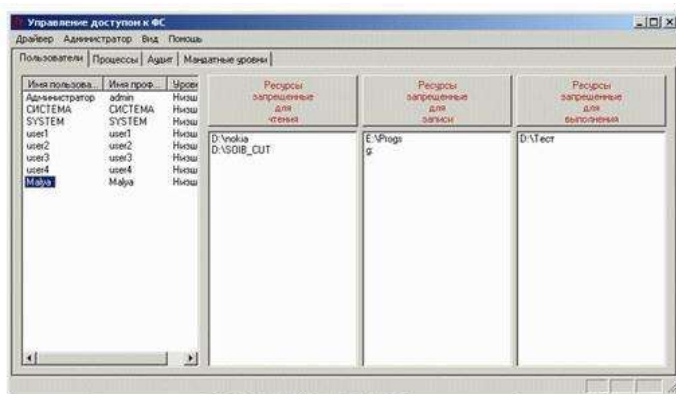


Рис.1 Пример интерфейса настройки дискреционного механизма управления доступом к объектам файловой системы в одной из СЗИ используемого в дополнение к мандатному механизму

Пример настройки матрицы доступа при организации дискреционной модели управления к объектам файловой системы, используемой в дополнение к мандатному механизму

Возможны несколько подходов к построению дискреционного управления доступом:

- Каждый объект системы имеет привязанного к нему субъекта, называемого **владельцем**. Именно владелец устанавливает права доступа к объекту.
- Система имеет одного выделенного субъекта — суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы.
- Субъект с определенным правом доступа может передать это право любому другому субъекту^[2].

Возможны и смешанные варианты построения, когда одновременно в системе присутствуют как владельцы, устанавливающие права доступа к своим объектам, так и суперпользователь, имеющий возможность изменения прав для любого объекта и/или изменения его владельца. Именно такой смешанный вариант реализован в большинстве операционных систем, например Unix или Windows NT.

Избирательное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений, согласно требованиям к системе защиты информации.

Внеаудиторная работа:

1. Придумать свою стратегию управления доступом.
2. Оформите отчет

Практическая работа №16. Реализация стратегии управления доступом

Задание:

- 1) Включите аудит на доступ к объектам на вашем компьютере.
- 2) Создайте на вашем компьютере текстовый файл C:\confidential.txt и внесите в него какой-либо текст. Настройте для этого текстового файла аудит для обращений на чтение от любых пользователей.
- 3) Установите на свой компьютер программу EventTracker (из каталога Мониторинг\Event Log Monitoring\EventTracker).
- 4) Настройте отслеживание событий аудита в EventTracker таким образом, чтобы при любом обращении к файлу c:\confidential.txt на ваш рабочий стол выдавалось соответствующее сообщение по NET SEND.
- 5) Обратитесь к файлу c:\confidential.txt и убедитесь, что настроенное оповещение срабатывает. По окончании лабораторной отключите оповещение.

Решение:

- 1) Откройте консоль Active Directory Users and Computers, раскройте узел для своего домена, щелкните правой кнопкой мыши по контейнеру Domain Controllers, в контекстном меню выберите Properties и перейдите на вкладку Group Policy. Выделите строку Default Domain Controller Policy и нажмите на кнопку Edit. Откроется окно Group Policy Object Editor.
- 2) В окне Group Policy Object Editor раскройте узел Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policies, щелкните по строке Audit object access и установите флажки Success и Failure. Закройте окно редактора групповых политик с сохранением сделанных изменений и выполните в командной строке команду GPUPDATE.
- 3) После создания текстового файла C:\confidential.txt щелкните по нему правой кнопкой мыши, в контекстном меню выберите Properties и перейдите на вкладку Security.
- 4) Нажмите на кнопку Advanced, перейдите на вкладку Auditing и нажмите на кнопку Add. В поле Enter the object name to select... введите Everyone, нажмите на кнопку Check Names, а затем нажмите OK.

- 5) В окне Auditing Entry for confidential.txt установите флажки Successful и Failed напротив строки List Folder/Read Data, затем три раза нажмите ОК, чтобы закрыть окно свойств файла.
- 6) Откройте файл confidential.txt в блокноте, затем откройте Event Viewer и просмотрите в журнале событий Security события с EventID 560.
- 7) Из каталога Мониторинг\Event Log Monitoring\EventTracker на компакт-диске запустите программу ETEwal4-6.exe. Произведите установку с параметрами по умолчанию. На экране Select Applications выберите Enterprise Management Console. На экране Basic Configuration оставьте значения по умолчанию. На экране Get Available Windows Events не устанавливайте флажок Get existing events into Event Tracker.
- 8) После окончания установки из меню Start -> Programs -> Prism Microsystems -> EventTracker запустите программу Event Tracker Management Console.
- 9) В Event Tracker Management Console в меню Configure выберите Configure Alerts и нажмите на кнопку Add.
- 10) На экране Alert Group Configuration введите имя оповещения, например, "Обращение к confidential.txt" и нажмите на кнопку Next.
- 11) На экране Event Details нажмите на кнопку Add Event и введите:
в поле Event Type - Audit Success;
в поле Log Type - Security;
в поле EventID - 560;
в поле Match in Event Descr - C:\confidential.txt.
Нажмите на кнопку ОК, а затем еще раз нажмите на кнопку Add и введите такое же событие, но для поля Event Type выберите тип Audit Failure.
Нажмите на кнопку Next.
- 12) На экране Computers выберите свой компьютер и нажмите на кнопку Add, чтобы поместить его в список выбранных компьютеров.
- 13) На экране Actions установите флажок Send net message и в окне Message введите имя своего компьютера. Затем три раза нажмите на кнопку ОК, чтобы завершить создание оповещения.
- 14) Откройте в блокноте файл confidential.txt, чтобы убедиться, что оповещение срабатывает (при генерации первого сообщения может быть пауза в 10-15 секунд).
- 15) Чтобы отключить оповещение, еще раз в меню Configure выберите Configure Alerts и снимите флажок в столбце Message напротив вашего оповещения.

Практическая работа №17. Мониторинг событий безопасности.

Цель работы: сформировать навыки и умения по организации мониторинга безопасности.

Реализуемые компетенции

- | | |
|--------|--|
| ПК 1.1 | Собирать данные для анализа использования и функционирования информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной системы. |
| ПК 1.2 | Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности. |
| ПК 1.3 | Производить модификацию отдельных модулей информационной системы в соответствии с рабочим заданием, документировать произведенные изменения. |
| ПК 1.4 | Участвовать в экспериментальном тестировании информационной системы на этапе опытной эксплуатации, фиксировать выявленные ошибки кодирования в разрабатываемых модулях информационной системы. |
| ПК 1.5 | Разрабатывать фрагменты документации по эксплуатации информационной системы. |
| ПК 1.6 | Участвовать в оценке качества и экономической эффективности информационной системы. |
| ПК 1.7 | Производить инсталляцию и настройку информационной системы в рамках своей компетенции, документировать результаты работ. |
| ПК 1.8 | Консультировать пользователей информационной системы и разрабатывать фрагменты методики обучения пользователей информационной системы. |
| ПК 1.9 | Выполнять регламенты по обновлению, техническому сопровождению и восстановлению данных информационной системы, работать с технической |

	документацией.
ПК 1.10	Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

Оборудование, технические и программные средства: персональный компьютер, операционная система Windows.

Ход работы. Установка политики аудита Прежде чем организовать аудит, Вы должны продумать политику аудита. В политике аудита определяются категории событий, связанных с безопасностью, которые должны регистрироваться системой. По умолчанию после установки Windows 2000 аудит всех категорий событий отключен. Включая аудит различных категорий событий, Вы можете установить такую политику аудита, которая будет отвечать требованиям безопасности Вашей организации.

Если Вы хотите использовать в политике аудита слежение за доступом к объектам, включите политику **Аудит доступа к службе каталогов (Audit directory service access)** (для наблюдения за объектами на контроллере домена) или политику **Аудит доступа к объектам (Audit object access)** (для наблюдения за объектами на рядовом сервере). После включения аудита доступа к требуемому объекту Вы можете для каждого отдельного объекта указать в его свойствах, нужно ли вести аудит успехов или отказов применительно к разрешениям, предоставленным каждой группе или пользователю.

Чтобы установить аудит доступа к файлам и папкам:

1. Нажмите кнопку **Пуск (Start)**, выберите **Выполнить (Run)**, введите **mmc /a**, после чего нажмите кнопку **ОК**.
2. В меню **Консоль (Console)** выберите пункт **Добавить/удалить оснастку (Add/Remove Snap-in)**, после чего нажмите кнопку **Добавить (Add)**.
3. В списке **Доступные изолированные оснастки (Available Standalone Snap-ins)** выберите оснастку **Групповая политика (Group Policy)** и нажмите кнопку **Добавить (Add)**.
4. В окне **Выбор объекта групповой политики (Select Group Policy Object)** выберите пункт **Локальный компьютер (Local Computer)**, нажмите кнопки **Готово (Finish)**, **Заккрыть (Close)** и **ОК**.
5. Раскройте узел **Политика “Локальный компьютер” (Local Computer Policy)** и выберите пункт **Политика аудита (Audit Policy)**.
6. В области сведений щелкните правой кнопкой мыши по элементу **Аудит доступа к объектам (Audit Object Access)**, после чего выберите пункт **Безопасность (Security)**.

7. В окне **Параметр локальной политики безопасности (Local Security Policy Setting)** установите нужные Вам настройки, после чего нажмите кнопку **ОК**.

Чтобы установить, просмотреть, изменить или удалить аудит доступа к файлам и папкам:

1. Откройте проводник Windows (Windows Explorer) и найдите файл или папку, для которой Вы хотите установить аудит.

2. Щелкните правой кнопкой мыши по этому файлу или папке, выберите пункт **Свойства (Properties)** и перейдите на вкладку **Безопасность (Security)**.

3. Нажмите кнопку **Дополнительно (Advanced)** и перейдите на вкладку **Аудит (Auditing)**.

Выполните одно из следующих действий:

- Чтобы установить аудит для новой группы или пользователя, нажмите кнопку **Добавить (Add)**. В поле **Имя (Name)** введите имя нужного пользователя и нажмите кнопку **ОК** – автоматически откроется диалоговое окно **Элемент аудита (Auditing Entry)**.

- Для просмотра или изменения параметров аудита для существующей группы или пользователя выберите требуемое имя и нажмите кнопку **Показать/Изменить (View/Edit)**.

- Чтобы удалить аудит для существующей группы или пользователя, выберите требуемое имя и нажмите кнопку **Удалить (Remove)**.

Примечание:

- В случае необходимости в диалоговом окне **Элемент аудита (Auditing Entry)** выберите область применения аудита из списка **Применять (Apply onto)**. Этот список доступен только для папок.

- В области **Доступ (Access)** для каждого вида доступа, который вы хотите отслеживать, установите флажок в столбце **Успех (Successful)** и/или **Отказ (Failed)**.

Если Вы не хотите допустить наследования этих параметров аудита файлами и подпапками, установите флажок **Применять этот аудит к объектам и контейнерам только внутри этого контейнера (Apply these auditing entries to objects and/or containers within this container only)**.

- Прежде чем Windows 2000 начнет регистрировать события доступа к файлам и папкам, Вы должны включить параметр **Аудит доступа к объекту (Audit Object Access)** в политике аудита (Audit Policy), используя для этого оснастку **Групповая политика (Group Policy)**. Если Вы этого не сделаете, то при включении аудита доступа к файлам и папкам получите сообщение об ошибке и аудит выполняться не будет. После включения аудита в групповой политике просматривайте журнал безопасности через оснастку **Просмотр событий (Event Viewer)** для анализа журнала безопасности. В нем отслеживаются успешные и неудачные попытки доступа к тем файлам и папкам, для которых Вы установили аудит.

Практическая работа №18. Организация управления совместными ресурсами

Задание: составьте план управления совместными ресурсами в своей ИС

Управление ресурсами сети многогранно и включает в себя следующие задачи:

1) выборочное компрессирование томов, папок и файлов NTFS, осуществляемое для экономии дискового пространства. Электронные таблицы, текстовые файлы и некоторые графические файлы способны уменьшиться в несколько раз;

2) архивация данных и решение сходных с этим задач;

3) разработка сценариев, которые задаются набором команд. Среди них можно выделить: сценарий автоматического выполнения задач при регистрации пользователя в системе, сценарий определенного собственного каталога пользователя, установления соответствующих сетевых связей при использовании разных пользовательских имен, фамилий и т. д.;

4) репликация папок на другие компьютеры, которая санкционирует тиражирование сценариев регистрации с одного контроллера домена на другой, базы данных с одного сервера на другой в целях поддержки и организации доверительных отношений;

5) совместное с диспетчером сервисов управление запуском и работой сервисов. Среди них могут быть приложения, функционирующие на сервере в фоновом режиме и обеспечивающие поддержку других приложений;

6) контроль производительности системы, осуществляемый при помощи программы Системный монитор;

7) управление дисками с использованием программы Администратор дисков, в том числе создание основных и расширенных разделов, форматирование разделов, создание составных томов и т. д.;

8) оптимизация работы Windows NT 4 как файлового сервера, как сервера приложений (контроль процессора сервера приложений, контроль виртуальной памяти, устранение сетевых проблем) и др. В этом случае осуществляется оптимизация работы жестких дисков, устранение проблем доступа к дискам на программном уровне, повышение пропускной способности сети;

9) управление службой печати. Обслуживание принтеров производится благодаря применению программы, доступ к которой осуществляется через папку Принтеры из панели управления или Настройка;

10) управление вводом компьютеров в состав домена своего сервера, организация доменов, удаление компьютеров, назначение сервера главным контроллером домена, репликация данных на другие серверы, объединение доменов, управление доверительными отношениями между доменами, аудит сетевых ресурсов каждого пользователя и т. д. Все перечисленные действия выполняются с помощью программ Диспетчер серверов и Диспетчер пользователей для доменов;

11) управление общими ресурсами. При загрузке компьютера системой Windows NT для каждого из дисков системы создаются системные общие ресурсы, заданные по умолчанию, в целях поддержки работы в сети и управления внутренними операциями;

12) установка управления удаленным доступом. Установка клиента и сервера удаленного доступа приводится в действие с помощью утилиты Сеть из панели управления. Модемы, протоколы и коммуникационные порты устанавливаются с помощью этой же утилиты;

13) управление всеми соединениями в сети и доступом к информации сервера удаленного доступа, для которого применяется утилита Управление удаленным доступом;

14) поиск неисправностей в сети с помощью сетевого монитора, которым можно пользоваться для просмотра поступающих на Windows NT и отправляемых пакетов.

Практическая работа №19. Архивация и синхронизация данных.

Цель работы: сформировать навыки выполнения архивации и синхронизации данных, сформировать умения по выполнению архивации и синхронизации данных.

Оборудование, технические и программные средства: персональный компьютер, операционная система Windows Vista.

Ход работы.

Синхронизация данных – это один из способов облегчить себе жизнь, чтобы наконец-то появилось время думать не только о работе, но и хоть иногда о семье: жене (или муже, это у кого как) и детях. Основное назначение этого странного термина заключается в следующем: помочь вам всегда и при любых условиях иметь при себе последние версии нужных документов. Иными словами, это именно то, что должно помочь ускорить ваш карьерный рост и повысить общий уровень счастья на Земле.

Портфель Windows. Самой долгоживущей функцией Windows, связанной с синхронизацией данных, является **Портфель**. Эта возможность была в Windows 95, есть в Windows Vista и, наверное, будет в Windows Seven и других, еще только ожидаемых операционных системах Windows.

Согласитесь, что название **Портфель** звучит немножко странно для функции операционной системы. На самом деле оно как нельзя лучше объясняет назначение функции.

Для современного делового человека портфель является основным предметом гардероба. В нем хранится все самое важное, без чего обойтись нельзя. Иначе зачем тогда брать это с собой, если оно не самое важное? Фактически, в портфеле содержатся самые сокровенные мечты делового человека.

По аналогии, «компьютерный» **Портфель** предназначен для хранения данных, которые нужно постоянно носить с собой. Что кричат вам родственники или жена в тот момент, когда вы уже вот-вот собрались идти на работу? Если они заботятся о вас, они обязательно заинтересуются, не забыли ли вы взять свой портфель.

Однако «компьютерный» **Портфель** – это не просто современный контейнер для документов. Это самообновляемый современный контейнер для документов. Он позволит вам быть уверенным в том, что уж вы-то точно взяли с собой все самое актуальное и самое новое. С ним вы

сможете забыть о таких недоразумениях, как более старая версия годового отчета, статьи и базы данных, которую обязательно нужно сдать начальству через 10 минут.

Итак, наконец-то заглянем внутрь нашего нового **Портфеля**.

Создание Портфеля

По своей сути **Портфель** является обычной папкой операционной системы, для которой реализована дополнительная функциональность. Перед тем как использовать **Портфель**, его нужно создать. Это делается при помощи команды **Создать > Портфель** контекстного меню **Рабочего стола**, папки **Документы** или любой другой папки (рис. 1.1). Однако перед созданием не забудьте взглянуть на **Рабочий стол** – быть может, **Портфель** там уже есть. С уверенностью можно сказать только одно – в операционных системах Windows Vista по умолчанию **Портфель** не создается.

После того как вы воспользуетесь командой **Создать > Портфель**, операционная система создаст примерно такую папку, как на рис. 1.2. Кстати, сразу определимся, что мы работаем в операционной системе Windows Vista, и все рисунки этой книги будут созданы именно в данной операционной системе. Единственное исключение – функции и программы, которые либо не поддерживаются Windows Vista, либо пока не совместимы с ней.

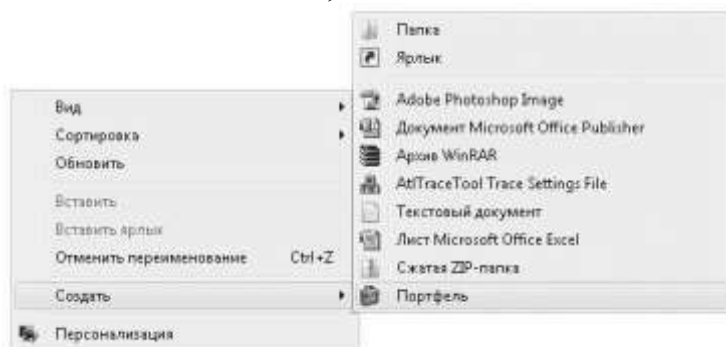


Рис. 1.1. Команда для создания Портфеля



Рис. 1.2. Значок Портфеля. Красивый, да?

Принцип работы Портфеля

Работать с **Портфелем** очень просто. Для этого достаточно поместить в него все свои самые важные документы, содержимое которых вы хотите держать в порядке. Причем свои документы в **Портфель** нужно скопировать, а не переместить. Ведь содержимое этой папки будет синхронизироваться с оригинальной копией документа, а если вы переместите свой документ в **Портфель**, то просто не с чем будет выполнять синхронизацию.

Вот, собственно, и все. Теперь вы можете брать **Портфель** с собой на работу. А после работы вам будет достаточно перенести копию этой папки на свой домашний компьютер (можно также просто подключить внешний накопитель, на котором находится **Портфель**), после чего зайти в **Портфель** и в его панели инструментов выбрать кнопку **Обновить все объекты** (рис. 1.3, слева).

Помимо синхронизации всего содержимого **Портфеля**, вы можете выполнить синхронизацию лишь отдельных его документов. Для этого достаточно выделить нужные вам документы. Сразу же после этого кнопка **Обновить все объекты** будет заменена кнопкой **Обновить выделенные объекты** (либо кнопкой **Обновить объект**, если вы выделили только один из документов, как показано на рис. 1.3, справа).



Рис. 1.3. Слева вид кнопки для синхронизации всего содержимого Портфеля, а справа – только для синхронизации одного выделенного документа

Окно Обновление <имя вашего портфеля>. После того как вы нажмете кнопку синхронизации содержимого, перед вами отобразится окно **Обновление <имя вашего портфеля>** (рис. 1.4). Замечу, что это окно отображается только в том случае, если документ в **Портфеле** или оригинальный документ были изменены. Если же оригинал и документ в **Портфеле** являются идентичными, то перед вами отобразится окно с сообщением об этом.



Рис. 1.4. Окно синхронизации данных

Подробнее изучим содержимое окна **Обновление <имя вашего портфеля>**. В центре приводится список всех файлов, которые вы пытаетесь синхронизировать. Как можно заметить из рис. 1.4, мы синхронизируем только один файл.

В левой части окна отображаются значки документов из **Портфеля**, а в правой части – значки оригинальных документов. Рядом с этими значками содержится очень важная информация: сведения о дате последнего изменения документа, а также о состоянии документа (**Изменен** или **Не изменен**).

Между двумя значками документов находится стрелка, которая наглядно указывает на то действие, которое произойдет при синхронизации. Например, стрелка вправо на рис. 1.4 указывает на то, что документ из **Портфеля** должен заменить собой оригинальный документ. Если вы щелкнете правой кнопкой мыши на этой стрелке, то перед вами отобразится контекстное меню со всеми возможными действиями синхронизации (рис. 1.5).

О **Заменить** (стрелка вправо) – заменить оригинальный документ документом из **Портфеля** (то есть документ из **Портфеля** был изменен, а оригинальный – нет).

О **Заменить** (стрелка влево) – заменить документ из **Портфеля** оригинальным документом (то есть оригинальный документ был изменен, а документ из **Портфеля** – нет).

О **Пропустить** (стрелка вниз) – при синхронизации над данным документом никаких действий не выполнять.

О **Подробности** (стрелки вправо и влево) – возник конфликт, так как оба документа были изменены. В этом случае дважды щелкните кнопкой мыши на стрелке либо на любом из двух значков документов, чтобы отобразить окно с вопросом о том, какой именно файл нужно заменить (рис. 1.6).

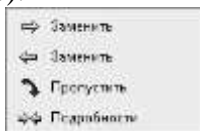


Рис. 1.5. Контекстное меню стрелки



Рис. 1.6. Выбор документа для замены при возникновении конфликта

Дополнительные сведения о работе Портфеля. Важным моментом в понимании работы папки является то, что **Портфелей** может быть несколько (они создаются простым копированием основной папки **Портфель** в каталог, отличный от содержащего основную папку **Портфель**), а оригинальный файл только один. При этом, если вы используете несколько папок **Портфель**, вам придется последовательно синхронизировать каждую из них, так как синхронизация одной из папок **Портфель** не распространяется на другие папки.

Сразу возникает интересный вопрос. Зачем вообще использовать несколько копий папок **Портфель**? Помимо очевидного ответа (если нужно хранить одну папку на работе, другую у друга, а третью носить с собой), существует еще один: в конкретный момент времени с одной

папкой **Портфель** может работать только один пользователь. Если вы попытаетесь открыть папку **Портфель**, которая уже открыта кем-то (либо, например, вы сами открыли **Портфель** при помощи **Проводника** и пытаетесь еще раз открыть его с помощью окна какой-либо другой программы), то будет выведено сообщение об ошибке.

Для понимания еще нескольких дополнительных моментов работы **Портфеля** взгляните на рис. 1.7. В нем представлено окно **Обновление <имя вашего портфеля>**, говорящее о том, что нужно синхронизировать два документа.

Первый из синхронизируемых документов удален. Как можно заметить из записи состояния напротив значка, он удален именно из **Портфеля**, и (внимание!) при синхронизации также будет удалена и оригинальная копия документа!!! По логике операционной системы, если документ из **Портфеля** был удален, а оригинальный документ изменен не был, значит, вы удалили его намеренно, чтобы впоследствии удалить и оригинальный документ.

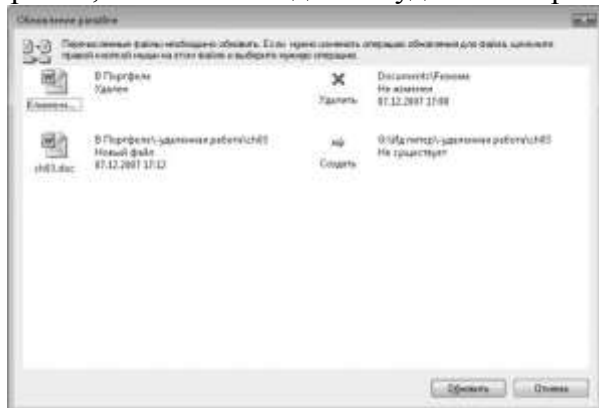


Рис. 1.7. Более сложный пример содержимого окна синхронизации

Если же вы удалили документ из **Портфеля** по ошибке, то следует отобразить контекстное меню стрелки и выбрать там команду **Создать**. Ну, а если вы удалили документ из **Портфеля** специально, чтобы он больше не синхронизировался, то придется вам сообщить, что сделали вы это неправильно. Перед тем как полностью удалить документ из **Портфеля**, необходимо открыть его окно **Свойства** и на вкладке **Состояние** нажать кнопку **Отделить от оригинала** (рис. 1.8).



Рис. 1.8. Вкладка настройки синхронизации для документа

Пока вы не закрыли вкладку **Состояние**, обратите внимание на кнопку **Найти оригинал**, с помощью которой можно открыть папку с оригиналом документа.

Есть еще одна интересная особенность папки **Портфель**, на которую стоит обратить внимание. Помимо отдельных документов, вы можете помещать в нее целые папки. Это необходимо не только для наглядности. Если вы помещаете в **Портфель** папку, то сможете создавать в ней новые папки и файлы. При синхронизации все созданные вами в **Портфеле** объекты будут созданы и в оригинальной папке.

И наконец-то последняя особенность. При помещении в папку **Портфель** базы данных Access вы фактически создаете ее реплику. Об этом вас предупредит операционная система в отобразившемся при копировании окне. Если вы согласитесь на создание реплики, то операционная система задаст вам еще три вопроса.

0 Хотите ли вы конвертировать базу данных в режим Design Master (основная реплика). Учтите, что после преобразования базы данных в основную реплику ее обратное преобразование будет невозможно.

0 Хотите ли вы перед конвертированием создать архивную копию.

0 Какая реплика должна заменяться (оригинальная или реплика Design Master) в том случае, если обе были изменены.

После создания основной реплики базы данных к ее содержимому будет добавлен ряд скрытых системных таблиц, предназначенных для управления репликой. Возможно, вы заметите это по увеличению размера базы данных. Удалить эти таблицы вы уже не сможете. Единственный способ это сделать – создать запросы, которые на основе содержимого таблиц базы данных основной реплики будут создавать новую базу.

Непредвиденные ситуации

В реальной жизни нельзя предсказать все возможные проблемы и ситуации, которые могут возникнуть. Но мы попробуем.

Попробуем предсказать хотя бы некоторые непредвиденные ситуации, которые могут возникнуть при работе с папкой **Портфель**.

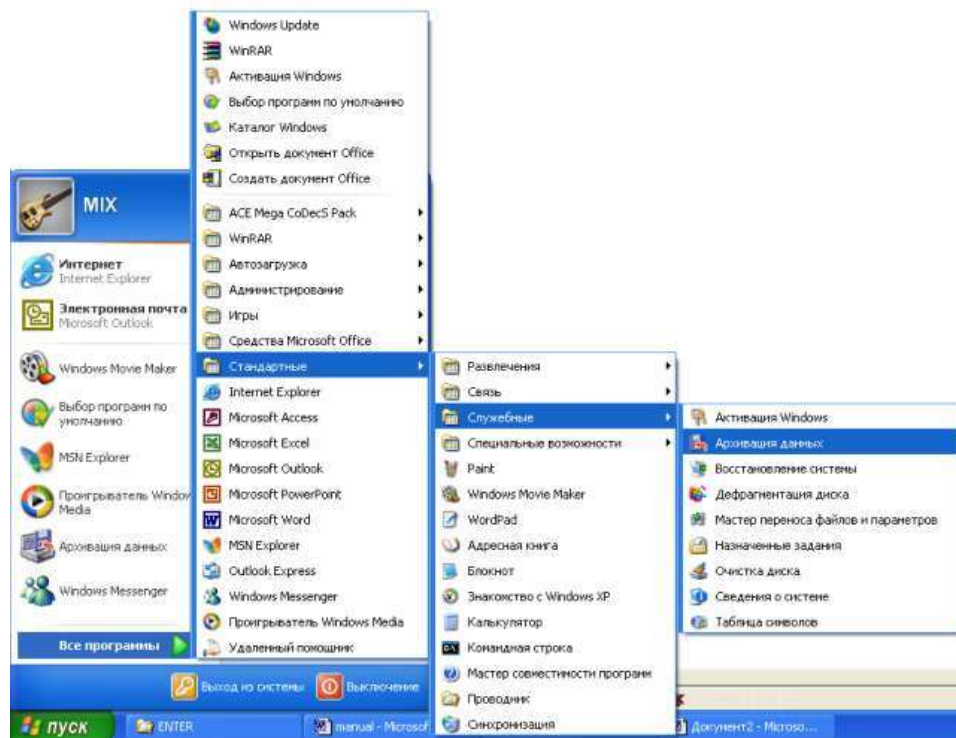
В контекстном меню нет команды Создать > Портфель. Такое может быть в том случае, если вы пытаетесь создать папку **Портфель** внутри папки, которая не поддерживает такой возможности, или вы не имеете в ней прав на это. В любом случае попробуйте создать папку **Портфель** на **Рабочем столе** или в папке **Документы**.

Если команды **Создать > Портфель** нет даже в контекстном меню **Рабочего стола** и папки **Документы**, то дело совсем плохо. Скорее всего, проблема в том, что какая-то программа удалила ветвь реестра, отвечающую за создание папки **Портфель**. В данной книге мы не будем рассматривать структуру и возможности реестра Windows, так как она рассчитана совсем не на тот уровень пользователей. Согласитесь, вряд ли офисному работнику необходимо знать святая святых операционной системы Windows. Однако если по любознательности вас можно сравнить с маленькой лисичкой чиффой из романов М. Фрая, то можете прочитать о реестре в моей книге «Реестр Windows Vista. На 100 %».[1]

Однако вернемся к нашей папке. Если в контекстном меню нет команды для создания портфеля, то ничего страшного, ведь аналог папки **Портфель** можно создать и без помощи команды **Создать > Портфель**. Для этого достаточно создать новую папку, после чего дописать к ее имени строку `{85BBD920-42A0-1069-A2E4-08002B30309D}` (обратите внимание на точку между именем папки и содержимым скобок `{ }` – она обязательна). После этого созданная вами папка преобразится в папку **Портфель** со всей ее функциональностью. Единственным недостатком будет имя папки, которое так и будет содержать добавленную строку.

Я создаю копию папки Портфель, однако в полученной копии нет кнопок для обновления содержимого (синхронизации). В этом случае все просто. Дело в том, что при создании копии **Портфеля** необходимо поместить ее в папку, отличную от той, в которой находится этот **Портфель**. Например, если вы пытаетесь сделать копию **Портфеля**, расположенного на **Рабочем столе**, то эта копия не должна находиться на **Рабочем столе**. Если же вы попытаетесь создать копию в той же папке, что и оригинальный **Портфель**, то вместо копии **Портфеля** будет создана обычная папка со всем его содержимым.

Архивация данных



Синхронизация данных и архивация данных – настолько родственные процессы, что практически все программы архивации данных содержат и возможности синхронизации данных. Архивация данных – это один из тех загадочных механизмов, о которых вспоминают только при наступлении глобальной катастрофы.

Как я уже говорил ранее, глобальная катастрофа может проявить себя по-разному, но ее результат всегда один и тот же – полная или частичная потеря самых важных данных и, естественно, потеря рабочего места.

Именно поэтому каждый служащий должен всегда помнить об этом загадочном механизме. Не следует надеяться на администраторов. Мол, если что, они должны периодически делать архивацию всех данных компании, а значит, мне нечего бояться. Нет! Об архивации своих данных – тех данных, которые доверили именно вам, – должны заботиться именно вы! И только в этом случае можно надеяться на быстрый карьерный рост. Ведь работодатели больше всего ценят тех служащих, с которыми у них никогда не бывает проблем.

В самом простом случае архивация данных – это процесс периодического копирования важных данных на другой жесткий диск. Такой процесс можно организовать и вручную – приучить себя один-два раза в день копировать все измененные данные на дополнительный накопитель. Однако это не самый верный способ решения данной проблемы.

Самым правильным способом архивации данных является организация RAID-массива из нескольких жестких дисков. В этом случае все создаваемые данные будут мгновенно копироваться и на второй диск массива. Однако мы не будем рассматривать этот способ, так как он не всегда подходит для применения внутри компании.

В первую очередь это связано с теми проблемами, которые не зависят от вас: как правило, на компьютерах компаний стоит только один диск, а установка дополнительных накопителей на каждый компьютер для крупных организаций может влететь в столь же крупные затраты.

Второй же проблемой при использовании RAID-массива является то, что он не сможет оградить вас от ваших же ошибок. Например, от нечаянного удаления важных данных. Иными словами, даже при использовании RAID-массива вам все равно придется подумать над автоматической архивацией важных данных на другой носитель.

Существует множество специальных программ и методик, предназначенных для облегчения архивации данных. С ними вы вообще забудете о том, что такое архивация, и будете вспоминать лишь в те моменты, когда придется быстро восстановить все потерянные данные из архивной копии, автоматически созданной программой архивации.

Стандартные возможности Windows

Некоторые возможности архивации данных поддерживает и операционная система Windows Vista. Таких возможностей несколько, поэтому рассмотрим их по порядку от простых к более сложным.

Мастер Центр архивации и восстановления

Мастер Центр архивации и восстановления (рис. 1.23), доступ к которому можно получить при помощи одноименного значка Панели управления, предлагает самый простой способ назначения задания на автоматическое периодическое выполнение архивации.

Архивация данных. Чтобы начать архивацию файлов, нужно нажать кнопку Архивировать файлы мастера Центр архивации и восстановления. После этого перед вами отобразится мастер Архивировать файлы, на первом шаге которого нужно выбрать место хранения архивных файлов.

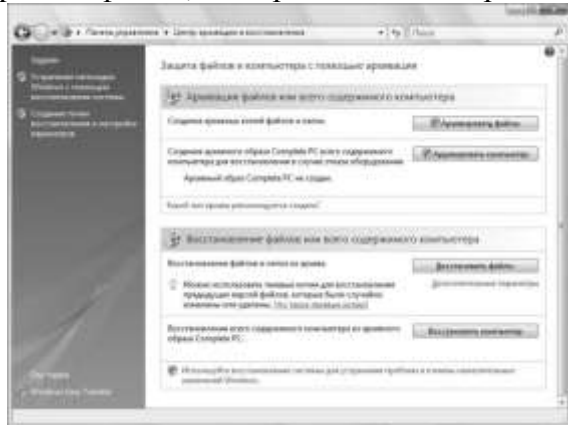


Рис. 1.23. Мастер Центр архивации и восстановления

Операционная система Windows Vista поддерживает использование трех различных мест хранения файлов: определенный раздел жесткого диска, компакт-диск либо общий ресурс локальной сети. Следует учитывать, что операционная система не может хранить файлы на системном и загрузочном разделах диска локального компьютера. Это связано с принципом архивирования файлов.

После того как вы выберете место хранения архивных файлов, операционная система предложит вам указать диски, содержимое которых будет включено в архив. Причем системный раздел диска (на который установлена операционная система Windows Vista) включается в архив по умолчанию, и отключить его нельзя.

К сожалению, вы не сможете выбрать отдельные папки, содержимое которых должно архивироваться. Архивирование средствами Windows Vista построено по другому принципу: архивируется либо все содержимое раздела диска, либо ничего.

Есть много типов файлов, которые различает мастер архивирования операционной системы Windows Vista, поэтому вы всегда сможете выбрать только те файлы, которые хотели бы видеть в архиве. При этом следует учитывать, что системные файлы, файлы программ и временные файлы никогда не помещаются в архив.

На последнем шаге мастера архивирования файлов нужно указать периодичность, с которой операционная система будет запускать архивирование файлов. При этом вы можете указать как время запуска, так и день либо число.

После того как вы определитесь с периодичностью архивирования файлов, просто нажмите кнопку Сохранить параметры и начать архивацию. Это приведет к запуску процесса архивации, перед началом которого будет создана теньная копия.

Восстановление данных. Если вам все-таки необходимо восстановить потерянные данные, следует воспользоваться кнопкой Восстановить файлы мастера Центр архивации и восстановления. После нажатия этой кнопки откроется окно мастера Восстановление файлов, на первом шаге которого следует выбрать, из какого именно архива вы будете восстанавливать файлы.

Можно выбрать восстановление из последнего созданного архива (дата последнего создания архива указывается рядом с кнопкой Архивировать файлы мастера Центр архивации и восстановления) либо указать архив в отобразившемся списке созданных архивов.

После того как вы укажете архив для восстановления, перед вами отобразится окно мастера на шаге выбора из архива конкретных файлов, которые нужно восстановить. Вид данного окна после добавления нескольких файлов представлен на рис. 1.24.

На описанном шаге мастера вы можете выбрать не только конкретный файл для восстановления, но и восстановление содержимого целой папки. Это делается при помощи кнопок Добавить файлы и Добавить папки соответственно. После того как вы нажмете одну из этих кнопок, перед вами отобразится стандартное окно выбора файла/папки, расположенных внутри архива

(архив принимается за корень, от которого строится дерево каталогов, где вы выбираете нужный файл или каталог).

Выбрать файлы и папки для восстановления можно и при помощи кнопки Поиск. В этом случае откроется окно для поиска файлов и папок по части их названия.

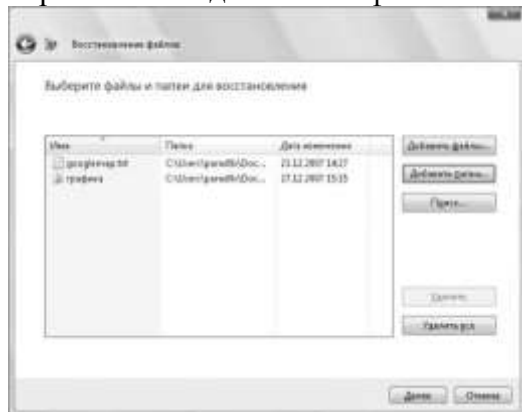


Рис. 1.24. Шаг мастера для выбора файлов и папок, которые нужно восстановить

После того как вы выберете данные для восстановления, мастер попросит вас выбрать место, в которое будут восстановлены указанные вами данные. Вы можете восстановить данные в исходное место (то есть туда, где они находились во время архивирования) либо указать другой каталог.

На этом мастер завершит свою работу и восстановит выбранные вами файлы.

Практическая работа №20. Выполнение резервного копирования данных в различных информационных системах. Перенос файлов и параметров.

Практическая работа №21. Выполнение резервного копирования данных в различных информационных системах. Копирование файлов вручную.

Цель работы: сформировать навыки выполнения резервного копирования, сформировать умения по выполнению резервного копирования в различных информационных системах.


Оборудование, технические и программные средства: персональный компьютер, операционная система Windows 7, Windows XP, Windows Vista.

Ход работы.

1. Резервное копирование данных на компьютере с системой Windows 7.


Перенос файлов и параметров на другой компьютер с системой Windows 7

Средство переноса данных Windows позволяет создать резервную копию файлов и параметров для всех учетных записей, а затем восстановить эти данные на другом компьютере. Чтобы запустить средство переноса данных Windows, выполните указанные ниже действия.

1. Нажмите кнопку **Пуск** , введите в поле **Начать поиск** запрос **средство переноса данных windows**, выберите в списке **Программы** пункт **Средство переноса данных Windows**
2. и следуйте инструкциям по переносу файлов и параметров.

Перенос файлов и параметров в систему Windows Vista

Если необходимо перенести данные из системы Windows 7 в Windows Vista, воспользуйтесь версией средства переноса данных Windows для Windows Vista. Для этого выполните действия, указанные ниже.

1. На компьютере с системой Windows 7 вставьте в дисковод компакт- или DVD-диск с системой Windows Vista.
2. Закройте программу установки системы Windows Vista.
3. Нажмите кнопку **Пуск** , выберите пункт **Компьютер**, щелкните дисковод для компакт- или DVD-дисков правой кнопкой мыши и выберите команду **Открыть**.
4. Откройте по очереди папки **support** и **migwiz**.
5. Дважды щелкните файл **Migwiz.exe**.
6. Следуйте инструкциям по переносу данных из системы Windows

Резервное копирование данных в качестве меры предосторожности

Для резервного копирования данных в качестве меры предосторожности можно использовать Центр архивации и восстановления Windows 7. Имейте в виду, что резервную копию данных Windows 7 можно восстановить только в операционной системе Windows 7.

1. Нажмите кнопку **Пуск** , в поле **Начать поиск** введите запрос **архивация** и в списке **Программы** выберите пункт **Архивация и восстановление**.

Если появится сообщение с предложением закрыть все программы, сохраните открытые документы и закройте программы самостоятельно или нажмите кнопку **Закрывать программы**, чтобы закрыть их автоматически.

2. Выберите в разделе **Архивация и восстановление файлов** параметр **Настройка архивации**.

3. Укажите место сохранения резервной копии и нажмите кнопку **Далее**.


4. Выберите параметр **Восстановить значения по умолчанию** или **Предоставить мне выбор** и нажмите кнопку **Далее**.

5. Выберите необходимые файлы и нажмите кнопку **Далее** или **Сохранить параметры и начать архивацию**.

6. Резервная копия будет сохранена в указанном месте.

Копирование файлов вручную

Чтобы вручную скопировать файлы в сетевую папку или на съемный носитель, например на внешний жесткий диск, компакт- или DVD-диск или карту памяти USB, выполните указанные ниже действия.

1. Нажмите кнопку **Пуск** , выберите пункт **Компьютер** и дважды щелкните диск, на котором установлена система Windows 7.

2. Откройте папку **Users**, а затем — папку пользователя, файлы из которой необходимо включить в резервную копию.

3. Скопируйте необходимые папки из папки пользователя в сетевую папку или на съемный носитель.

Примечание. Чтобы создать резервные копии данных для всех пользователей, повторите действия 2 и 3.

Совет. Чтобы определить размер всех файлов в папке пользователя, выделите все папки, щелкните их правой кнопкой мыши и выберите пункт **Свойства**.


Сохраненные файлы можно скопировать на любой компьютер. Однако чтобы можно было открыть эти файлы, на компьютере должны быть установлены соответствующие приложения.

Внимание! Не все приложения хранят свои файлы в папке пользователя. Выясните места хранения файлов необходимых приложений и скопируйте эти файлы в сетевую папку или на съемный носитель.

2. Резервное копирование данных на компьютере с системой Windows Vista

Перенос файлов и параметров на другой компьютер с системой Windows Vista

Средство переноса данных Windows позволяет создать резервную копию файлов и параметров для всех учетных записей, а затем восстановить эти данные на другом компьютере. Чтобы запустить средство переноса данных Windows, выполните указанные ниже действия.

1. Нажмите кнопку **Пуск** , введите в поле **Начать поиск** запрос **перенос** и выберите в списке **Программы** пункт **Средство переноса данных Windows**.

2. Нажмите кнопку **Далее**. Если появится сообщение с предложением закрыть все программы, сохраните открытые документы и нажмите кнопку **Закрывать все**.

3. Нажмите кнопку **Начать новый перенос**.

4. Щелкните элемент **Исходный компьютер**.

5. Выберите параметр **Использовать CD, DVD или другой съемный носитель**.

6. Выберите параметры переноса файлов.

7. Укажите расположение для файлов, задайте пароль (если необходимо) и нажмите кнопку **Далее**.


8. Выберите переносимые файлы.

9. Просмотрите выбранные файлы, нажмите кнопку **Далее** или **Перенести**

10. и следуйте инструкциям по переносу файлов и параметров.


Резервное копирование данных в качестве меры предосторожности

Для резервного копирования данных в качестве меры предосторожности можно использовать Центр архивации и восстановления Windows Vista. Имейте в виду, что резервную копию данных Windows Vista можно восстановить только в операционной системе Windows Vista.

1. Нажмите кнопку **Пуск** , в поле **Начать поиск** введите запрос **архивация** и в списке **Программы** выберите пункт **Архивация и восстановление**.
2. В разделе **Архивация файлов или всего содержимого компьютера** выберите пункт **Архивация файлов**.
3. Укажите место сохранения резервной копии и нажмите кнопку **Далее**.
4. Выберите для архивации один или несколько дисков и нажмите кнопку **Далее**.
5. Выберите для архивации один или несколько типов файлов и нажмите кнопку **Далее**.
6. Щелкните элемент **Сохранить параметры** и запустите резервное копирование.
7. Резервная копия будет сохранена в указанном месте.

Копирование файлов вручную

Чтобы вручную скопировать файлы в сетевую папку или на съемный носитель, например на внешний жесткий диск, компакт- или DVD-диск или карту памяти USB, выполните указанные ниже действия.

1. Нажмите кнопку **Пуск** , выберите пункт **Компьютер** и дважды щелкните диск, на котором установлена система Windows Vista.
2. Откройте папку **Users**, а затем — папку пользователя, файлы из которой необходимо включить в резервную копию.
3. Скопируйте необходимые папки из папки пользователя в сетевую папку или на съемный носитель.

Примечание. Чтобы создать резервные копии данных для всех пользователей, повторите действия 2 и 3.

Совет. Чтобы определить размер всех файлов в папке пользователя, выделите все папки, щелкните их правой кнопкой мыши и выберите пункт **Свойства**.

Сохраненные файлы можно скопировать на любой компьютер. Однако чтобы можно было открыть эти файлы, на компьютере должны быть установлены соответствующие приложения.

Внимание! Не все приложения хранят свои файлы в папке пользователя. Выясните места хранения файлов необходимых приложений и скопируйте эти файлы в сетевую папку или на съемный носитель.

3. Резервное копирование данных на компьютере с системой Windows XP или Windows Server 2003

Перенос файлов и параметров из системы Windows XP

Для переноса файлов с компьютера с системой Windows 2000, Windows XP или Windows Server 2003 на другой компьютер с одной из этих же систем используйте мастер переноса файлов и параметров Windows XP.

1. Нажмите кнопку **Пуск** и выберите по очереди пункты **Программы**, **Стандартные**, **Служебные** и **Мастер переноса файлов и параметров**.
2. Нажмите кнопку **Далее**, выберите вариант **Исходный компьютер** и снова нажмите кнопку **Далее**.
3. Выберите параметры переноса файлов. Если выбрать параметр **Другое**, можно будет сохранить файлы в сетевой папке или на съемном носителе, что позволит создать резервную копию данных.
4. Выберите элементы, подлежащие резервному копированию, и нажмите кнопку **Далее**.

Внимание! Не все приложения хранят свои файлы в папке пользователя, поэтому сначала выясните места хранения файлов приложений сторонних производителей, а затем скопируйте эти файлы в сетевую папку или на съемный носитель.

Копирование файлов вручную

Чтобы вручную скопировать файлы в сетевую папку или на съемный носитель, например на внешний жесткий диск, компакт- или DVD-диск или карту памяти USB, выполните указанные ниже действия.

1. Нажмите кнопку **Пуск**, выберите пункт **Компьютер** и дважды щелкните диск, на котором установлена система Windows.
2. Откройте папку **Users**, а затем — папку пользователя, файлы из которой необходимо включить в резервную копию.
3. Скопируйте необходимые папки из папки пользователя в сетевую папку или на съемный носитель.

Примечание. Чтобы скопировать данные всех пользователей, повторите действия 2 и 3.

Совет. Чтобы определить размер всех файлов в папке пользователя, выделите все папки, щелкните их правой кнопкой мыши и выберите пункт **Свойства**.

Сохраненные файлы можно скопировать на любой компьютер. Однако чтобы можно было открыть эти файлы, на компьютере должны быть установлены соответствующие приложения.

Внимание! Не все приложения хранят свои файлы в папке пользователя. Выясните места хранения файлов необходимых приложений и скопируйте эти файлы в сетевую папку или на съемный носитель.

Внеаудиторная работа:

4. Составить отчет по практической работе.
5. Составить таблицу сходств и различий выполнения резервного копирования в различных операционных системах.
6. Сделать выводы.

Практическая работа №22. Планирование действий на случай аварийных ситуаций

Цель: получить навыки планирования действий на случай аварийных ситуаций

Задание: выполнить планирование действий на случай аварийных ситуаций

Отказы в работе информационных систем – события, которые невозможно исключить полностью. Вне зависимости от причин случившегося сбоя, в момент его возникновения на системного администратора ложится груз ответственности по оперативному восстановлению работоспособности не только ИТ-систем, но и бизнеса в целом.

В цикле из трех коротких статей я постараюсь доступно описать процесс формирования плана аварийного восстановления, который позволяет перевести задачи по восстановлению работоспособности систем в разряд заранее согласованных с руководством мероприятий, имеющих свой график, ресурсы и бюджет.

В первой статье речь пойдет об определении зоны планирования, или поиске тех инфраструктурных элементов, отказ в работе которых негативно влияет на частоту пульса системного администратора. Итак, по порядку:

1. Составляем список критичных пользовательских ИТ-сервисов

Цель планирования аварийного восстановления — обеспечить оперативное восстановление работы конечного сервиса, который получает пользователь, а не какой-то конкретной железки или программы. Пользователю не важно, работает или сломан его принтер – ему важно может он отпечатать документы или нет. Жаловаться пользователь будет не на то, что в сервере отказал жесткий диск, а на то, что у него не работает «1С-ка» или «почта».

По этой причине первое, что мы делаем – определяем список критичных пользовательских ИТ-сервисов, для которых будем планировать аварийное восстановление. Обычно это:

- Электронная почта,
- Телефонная связь,
- Система управления предприятием,
- Совместная работа с документами,
- Печать документов,
- Доступ в Интернет,
- И так далее.

По сути, пользовательские сервисы – это те рабочие инструменты, которые покупает бизнес, вкладывая деньги в железо, ПО и зарплаты специалистов и которые критичны для его функционирования. К примеру сервер «Counter Strike», конечно же, является важным элементом в вопросах улучшения рабочего настроения сотрудников, но не критичным для работы бизнеса.

2. Определяем точки отказа пользовательских сервисов

Если пользователь будет жаловаться на проблемы в каком-то конечном сервисе, то чинить все равно придется конкретный элемент в ИТ-инфраструктуре. Поэтому на данном этапе необходимо обнаружить все системы, приложения и ИТ-сервисы, отказ в работе которых неминуемо приведет к остановке или снижению качества работы критичных пользовательских сервисов. Проще говоря, ваша задача найти все точки отказа.

Под точкой отказа мы подразумеваем ту инфраструктурную единицу, о которой мы не можем

сказать больше, чем «оно не работает». К примеру, если ваш маршрутизатор модульный, то в нем может отказать как само шасси, так и вставляемые в него модули. Если вашей компетенции достаточно для локализации и замены отказавших блоков в случае сбоя – у вас несколько точек отказа в одном устройстве, если нет – то точка отказа одна.

Так, у сервиса «Электронная почта» могут быть следующие точки отказа (включая, но не ограничиваясь):

- Серверная ОС,
- Серверное почтовое приложение,
- Коммутатор ядра,
- Электроснабжение,
- Внешняя зона DNS,
- Попадание в «черные списки»,
- Кондиционирование серверной.

Важно! Не надо исключать из точек отказа сверхнадежное оборудование, с которым «точно ничего не случится». Когда (именно когда, а не если) ваша сверхнадежная СХД потеряет все данные, продолжите ли вы смеяться в цирке или нет, будет зависеть только от вашей готовности к этой ситуации.

3. Определяем зависимости точек отказа

Сбои в работе некоторых точек отказа могут провоцировать сбои в работе других. К примеру, отказ ИБП приведет к остановке в работе серверов и, как следствие, при восстановлении электроснабжения у вас может не заработать что-то еще. Также и остановка гипервизора может вызвать ошибки в работе виртуальных серверов, размещавшихся на нем. В то же время, отказ клиентского коммутатора не влияет на работу другого оборудования или сервисов, и при его корректной замене все будет работать, как и раньше.

Для пользовательского сервиса «Электронная почта» зависимости точек отказа могут выглядеть так:

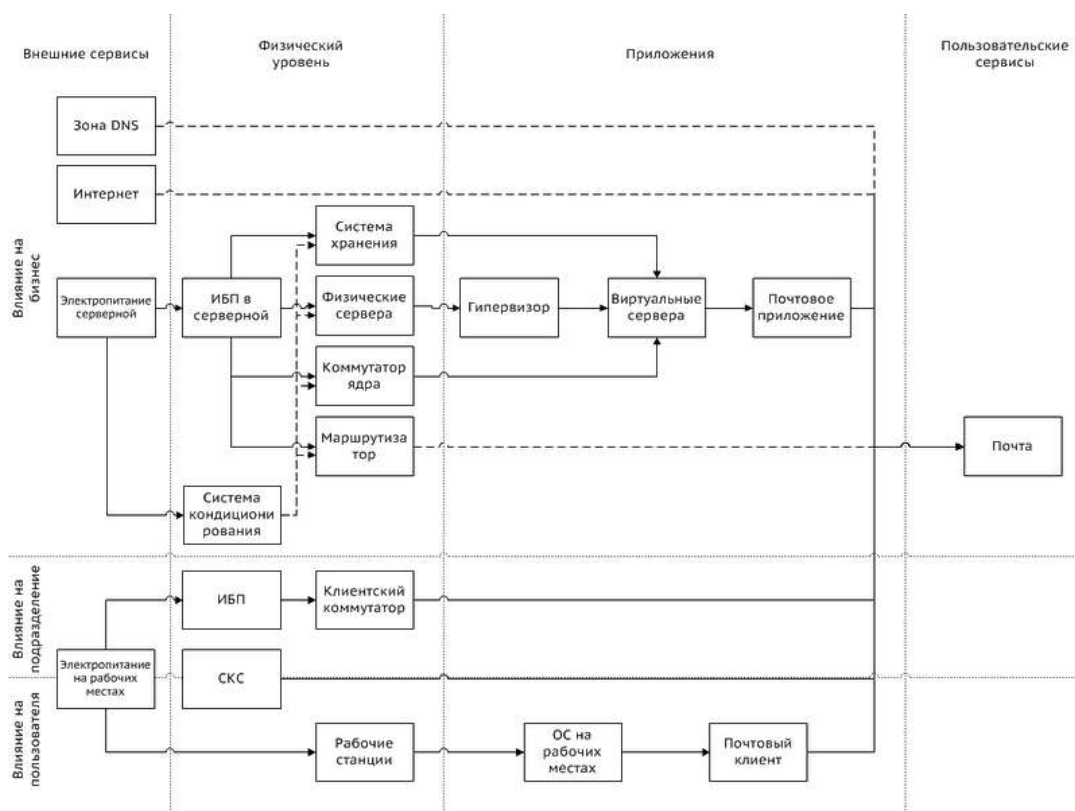


Схема 1. Зависимости точек отказа.

В данную схему необходимо добавить и остальные критичные пользовательские сервисы и соответствующие точки отказа.

Четкое понимание влияния точек отказа друг на друга и на пользовательские сервисы поможет вам при дальнейшем планировании, а именно при составлении процедур локализации точек отказа, определении условий восстановления и факторов риска. Но об этом подробнее в следующей статье.

Практическая работа №23. Отказоустойчивость информационной системы.

Цель работы: усвоить основные понятия отказоустойчивости информационной системы

Задание: рассмотреть примеры отказоустойчивых решений, ориентированных на небольшие организации. Оценить стоимость, преимущества и ограничения.

Практическая работа №24. Организация технической поддержки отказоустойчивости информационной системы.

Цель работы: сформировать навыки и умения по организации тех. поддержки отказоустойчивости системы.

Ход работы.

Все версии Windows, предшествовавшие Windows 2000, имели один общий недостаток – при установке дополнительного программного обеспечения практически любые совместно используемые системные файлы, в том числе *.dll и *.exe, могли быть изменены. Последствия замены этих файлов некорректными или несовместимыми версиями могли быть непредсказуемыми: от снижения производительности операционной системы до некорректного поведения остальных приложений, периодического появления ошибок STOP и даже проблем с загрузкой.

В Windows 2000 впервые за всю историю Windows сделана попытка исправления этой ситуации. Функция защиты системных файлов, работающая по принципу определения цифровых подписей защищенных системных файлов (в их число входят файлы с расширениями .sys, .dll, .ocx, .ttf, .fon и .exe), не позволяет произвольно модифицировать и замещать эти файлы. Данная функция работает в фоновом режиме и защищает все файлы, установленные программой **Windows 2000 Setup**.

Функция защиты системных файлов выявляет все попытки других программ выполнить замену или перемещение защищенных системных файлов, выполняя проверку наличия у файла цифровой подписи, свидетельствующей о том, что версия, предназначенная на замену, совместима с Windows 2000. Если новая версия системного файла не является корректной, то этот файл замещается резервной копией из папки **%SystemRoot%\System32\Dllcache** или с компакт-диска Windows 2000.

Если функция защиты системных файлов не может обнаружить надлежащей версии файла, она предлагает пользователю указать путь к каталогу, из которого такая Версия может быть скопирована, а также регистрирует попытку замещения файла в системном журнале событий.

По умолчанию эта функция всегда активизирована и позволяет выполнять замену системных файлов только в случае установки следующих видов программного обеспечения:

- Сервисные пакеты Windows 2000 (с использованием программы **Update.exe**)
- Дистрибутивные пакеты типа **Hotfix** (с использованием Hotfix.exe)
- Обновление версии операционной системы (с помощью Winnt32.exe)
- Программное обеспечение **Windows Update**

В состав Windows 2000 включено средство проверки системных файлов (**SystemFileChecker**, Sfc.exe), которое представляет собой утилиту командной строки. Эта утилита сканирует все установленные системные файлы и выполняет проверку их версий при перезагрузке компьютера.

Если эта утилита обнаружит, что один из защищаемых системных файлов был замещен, она найдет корректную версию этого файла в каталоге **%SystemRoot%\system32\Dllcache** и запишет ее поверх измененного файла.

Эта утилита командной строки имеет следующий синтаксис:

```
sfc [/scannow] [/scanonce] [/scanboot] [/cancel] [/quiet] [/enable] [/purgecache] [/cachesize=x]
```

Где:

- **/scannow** – параметр, при использовании которого выполняется немедленное сканирование всех защищаемых системных файлов.
- **/scanonce** – параметр, указывающий на необходимость однократного сканирования всех защищаемых системных файлов при следующей загрузке системы.

- **/scanboot** – параметр, задающий опцию сканирования всех защищаемых системных файлов при каждой загрузке системы.
- **/cancel** – параметр, отменяющий все отложенные запросы на сканирование защищаемых системных файлов.
- **/quiet** – параметр, при установке которого замена всех некорректных версии защищаемых файлов будет происходить без вывода предупреждения для пользователя.
- **/enable** – устанавливает стандартный режим работы средства **SystemFileChecker**.
- **/purgecache** – очищает файловый кэш WFP и выполняет немедленное сканирование системных файлов.
- **/cachesize=x** – устанавливает размер файлового кэша WFP (в Мбайт).

Примечание

Чтобы иметь возможность работы с утилитой **sfc.exe**, необходимо зарегистрироваться на компьютере как Администратор или как пользователь, являющийся членом группы Администраторы.

Если содержимое папки %System/?oor%\System32\dlcache окажется поврежденным, воспользуйтесь опциями **sfc /scanonce**, **sfc /scannow** или **sfc /scanboot**, которые позволят восстановить содержимое папки Dllcache.

Как уже говорилось, в некоторых случаях установка нового программного обеспечения приводит к замещению системных файлов некорректными или несовместимыми версиями (которые, естественно, не имеют цифровой подписи). Такая замена, как уже неоднократно упоминалось, как раз и может послужить источником нестабильности системы (в том числе ошибок типа "синий экран" и проблем с загрузкой Windows 2000).

Во избежание таких проблем все системные файлы, устанавливаемые в процессе инсталляции операционной системы Windows 2000, снабжены цифровой подписью Microsoft. Если системный файл имеет подпись, это служит гарантией его совместимости с Windows 2000 и указывает на то, что данный файл либо представляет собой оригинальную версию, разработанную Microsoft, либо прошел тестирование и признан пригодным для использования с Windows 2000.

Верификация цифровой подписи файлов позволяет идентифицировать все установленные на проверяемом компьютере файлы, не имеющие цифровой подписи, и получить об этих файлах следующую информацию:

- Имя файла и точный путь к нему
- Дату модификации файла
- Тип файла и точный номер его версии

Чтобы запустить средство верификации цифровых подписей файлов, нажмите кнопку **Пуск**, из раскрывшегося меню выберите команду **Выполнить** и введите команду **sigverif**.

Максимальную практическую пользу при устранении проблем, связанных с заменой системных файлов некорректными версиями, можно получить, регистрируя информацию, собранную программой **Sigverif**, в файле журнала.

Для этой цели сделайте следующее:

1. Запустите программу Sigverif, и в появившемся на экране окне **Проверка подписи файла** (FileSignatureVerification) нажмите кнопку **Дополнительно** (Advanced).
2. В раскрывшемся диалоговом окне **Дополнительные параметры проверки подписи файла** (AdvancedFileSignatureVerificationSettings) перейдите на вкладку **Ведение журнала** (Logging) (рис. 8.1) и установите флажок **Сохранять результаты проверки подписи в журнале** (Savethefilesignatureverificationresultsto a logfile).
3. Перейдите в группу **Параметры журнала** (Loggingoptions), где имеется возможность установить по выбору следующие опции ведения файла журнала:
 - **Добавлять к существующему журналу** (Appendtoexistinglogfile) – если установить этот переключатель, то результаты новой операции поиска будут добавлены в конец существующего файла журнала.
 - **Заменять существующий журнал** (Overwriteexistinglogfile) – если выбран этот переключатель, то результаты новой операции сканирования заместят существующий файл журнала.
 - В поле **Имя файла журнала** (Logfilename) можно вручную ввести имя файла журнала.
4. Нажмите кнопку **ОК**.

Вы вернетесь в окно **Проверка подписи файла**. Чтобы начать операцию сканирования, нажмите в этом окне кнопку **Начать** (Start). Степень завершенности процесса сканирования будет отражаться индикатором **Просмотр файлов** (Scanningfiles).

Для отмены сканирования нажмите кнопку **Остановить** (Stop). По завершении процесса сканирования на экране появится окно **Результаты проверки подписи** (SignatureVerificationResults) (рис. 8.2), в котором будет отображен список всех обнаруженных файлов, не имеющих цифровой подписи.

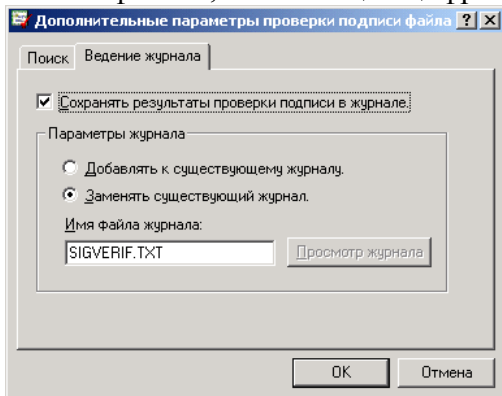


Рис. 8.1. Вкладка Ведение журнала (Logging) окна Дополнительные параметры проверки подписи файла (AdvancedFileSignatureVerificationSettings)

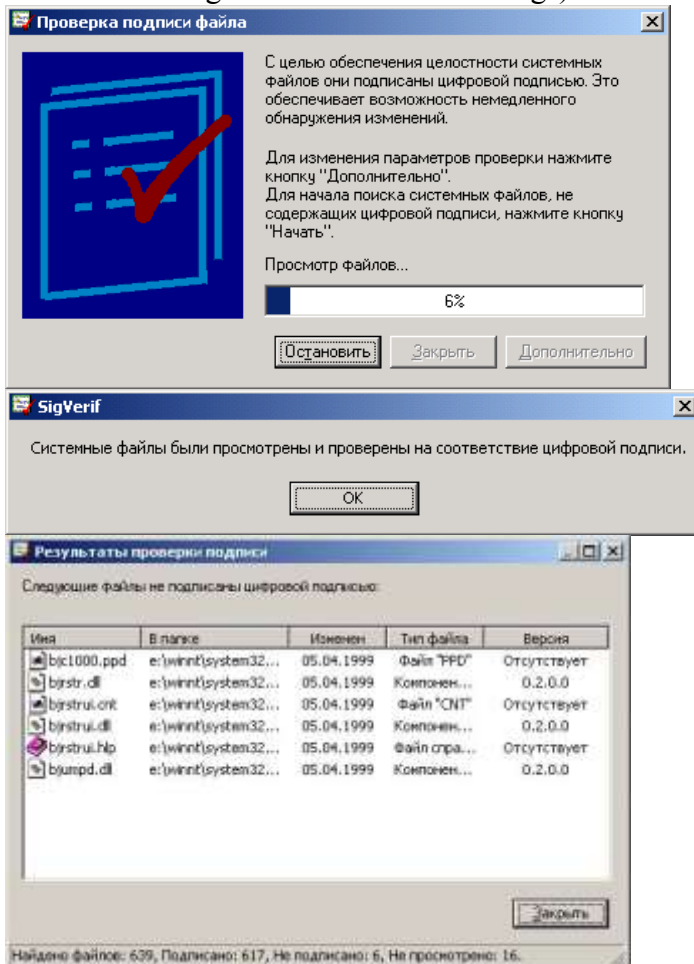


Рис. 8.2. Окно Результаты проверки подписи (SignatureVerificationResults)

Загрузчик Windows 2000 (NTLDR) отображает на экране меню, из которого можно выбрать запускаемую операционную систему (см. главу 2). Если при появлении меню загрузки Windows 2000 нажать клавишу **F8**, то на экране появится меню опций отладки и дополнительных режимов загрузки, которое будет оставаться на экране до тех пор, пока не будет выбрана одна из опций.

При загрузке в безопасном режиме Windows 2000 использует стандартные параметры настройки (монитор VGA, без запуска сетевых средств, с запуском минимального количества драйверов – фактически, запускаются только драйверы, минимально необходимые для запуска Windows). Например, если после инсталляции нового программного обеспечения Windows 2000 перестала запускаться, то вполне возможно, что загрузка в безопасном режиме позволит выполнить

запуск операционной системы с минимальным количеством сервисов и драйверов. После загрузки вы сможете изменить параметры настройки компьютера, не позволяющие выполнить корректную загрузку Windows 2000, или удалить программное обеспечение, вызвавшее эти проблемы.

Если вы имеете некоторый опыт работы с Windows NT 4.0, то наверняка знаете, что в этой системе проблемы с загрузкой чаще всего вызывались некорректно работающими драйверами устройств. Такие несовместимые драйверы могли привести к краху системы либо сразу же после инсталляции, либо даже после некоторого времени, когда их работа на первый взгляд казалась корректной. Причем вторая ситуация, когда драйвер в течение некоторого времени все же работал, не вызывая никаких проблем, всегда была более труднообъяснимой, (а в самом деле, что же могло вызвать ошибку?).

При этом, хотя на первый взгляд и кажется, что нет причин, которые могли бы хоть как-то объяснить это непредсказуемое поведение, причины этому все же есть. Заключаются они в том, что как программная, так и аппаратная конфигурация компьютера со временем могут меняться, а эти изменения могут спровоцировать ошибки, допущенные при проектировании драйвера и оставшиеся незамеченными. Windows 2000, как и Windows NT 4.0, тоже может быть выведена из строя установкой несовместимого драйвера. Однако загрузка в безопасном режиме (**safemode**), концепция которого была позаимствована из Windows 9x, предоставляет более удобные средства быстрого восстановления системы после подобных ошибок, нежели Windows NT 4.0.

Если несовместимый драйвер вызывает проблему при первой же перезагрузке, то вам очень повезло, потому что, как правило, в этом случае вам действительно поможет опция **Загрузка последней удачной конфигурации** (LastKnownGoodConfiguration). Когда пользователь выбирает из меню безопасного режима эту опцию, система при загрузке использует информацию ключа реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet и восстановит всю конфигурационную информацию, сохраненную после того, как компьютер в последний раз был успешно загружен.

В ряде случаев, если использование опции **Загрузка последней удачной конфигурации** не помогло, но вам известен драйвер, вызвавший проблему (список таких драйверов можно получить с помощью утилиты **Sigverif**, описанной ранее в этой главе), то вы можете попробовать другие способы быстрого восстановления. Например, можно попытаться использовать такие опции меню безопасного режима, как **Безопасный режим** (SafeMode), **Безопасный режим с загрузкой сетевых драйверов** (SafeModewithNetworking) или **Безопасный режим с поддержкой командной строки** (SafeModewithCommandPrompt). Как уже говорилось, при использовании этих опций Windows 2000 загружается с минимальным набором драйверов и сервисов.

После загрузки системы вы сможете удалить из системы проблемный драйвер с помощью штатных средств Windows 2000 – **Мастера оборудования** (HardwareWizard) или **Диспетчера устройств** (DeviceManager). (Чтобы вызывать мастер оборудования, выберите из меню Пускопции **Настройка > Панель управления > Установка оборудования** (Settings > ControlPanel > Add/RemoveHardware), а для вызова диспетчера устройств используйте опцию **Пуск > Настройка > Панель управления > Система** (Start > Settings > ControlPanel > System), перейдите на вкладку **Оборудование** и нажмите кнопку **Диспетчер устройств**.)

Если системный и загрузочный раздел отформатированы для использования файловой системы FAT, можно попытаться загрузить компьютер с помощью загрузочной дискеты MS-DOS (или Windows 9x) и вручную удалить или переименовать файл проблемного драйвера.

Если в Windows NT 4.0 изготовление диска аварийного восстановления (**EmergencyRepairDisk**, ERD) выполнялось при помощи утилиты Rdisk.exe, отлично известной всем опытным пользователям и специалистам из групп технической поддержки, то в Windows 2000 эти функции были перенесены в программу архивации.

Чтобы изготовить ERD для Windows 2000, сделайте следующее:

1. Приготовьте свободную дискету емкостью 1.44 Мбайт.
2. Запустите программу архивации. В окне программы выберите из меню **Сервис** (Tools) команду **Создание диска аварийного восстановления** (CreateanEmergencyRepairDisk).
3. На экране появится окно **Диск аварийного восстановления**, в котором настоятельно рекомендуется установить флажок **Архивировать реестр в папку восстановления** (Alsobackuptheregistrytotherepairdirectory), поскольку, как было убедительно показано в главе 2, реестр является одним из жизненно важных компонентов системы, и его повреждение может привести к сбою уже на самых ранних этапах загрузки.

Примечание

Резервное копирование реестра будет произведено в папку **%SystemRoot% \repair**. Процедура аварийного восстановления использует информацию из этой папки, поэтому никогда не следует ни удалять, ни модифицировать ее содержимое.

4. Нажмите кнопку **ОК**, и программа архивации создаст диск аварийного восстановления.

Не забывайте выполнять эту процедуру каждый раз перед внесением серьезных изменений в системную конфигурацию.

Функции аварийного восстановления Windows 2000 предназначены для восстановления поврежденной системы в тех случаях, когда возникают проблемы, вызванные повреждением реестра, системных файлов, загрузочного сектора раздела и среды запуска.

Важным отличием от процесса аварийного восстановления в Windows NT 4.0 является возможность выполнить попытку восстановления системы даже без диска аварийного восстановления (если он не был изготовлен заблаговременно). Однако в случае выполнения процедуры аварийного восстановления без ERD, все изменения, внесенные в состав системы, будут потеряны, а установленное в системе дополнительное программное обеспечение может потребовать переустановки.

Запуск процесса аварийного восстановления с помощью ERD аналогичен запуску процедуры восстановления с помощью консоли восстановления: нужно загрузить компьютер с компакт-диска или с дискеты и выбрать опцию исправления системы, нажав клавишу **R**. После этого вам будет предложено выбрать опцию быстрого (автоматического) или ручного восстановления. Быстрое восстановление очень просто и не требует от пользователя никакого дальнейшего вмешательства.

При ручном восстановлении можно выбирать необязательные проверки компонентов системы, к числу которых относятся системные файлы, загрузочный сектор раздела и среда загрузки (**startupenvironment**, если вы имеете мультизагрузочную систему).

Если процесс аварийного восстановления системы завершится успешно, то компьютер будет автоматически перезагружен, и после перезагрузки вы получите работающую систему.

Примечание

Опция ручного восстановления (**M**) при использовании ERD предназначена для устранения проблем с системными файлами, загрузочным сектором раздела и средой загрузки, но не устраняет проблем с реестром. Для устранения проблем с реестром пользуйтесь консолью восстановления (и не забывайте иметь качественную резервную копию реестра). Опция быстрого восстановления использует резервную копию реестра, созданную при запуске программы **Setup**.

Если восстановление с помощью ERD не помогло решить возникших проблем, воспользуйтесь опциями консоли восстановления. Если не поможет и это, то, вероятнее всего, вам придется переустанавливать систему.

Практическая работа №25. Диагностика и восстановление информационных систем.

Цель работы: сформировать навыки по выполнению диагностики и восстановления системы, сформировать умения по выполнению восстановления системы через создание точки восстановления.

Оборудование, технические и программные средства: персональный компьютер, операционная система Windows XP.

Точка восстановления Windows XP

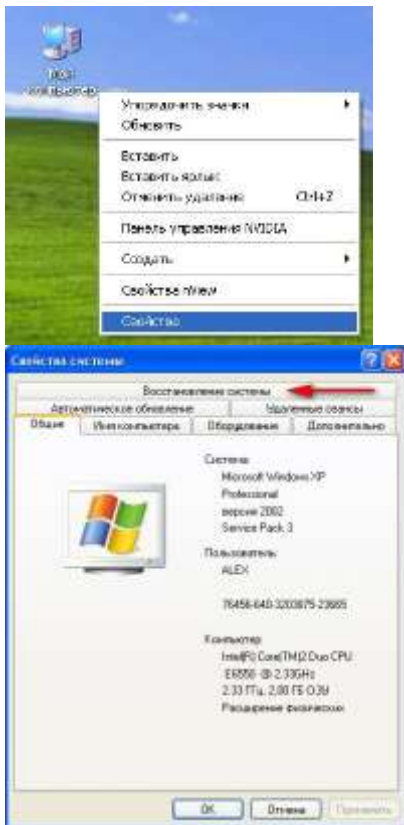
Написать статью про то как работает простое восстановление системы Windows XP и какие могут быть при этом интересные моменты, неизвестные начинающим и не только, меня просил уже давно наш постоянный читатель. Статей про то как восстановить Windows XP в самых безнадежных случаях и разными малоизвестными методами у нас много, например Восстановление загрузчика Windows XP, а вот статьи о том как создается простая *точка восстановления Windows XP* и как с помощью неё откатиться назад нет, а значит исправляемся.

Давайте рассмотрим применение **точки восстановления XP** на конкретном примере. Допустим вы установили какую-нибудь программу или пакет драйверов, а потом выяснили, что ваша операционная система работает не стабильно, удалив всё, что устанавливали, вы вопрос

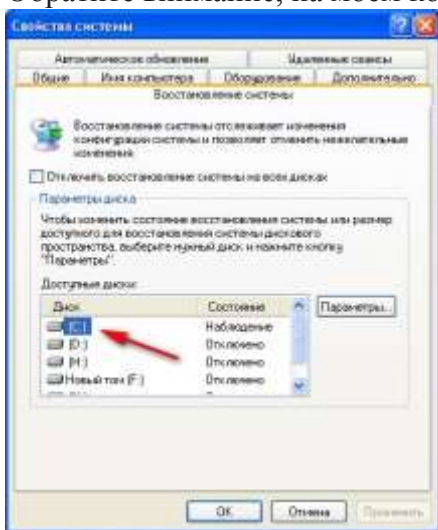
скорее всего не решите, вот здесь и пригодится наша с вами точка восстановления. Прежде чем её создать, давайте убедимся в том, что восстановление системы включено на нашем компьютере.

Щёлкаем правой кнопкой мыши на значке **Мой компьютер** и в выпадающем меню

выбираем **Свойства->Восстановление системы**.



Обратите внимание, на моём компьютере включено наблюдение за диском (C:),



это значит что у меня включено Восстановление системы для данного диска и создаются так называемые точки восстановления или снимки системы, а многие их ещё называют слепки операционной системы, то есть всё, что делается на вашем компьютере запоминается. Важно когда запоминается?

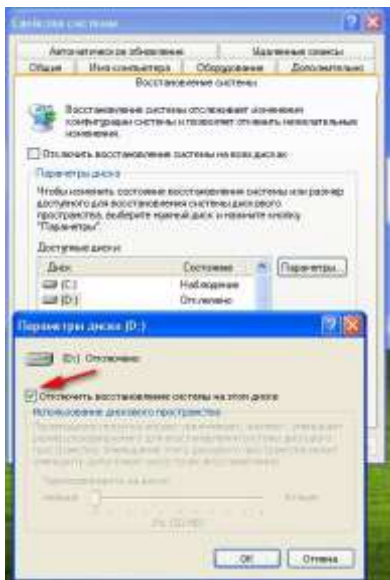
1. Точка восстановления XP создаётся автоматически каждые 24 часа.
2. Перед установкой многих программ и драйверов без цифровой подписи.
3. А так же вы сами, перед каким-нибудь серьёзным действием, можете создать точку восстановления.

Итак Восстановление системы у нас включено для диска (C:), по умолчанию Windows XP резервирует для точек восстановления 12% дискового пространства. В окне Параметры вы можете увеличить с помощью ползунка место на жёстком диске для хранения точек восстановления, тогда даже старые снимки системы у вас будут храниться долго и вы в любой момент сможете к ним откатиться.



Ещё нужно знать, что восстановление системы затрагивает в основном только важные системные файлы, но не ваши данные, не удастся к примеру вернуть случайно удалённый файл с помощью применения точки восстановления.

Если у вас есть желание, вы можете включить наблюдение за любым другим диском системы. Нажмите на нужном томе мышкой, далее кнопка Параметры и снимите галочку с пункта Отключите восстановление системы.

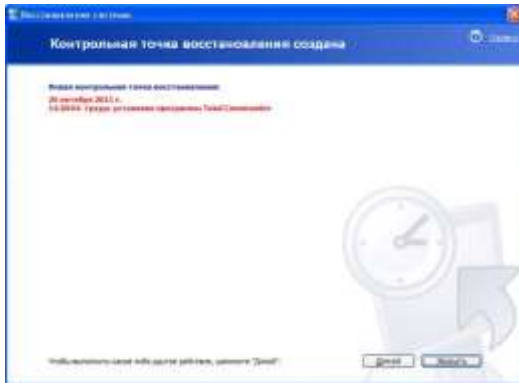
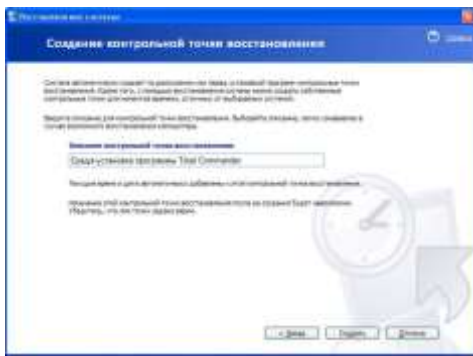


Теперь давайте представим, что мы устанавливаем незнакомую программу на компьютер. Естественно перед установкой мы создадим точку восстановления Пуск->Все программы->Стандартные Службные->Восстановление системы. В данном диалоговом окне вы можете восстановить более раннее состояние компьютера, создать новую точку восстановления или отменить последнее восстановление.

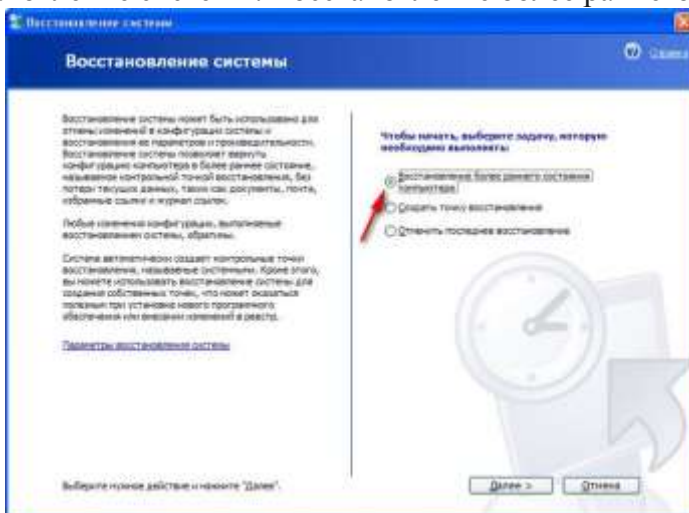
Создать точку восстановления Windows XP и далее



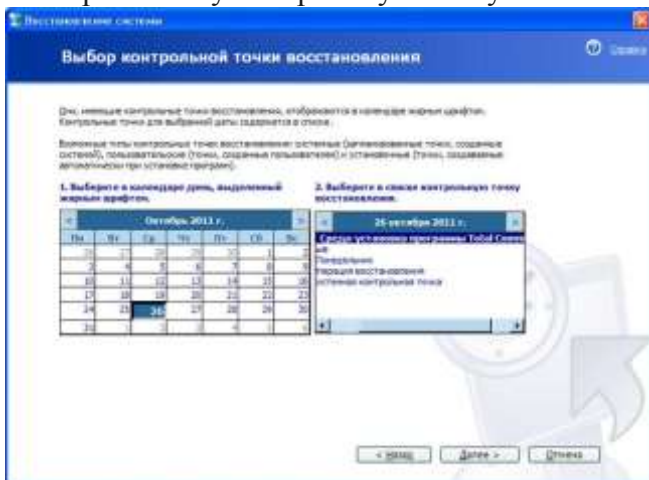
Описание точки восстановления должно содержать информацию, почему именно создана данная точка, сегодня среда, ну и назовём к примеру назовём к примеру Среда-установка программы Total Commander, далее Создать и можем смело устанавливать нашу программу.



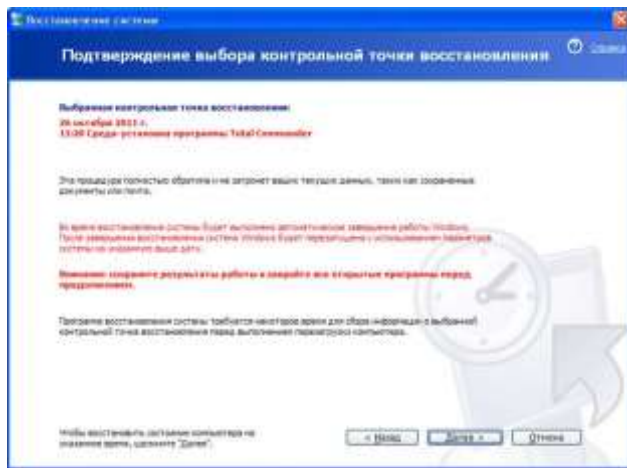
Теперь представим ситуацию, что после установки нашей программы, компьютер стал вести себя не стабильно и мы решили откатиться с помощью созданной нами точки восстановления назад. Запускаем восстановление системы. Пуск->Все программы->Стандартные->Служебные->Восстановление системы. Восстановление более раннего состояния компьютера.



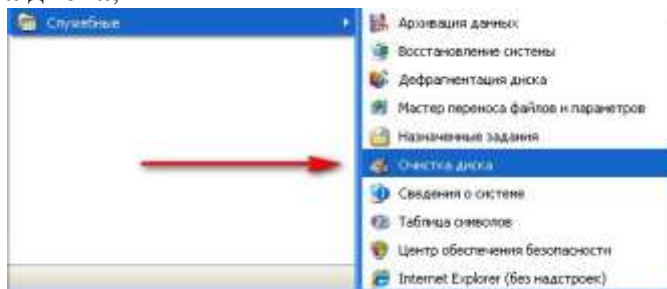
Выбираем нашу контрольную точку восстановления.



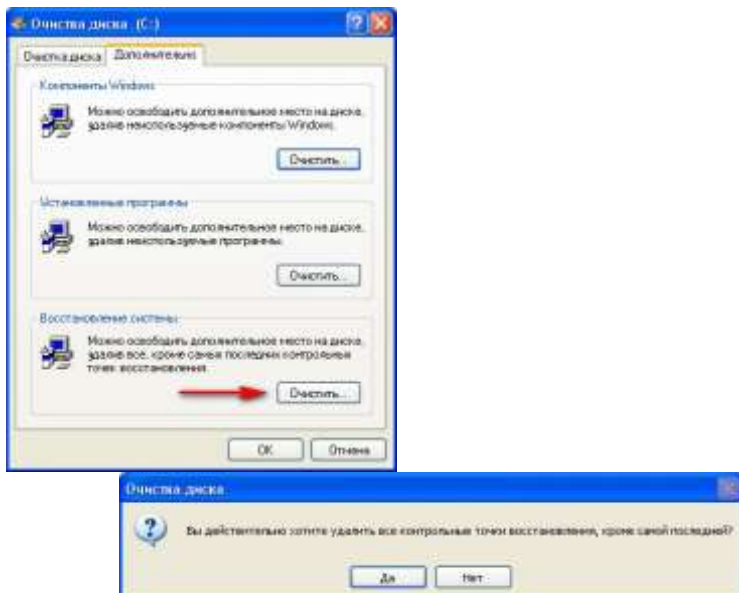
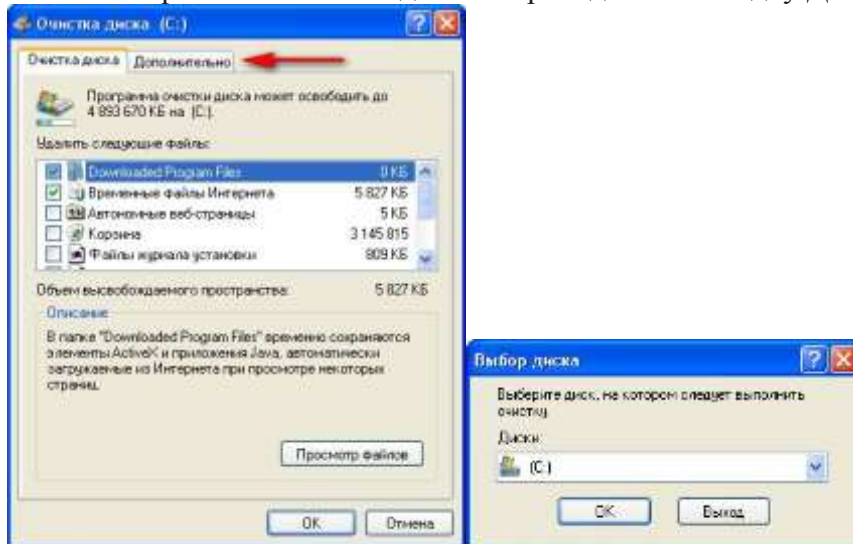
Процедура обратима и не затронет наших текущих данных. Далее и начнётся процесс восстановления с перезагрузкой компьютера, затем вы сможете убедиться, что ни каких следов программы, из-за которой компьютер вёл себя нестабильно у вас как не бывало.



Если вы захотите удалить все точки восстановления, кроме последней, для экономии места на винчестере, это можно проделать так: Пуск->Программы->Службные->**Очистка диска**,



затем выбираете системный диск и переходим на вкладку Дополнительно,

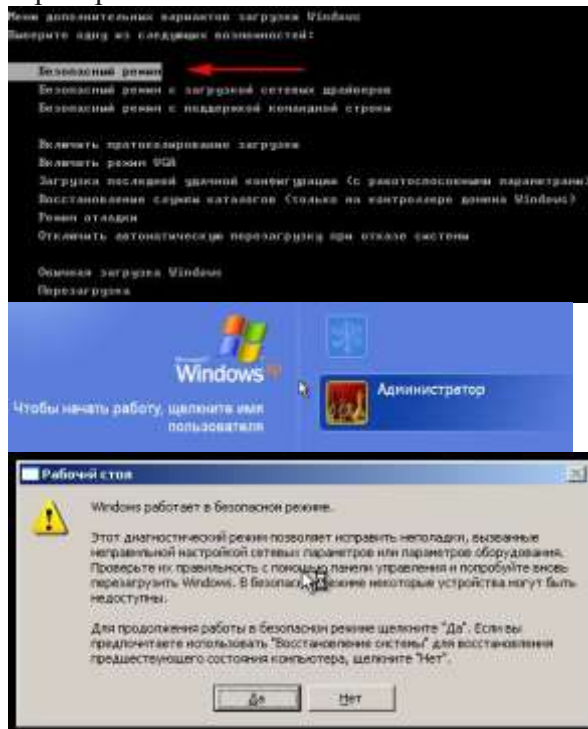


выбираем **Восстановление системы**, нажимаем и удалятся все точки, кроме последней.

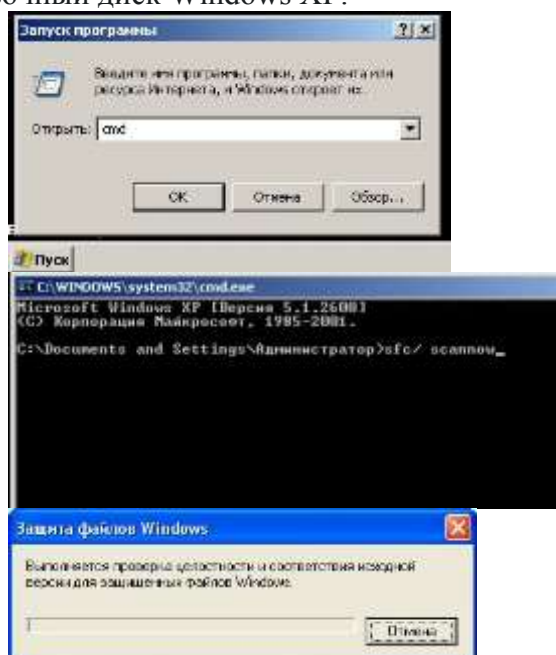
В следующей статье мы с вами рассмотрим случай, когда из-за серьёзной неполадки, нам с вами совсем не удастся загрузить операционную систему Windows XP и нам придётся восстанавливать систему с помощью точки восстановления в **Безопасном режиме**, а так же Безопасном режиме с поддержкой командной строки.

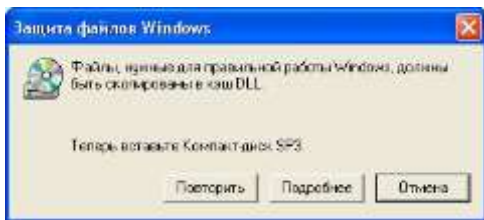
Загрузка в безопасном режиме XP

Прежде чем запускать Windows XP в Безопасном режиме стоит также попробовать Загрузку последней удачной конфигурации с работоспособными параметрами, ещё у нас на сайте есть много статей, которые смогут вам помочь, например: [Не загружается Windows XP](#), [Точка восстановления XP](#), [Восстановление системы через меню установки Windows XP](#). Что бы осуществить **загрузку в безопасном режиме XP**, при запуске компьютера нужно нажать несколько раз клавишу **F-8** и вы зайдёте в меню дополнительных вариантов загрузки Windows XP. Входить нужно от лица Администратора.

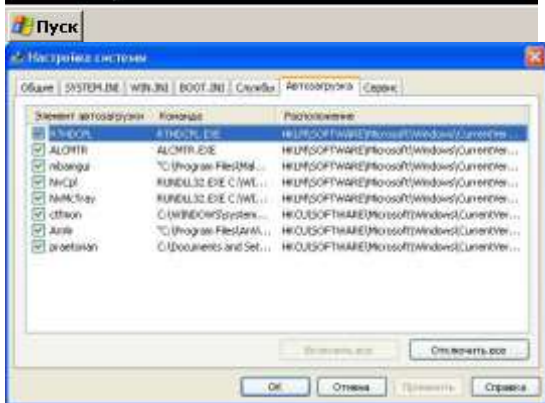
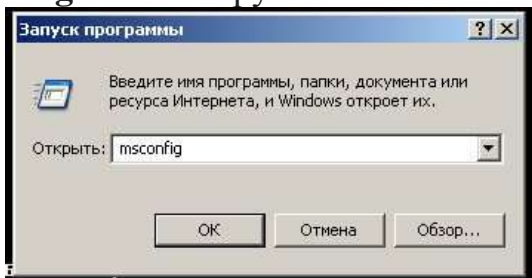


В безопасном режиме Windows XP, можно попытаться удалить через меню **Удаление и установка программ**, программное обеспечение, которое вы устанавливали последним или пакеты драйверов мешающие по вашему мнению нормальной загрузке Windows XP. Лично я бы ещё выполнил проверку целостности системных файлов операционной системы, Пуск->Выполнить->cmd далее введите команду **sfc /scannow**, в большинстве подобных случаях вам понадобится установочный диск Windows XP.



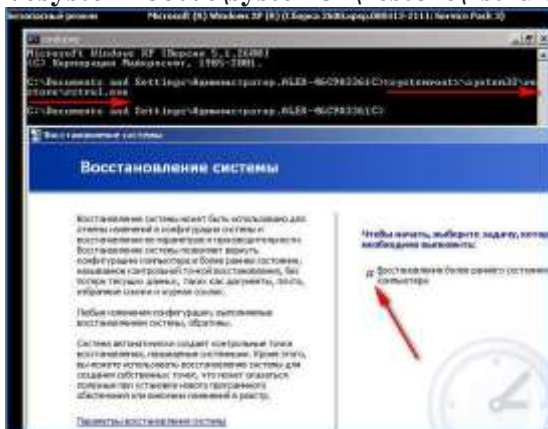


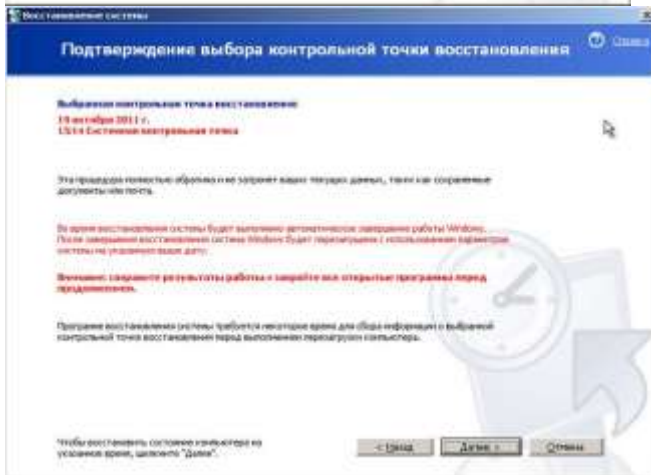
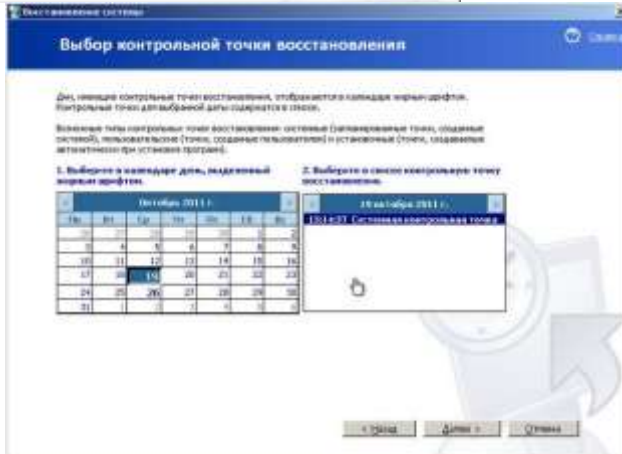
Так же нужно убрать все программы из автозагрузки Пуск->Выполнить->**mscconfig**->Автозагрузка.



При использовании не просто безопасного режима, с загрузкой сетевых драйверов, вместе с основными драйверами Windows XP загрузятся драйвера на вашу сетевую карту и вы сможете выходить в интернет. Если после предпринятых действий загрузить Windows XP в нормальном режиме не удастся, вам нужно опять **загрузиться в безопасный режим XP** и запустить **Восстановление системы**, то есть попытаться откатится назад с помощью точки восстановления. Так же вам нужно знать, что в безопасном режиме не получится создать точку восстановления, можно лишь использовать восстановление к более ранним настройкам компьютера. Пуск->Все программы->Стандартные Службные->Восстановление системы. Выбираем нужную точку и восстановления и восстанавливаемся.

Ну и напоследок, если в безопасный режим вам зайти не удастся, можете попытаться зайти в безопасный режим с поддержкой командной строки. Наберите explorer и попадёте в почти нормальный рабочий стол или можете вызвать средство Восстановления системы командой **%systemroot%\system32\restore\rstrui.exe**.





Внеаудиторная работа:

1. Составить отчет по проделанной работе.
2. Написать выводы.

Практическая работа № 26. Защита информации и управление доступом в базе данных.

Цель работы: сформировать навыки защиты информации и управление доступом в базе данных, сформировать умения по настраиванию защиты базы данных при помощи паролей и шифров.

Оборудование, технические и программные средства: персональный компьютер, СУБД Access.

Теоретическое обоснование

В процессе администрирования баз данных (БД) существенное внимание должно уделяться их защите. Основными методами защиты БД являются парольная защита, защита на уровне пользователя и шифрование.

В данной лабораторной работе рассмотрим подробно процесс администрирования и защиты баз данных с помощью паролей.

Парольная защита является наиболее простым и распространенным способом защиты данных и администрирования БД. В этом случае этот пароль называют *паролем базы данных*.

При условии знания пароля к базе данных каждый из пользователей может её открыть, а также выполнять все необходимые операции с ней.

Однако использование методов парольной защиты совместно с защитой на уровне пользователей недопустимо. Это возможно только в том случае, если доступ по паролю к БД получает её администратор.

При односвременной установке на БД пароля и защиты на уровне пользователей последнему предоставляется возможность выполнять только те операции над БД, которые предусматриваются его полномочиями.

Парольная защита БД не может быть использована в том случае, если в дальнейшем предполагается создание копий (или репликаций) БД. В частности, СУБД Access не поддерживает такой возможности.

Метод парольной защиты при администрировании БД является достаточно надежным, так как многие СУБД шифруют пароль, а для открытия и работы с базой данных необходим прямой доступ. Сам пароль к базе хранится в специальном файле, а поэтому открыть БД невозможно даже на другом компьютере с установленной системой.

Защита баз данных на уровне пользователя применяется в том случае, если с одной и той же базой данных работают одновременно несколько групп пользователей или несколько пользователей, имеющих к ней доступ.

Для организации защиты данных в базе на уровне пользователя создаются рабочие группы, причем каждая из них определяет единую технологию работы с базой данных для совокупности пользователей.

Вся информация о каждой из рабочих групп сохраняется в соответствующем **файле рабочих групп (РГ)**. В нем содержится информация об отдельных пользователях и их группах, учетные записи отдельных пользователей и групп пользователей. Для каждой из учетных записей в СУБД сохраняются права доступа к объектам базы данных. По умолчанию СУБД создается две группы пользователей: администраторы (имя группы Admins), пользователи (Users)

При организации администрирования баз данных с помощью их защиты на уровне пользователя необходимо каждому из них присвоить уникальный пароль. Однако не следует путать этот пароль с тем паролем, который был установлен на всю базу данных в целом. Он называется **паролем учетной записи** и сохраняется в учетной записи файла рабочей группы.

При создании рабочих групп для использования БД и дальнейшей регистрации посетителей и ее пользователей следует учитывать следующие моменты.

1. Группы Admins и Users не могут быть удалены, так как создаются системой по умолчанию.

2. Группа Admins не может быть пустой, в ней должен храниться хотя бы один пользователь.

3. Все пользователи, получающие права доступа к базе данных, автоматически становятся членами группы Users. Произвести удаление пользователей базы данных из группы Users нельзя.

4. Удаление пользователей базы данных из группы Admins невозможно.

5. Иерархия групп пользователей баз данных недопустима, то есть нельзя размещать создаваемые рабочие группы в ранее созданных.

6. В системе защиты баз данных могут быть пустые группы, однако не может быть пользователей, не входящих не в одну из групп. По умолчанию они заносятся в группу Users.

Установка защиты базы данных на уровне пользователя сложнее парольной защиты, так как она предполагает создание файлов рабочих групп, учетных записей пользователей, добавление пользователя в группу. При использовании защиты базы данных на уровне пользователя в СУБД Access предполагается активизация подключения к СУБД и защита каждой отдельно взятой базы данных при помощи *мастера защиты*.

При совместном использовании баз данных несколькими пользователями созданных по умолчанию рабочих групп очень часто оказывается недостаточно. Поэтому перед созданием новых рабочих групп пользователей вначале необходимо зарегистрировать сами группы, а только потом создавать учетные записи пользователей, принадлежащих этим группам. Средства шифрования баз данных позволяют закодировать их таким образом, что она окажется недоступной для чтения другими СУБД, которые поддерживают формат исходной СУБД.

При использовании механизма шифрования баз данных, разработанных с помощью средств СУБД Access, следует отметить, что она вначале должна быть защищена паролем, так как в противном случае операцию дешифрации может выполнить любой пользователь на том персональном компьютере, на котором установлен Access.

Шифрование баз данных в Access как метод администрирования применяется для того, чтобы изменить до неузнаваемости стандартный формат базы данных, при этом ненужно дополнительно задавать ключ для шифрования.

Методика и порядок выполнения задания 1

При выполнении задания 1 студенты должны использовать практические навыки проектирования баз данных, полученные при изучении дисциплин «Базы данных», «Предметно-ориентированные экономические информационные системы».

Задание 1. Для заданной предметной области сформируйте Базу данных. Предметную область выберите либо из списка предлагаемого преподавателем, либо предложите самостоятельно.

Список предметных областей для выполнения задания 1

Задание 1.

1. Гостиница.
2. ГАИ (ГИБДД).
3. Спортивные соревнования.
4. Паспортный стол.
5. Трудоустройство.
6. Поставка и реализация программного обеспечения на CD – дисках.
7. Поликлиника.
8. Отдел кадров.
9. Учет материальных ценностей.
10. Фонотека.
11. Обзор компаний мобильной связи.
12. Videотека.
13. Станция технического обслуживания автомобилей.
14. Аптечный склад.
15. Поставка и реализация продуктов питания.
16. Поставка и реализация бытовой техники.
17. Грузоперевозки.
18. Санкции ГИБДД (ГАИ).
19. Автовокзал.
20. Операции с недвижимостью.
21. Налогообложение малых предприятий.
22. Поставка и реализация компьютерной техники.
23. Аэропорт.
24. Железнодорожный вокзал.
25. Банковские операции.
26. Рынок Internet – провайдеров.
27. Жилищно-коммунальное хозяйство.
28. Договор.
29. Учет сетевого и компьютерного оборудования.
30. Страховая компания.
31. Библиотека.
32. Поставка и реализация легковых автомобилей российских производителей.
33. Поставка и реализация сельскохозяйственной продукции.
34. Поставка и реализация легковых автомобилей зарубежных производителей.
35. Больница.
36. Автозаправочная станция.
37. Отпуск изделий.
38. Учет бегущих строк на телевидении.
39. Энциклопедия "Формулы – 1".

Задания 2.

1. Закройте базу данных, для которой следует установить парольную защиту. В том случае, если она является сетевой, то необходимо закрыть её на всех рабочих станциях.

2. Перейдите в главное меню СУБД Access, нажав клавишу **F10**, или выполнив щелчок правой кнопкой мыши на любом его пункте.

3. Затем в опции **File (файл)** активизируйте команду **Open (открыть)** и нажмите клавишу Enter.

4. В диалоговом окне **Open databases (открытие базы данных)** установите флажок в поле **Монопольно (Exclusive)**, что позволяет открыть базу данных в режиме монопольного доступа.

5. Для установки парольной защиты базы данных перейдите в опцию меню **Сервис (Tools)**, в которой затем выберите команду **Защита (Security)**.

6. В появившемся контекстном меню активизируйте команду **Задать пароль базы данных (SetDatabasePassword)**.

7. В поле **Password (пароль)** диалогового окна **Задать пароль базы данных (SetDatabasePassword)** введите кодовое слово, учитывая регистр и раскладку клавиатуры.

8. Для записи, введенного пароля в специальный файл, необходимо выполнить операцию его подтверждения. Для этого перейдите в поле **Verify (подтверждение)** окна **Задать пароль базы данных (SetDatabasePassword)** и вновь введите пароль, а затем нажмите кнопку ОК.

Для созданной в задании №1 базы данных, задайте парольную защиту.

Задание 3.

1. Откройте сформированную ранее БД в режиме монопольного доступа.

2. Перейдите в главное меню СУБД Access в опцию **Сервис**, а затем выполните следующие команды: **Защита → Удалить пароль базы данных: F10 → Tools → Security → UnsetDatabase Password**. Следует заметить, что команда удаления пароля будет доступна только в том случае, если он был установлен ранее.

3. После нажатия на клавишу Enter на экран будет выведено диалоговое окно **Удалить пароль базы данных**.

4. В нем перейдите в поле **Пароль (Password)** и введите заданный пароль базы данных.

5. Нажмите кнопку ОК, при этом база данных будет открыта, но уже при последующей загрузке система уже не будет запрашивать пароль.

Удалите парольную защиту базы данных, спроектированной в задании 1.

Методика и порядок выполнения задания 2

Задание 1.

1. Загрузите созданную Вами базу данных.

2. Войдите в главное меню Access и перейдите в опцию **Сервис (Tools)**, в которой затем активизируйте команду **Защита (Security)**.

3. В появившемся контекстном подменю выберите команду **Пользователи и группы (User and Group Accounts)** и нажмите кнопку ОК.

4. В диалоговом окне **Пользователи и группы (User and Group Accounts)** активной является вкладка **Пользователи**. По умолчанию в ней установлен пользователь **Admin**.

5. Для установки защиты базы данных на уровне пользователя перейдите на вкладку **Изменение пароля**. В ней следует пустым оставить поле **Текущий пароль (Old Password)**, а в поле **Новый пароль (New Password)** ввести пароль.

6. Для подтверждения заданного пароля его необходимо ввести в поле **Verify (подтверждение)**.

Для спроектированной в задании 1 в разделе **Методика и порядок выполнения задания 1** базы данных, установите защиту на уровне пользователя. При этом предусмотрите, что для рабочих групп **Admins** и **Users** пароли для входа в базу данных будут различными.

Задание 2.

1. Загрузите СУБД Access.

2. Откройте спроектированную Вами базу данных.

3. Выполните следующую последовательность действий для создания рабочей группы: 1) **F10 → Tools → Security → User and Group Accounts (F10 → Сервис → Защита → Пользователи и рабочие группы)**; 2) в диалоговом окне **Пользователи и группы** перейдите на вкладку **Группы**; 3) в этой вкладке в поле «Имя» введите название группы; 4) затем вернитесь во вкладку **Пользователи** и введите в поле «Имя» имя пользователя, принадлежащего этой группе.

4. Пароль для доступа к базе данных для пользователя новой группы создается, используя с помощью алгоритма приведенного в задании 1.

Создайте для работы с разработанной базой данных еще одну или несколько рабочих групп. В каждой из групп предусмотрите не менее трех пользователей.

Задание 3.

1. Запустите СУБД Access и откройте спроектированную базу данных.

2. Войдите в главное меню Access, нажав F10.

3. В главном меню СУБД выберите опцию **Сервис (Tools)**, в которой затем последовательно выполните команды **Защита → Разрешения (Security → UserAndGroupPermission)**.

4. После нажатия на кнопку ОК на экран будет выведено диалоговое окно **Разрешения (UserAndGroupPermission)**, которое содержит две вкладки **Разрешения (UserAndGroupPermission)** и **Смена Владельца (ChangeOwner)**.

5. Для определения прав пользователей базы данных и рабочих групп следует выполнить следующие действия:

1) в поле **Пользователи и группы** выберите имя пользователя или наименование рабочей группы;

2) в поле **Имя объекта** укажите к какому из объектов получает доступ пользователь;

3) установите переключатель в положение «**пользователи**» или «**группы**»;

4) в ниспадающем меню «**Тип объекта**» выберите элемент базы данных, для которого следует установить разрешения;

5) в области разрешения установите флажки те позиции, отвечающие за выполнение тех операций с базой данных, которые доступны отдельному пользователю или рабочей группе.

6. Для завершения установки разрешений к объектам базы данных нажмите кнопку **Apply (Применить)**.

Для каждого из пользователей и каждой из рабочих групп, спроектированной базы данных. Установите прав доступа к ней и разрешения на ее использования.

Задание 4.

1. Запустите СУБД Access

2. Подключитесь к базе данных в режиме администратора, то есть члена группы Admins.

3. Откройте её.

4. Предоставьте членам группы Users полные прав доступа к базе данных.

5. Выйдите из системы Access.

Отмените защиту базы данных на уровне пользователя, для спроектированной Вами в задании 1 лабораторной работы №1 базы данных.

Задание 5.

1. Запустите СУБД Access.

2. Закройте базу данных, которую необходимо зашифровать. Если она доступна группе пользователей, то она должна быть закрыта одновременно на всех машинах.

3. Войдите в главное меню (F10) и выполните последовательность действий: **F10 → Tools → Security → EncryptDatabase (F10 → Сервис → Защита → Шифрование базы данных)**.

4. После нажатия на ОК на экран будет выведено диалоговое окно **Шифровать базу данных (EncryptDatabase)**, в котором выберите имя базы данных, которую следует зашифровать и нажмите ОК.

5. Укажите путь доступа к зашифрованной базе данных и её новое имя.

Зашифруйте базу данных, спроектированную Вами в задании 1 лабораторной работы №1.

Задание 6.

1. Загрузите СУБД Access.

2. Завершите работу с зашифрованной базой данных, так как в противном случае операцию дешифрации выполнить нельзя.

3. Вызовите диалоговое окно **Дешифрация базы данных (DecryptDatabase)**, выполнив последовательность действий: **F10 → Tools → Security → DecryptDatabase (F10 → Сервис → Защита → Дешифровать базу данных)**.

4. В появившемся на экране диалоговом окне выберите имя базы данных, которую следует дешифровать, и нажмите ОК.

5. Затем укажите имя дешифрованной базы данных и полный путь доступа к ней.

Выполните операцию дешифрации базы данных.

Отчет по лабораторной работе должен состоять из:

- 1) названия лабораторной работы;
- 2) цели лабораторной работы;
- 3) ответов на контрольные вопросы;
- 4) формулировки заданий и порядка их выполнения.

Отчет о выполнении лабораторной работы в письменном виде сдается преподавателю.

Контрольные вопросы:

1. Охарактеризуйте защиту базы данных на уровне пользователя как один из способов администрирования баз данных.
2. Каким образом устанавливается защита на уровне пользователя в СУБД Access.
3. Создание пользователей в Access.
4. Создание рабочих групп в Access.
5. Предоставление прав доступа к базе данных и разрешений на ее использование.
6. Снятие защиты на уровне пользователя в Access.
7. Шифрование баз данных как метод администрирования баз данных.
8. Последовательность действий при шифровании баз данных.
9. Алгоритм дешифрования баз данных.

Практическая работа № 27. Проектирование стратегий резервного копирования баз данных.

Цель работы: сформировать проектирования стратегий резервного копирования, сформировать умения по проведению резервного копирования.

Оборудование, технические и программные средства: персональный компьютер, СУБД Access.

Теоретическое обоснование

Администрирование баз данных методом репликации позволяет создавать так называемые специальные «горячие» копии баз данных средствами СУБД Access.

Репликацией будем называть процесс создания специальных копий (реплик) базы данных, спроектированных средствами СУБД Access, с которыми могут одновременно работать пользователи сразу на нескольких компьютерах. Отличие репликации от обычного резервного копирования баз данных заключается в том, что для каждой из создаваемых реплик возможна синхронизация с остальными.

В том случае, если для хранения реплик баз данных используется системная папка **«Портфель»**, то такую репликацию баз данных называют *портфельной репликацией*.

Для каждой из баз данных можно создать группу реплик, называемую набором. В этот набор обычно входят *основная* и *дополнительная* реплики. Основная реплика отличается от обычной дополнительной реплики тем, что при работе с ней каждый из пользователей базы данных может изменять ее структуру.

Однако при работе с базой данных основную реплику можно считать обычной, а дополнительную – основной, но следует заметить, что в каждом наборе реплик только одна может являться основной, а все остальные – дополнительными. Дополнительные реплики могут создаваться как из основной, так и из дополнительных реплик.

Создание основной реплики заключается в преобразовании файла исходной базы данных в новый файл. В этом случае исходную базу данных будем называть *реплицируемой*. Если же основной реплике присвоить то же имя, что и у исходной базы данных, то произойдет замена исходного файла БД на его репликацию.

Для безопасности и сохранности данных, внесенных в базу, целесообразно вначале сделать ее резервную копию. Если это не сделано до начала операции репликации, то это возможно в процессе ее выполнения.

В процессе репликации в файл исходной базы данных добавляются специальные таблицы, поля и свойства. После выполнения операции репликации исходная база данных становится основной репликой в наборе. Основная и дополнительные реплики могут содержать

реплицируемые и не реплицируемые (локальные) объекты. Для пользователя работающего с полученной базой данных основная реплика ничем не будет отличаться от файла исходной БД.

Репликация базы данных позволяет обмениваться изменениями отдельных ее копий и может применяться для решения следующих задач:

- 1) распространение приложений;
- 2) доступ к данным;
- 3) резервное копирование;
- 4) перераспределение нагрузки и распараллеливание работы пользователей.

Репликацию базы данных, спроектированной средствами СУБД Access можно выполнить одним из следующих способов:

1) выполнив последовательность действий: **F10 → Сервис → Репликация (F10 → Tools → Replication)**;

2) используя стандартную программу Windows **Проводник**;

3) с помощью Диспетчера Репликации пакета Microsoft Office для разработчиков;

4) используя программируемые объекты доступа к данным DAO.

Синхронизацией называется процесс, при котором происходит обновление двух компонентов в наборе реплик. На этапе синхронизации происходит обмен обновленными записями и объектами для каждого из компонентов. В СУБД Access одной командой может быть выполнена синхронизация двух реплик из одного набора, при этом можно синхронизировать только две дополнительные реплики.

Для защиты реплицируемой базы данных рекомендуется использовать ее защиту на уровне пользователя, которая позволяет определить права пользователя на все объекты, входящие в нее. Эти права не мешают синхронизации базы данных. Базу данных, защищенную паролем реплицировать нельзя.

[Методика и порядок выполнения работы](#)

[Методика и порядок выполнения задания 1](#)

1. Загрузите СУБД Access и выберите ту базу данных, для которой вы хотите создать реплики

2. Для выполнения процесса репликации выполните последовательность действий: **F10 → Сервис → Репликация → Создать реплику → Ввод (F10 → Tools → Replication → CreateReplica → Enter)**.

3. После этого на экран будет выведено диалоговое окно, содержащее предупреждение о закрытии исходной базы данных.

4. В следующем диалоговом окне, содержащем предупреждение, нажмите кнопку «ДА», что позволит системе создать резервную копию исходной базы данных. Если же копия была создана пользователем ранее, то следует нажать кнопку «НЕТ».

5. После создания резервной копии базы данных на экран будет выведено диалоговое окно «Размещение реплики». В этом окне в поле «Имя» укажите название реплики для исходной базы данных. Если имена исходной базы данных и реплики будут совпадать, то произойдет замещение исходной БД ее реплицируемой копией.

6. Для завершения операции репликации нажмите кнопку ОК.

Задание 1. Для созданной в задании 1 лабораторной работы № 1 базы данных проведите репликацию

[Методика и порядок выполнения задания 2](#)

Методика и порядок выполнения задания 2 совпадает с методикой и порядком выполнения задания 1. Только вместо последовательности операций следует выполнить действия:

F10 → Сервис → Репликация → Частичная репликация → Ввод

Задание 2. Для созданной в задании 1 лабораторной работы № 1 базы данных выполните частичную репликацию.

Методика и порядок выполнения задания 3

1. Запустите СУБД Access.

2. Откройте реплицированную базу данных.

3. Для проведения операции синхронизации выполните действия: **F10 → Сервис → Репликация → Синхронизация → Ввод (F10 → Tools → Replication → SynchronizeNow → Enter)**.

4. В появившемся диалоговом окне синхронизации укажите путь доступа к реплике, с которой требуется синхронизировать открытую базу данных, а затем изменить статус одной из реплик в наборе.

5. Для завершения процесса синхронизации нажмите кнопку ОК.

Задание 3. Для реплицируемых в заданиях 1 и 2 данной лабораторной работы баз данных выполните синхронизацию реплик.

Методика и порядок выполнения задания 4

1. Загрузите СУБД Access.

2. Откройте реплицированную базу данных, подлежащую синхронизации.

3. Для устранения ошибок при синхронизации реплик выполните действия: **F10** → **Сервис** → **Репликация** → **Устранить конфликты** → **Ввод (F10)** → **Tools** → **Replication** → **ResolveConflicts** → **Enter**).

4. Если в процессе синхронизации были обнаружены ошибки, то СУБД выводит на экран окно, содержащее справочную информацию по устранению конфликтов. Используя это окно, пользователь может выяснить причину возникновения конфликта, уточнить конфликтные записи в репликах.

5. Для завершения процесса синхронизации нажмите кнопку ОК.

Задание 4. Для реплицируемых в заданиях 1 и 2 данной лабораторной работы баз данных выполните разрешите конфликты, возникшие при синхронизации реплик.

Отчет по лабораторной работе должен состоять из:

- 1) названия лабораторной работы;
- 2) ответов на контрольные вопросы;
- 3) формулировки заданий и порядка их выполнения.

Отчет о выполнении лабораторной работы в письменном виде сдается преподавателю.

Контрольные вопросы:

1. Что такое репликация баз данных?
2. Какие реплики входят в набор?
3. В чем заключается процесс создания основной реплики?
4. Для чего используется репликация баз данных?
5. Алгоритм выполнения репликации баз данных.
6. В чем заключается процесс синхронизации реплик в базе данных?
7. Последовательность действий при выполнении синхронизации.

Практическая работа №28. Восстановление информации в базе данных.

Цель работы: сформировать представление о восстановлении информации в базе данных, сформировать умения по проведению восстановления информации в базе данных.

Оборудование, технические и программные средства: персональный компьютер, SQLServer 2000.

Теоретическое обоснование

Контрольные точки (checkpoints) — это функции, которые в SQLServer выполняется с целью записи изменений или параметров конфигурации в базу данных в определенный момент времени. При этом в некоторых случаях (достаточно часто) необходимо произвести повторную загрузку сервера, что влечет за собой процесс установки контрольных точек вручную.

Процесс установки контрольных точек может осуществляться либо «вручную», либо в результате естественного процесса, основанного на событиях сервера, все "грязные" страницы (dirty pages) памяти сохраняются на диске. "Грязная" страница — это область диска, содержащая обновленные данные, которые еще не были сохранены на диске. Без принудительного выполнения контрольные точки обычно фиксируются через каждую минуту.

При работе с контрольными точками может быть использован флажок **TruncateLogonCheckpoint**. Он автоматически укорачивает журнал транзакций при выполнении контрольной точки. Для установки этого флажка в окне SQLServerEnterpriseManager выберите базу данных и щелкните правой кнопкой мыши. Выберите команду Edit, а затем перейдите на вкладку Options.

Если отменить установку флажка **TruncateLogonCheckpoint**, то операция репликации баз

данных не используется, а SQLServer укорачивает журнал транзакций до последней успешно завершённой транзакции. В случае применения репликации SQLServer укорачивает журнал до последней успешно реплицированной и успешно завершённой транзакции. Репликация требует работы с журналом транзакций. Поэтому нельзя укоротить журнал транзакций, если транзакция не была распространена на подписчиков данной публикации

Средство проверки целостности базы данных (DatabaseConsistencyChecker, DBCC), как метод ее администрирования, применяется для генерирования подробной информации об объектах базы данных, управляемых системой SQLServer. Существует большое количество реализаций систем SQLServer и способов управления таблицами, правилами, триггерами, хранимыми процедурами и т. п., поэтому очень важно иметь возможность войти в систему сервера и произвести проверку целостности базы данных. Одним из основных средств проверки целостности базы данных является метод обеспечения наилучших результатов (режим одного пользователя). Все эти функции и выполняет утилита DBCC. Она поддерживает много различных инструкций для проверки логической и физической целостности базы данных, использования памяти, уменьшения размера базы данных, проверки статистик и т. д.

При проектировании базы данных чаще всего пользователем запрашивается объем дискового пространства несколько больший, чем это реально необходимо. После того как база данных начинает работать в штатном режиме, то можно будет определить, каким образом она будет увеличиваться и каков объем дискового пространства ей. Если база данных может быть уменьшена, то следует освободить пространство для других баз данных в вашей системе. Это можно сделать с помощью опции **DBCCSHRINKDATABASE**. Всегда помните, что эта опция работает со страницами. Поэтому следует определить размер базы данных и разделить его на 8196 (размер страницы в базе данных).

Получится. Синтаксис параметра SHRINKDB:

```
DBCCSHRINKDATABASE (имя_базы_данных  
[, новый_размер_в_процентах]  
[, {NOTTRUNCATE | TRUNCATEONLY}])
```

Не следует уменьшать размер главной базы данных, поскольку она содержит всю информацию о базах данных в системе. Если все же необходимо его уменьшить, обязательно предварительно создайте резервную копию этой базы данных. При уменьшении главной базы данных вы модифицируете базу, которая управляет в системе различными механизмами восстановления. Если при уменьшении размера главной базы данных произойдет отказ системы, вы не сможете восстановить эту базу данных без помощи резервной копии.

Аналогичные действия можно выполнить и с помощью SQLServerEnterpriseManager. Для этого щелкните правой кнопкой мыши на базе данных и в контекстном меню выберите команду **Task | ShrinkDatabase**. Появится диалоговое окно **ShrinkDatabase – имя_базы_данных**.

Как обычно, предлагается несколько вариантов действий. Можно принудительно уменьшить размер на заданное число процентов – установите переключатель **Shrinkdatabaseby (%)** и укажите проценты. Установите переключатель **Removeasmuchfreespaceaspossible**. В этом случае база данных "лишится" всего неиспользуемого пространства.

Последняя группа (Schedule) позволяет возложить на специальную службу SQLServer задачу периодического отслеживания размеров базы данных. Для этого нужно установить флажок **Periodicallychecktoseeifthedatabediskspacecanbeshrunk** и нажать кнопку **Schedule** для вызова диалогового окна **EditSchedule**, где можно установить расписание выполнения работы.

Методика и порядок выполнения работы

Методика и порядок выполнения задания 1

Методика и порядок выполнения задания 1 заключается в использовании основных приемов проектирования баз данных в SQLServer 2000.

Задание 1. Спроектируйте базу данных средствами SQLServer 2000.

Предметную область для ее проектирования выберите из перечня предметных областей, приведенных в задании 1 лабораторной работы № 1.

Методика и порядок выполнения задания 2

1. Запустите SQLServer 2000.

2. Войдите в спроектированную Вами базу данных. Для входа в базу данных Вы должны знать пароль доступа к ней.

3. Воткрывшемся окне **SQL Server Enterprise Manager** выберите базу данных, для которой следует установить контрольную точку.
4. Вызовите контекстное меню, выполнив щелчок правой кнопкой мыши.
5. В появившемся контекстном меню выберите команду **Edit**.
6. После этого на экран будет выведено диалоговое окно «... **Properties**», в котором перейдите на вкладку **Options**.
7. При помощи манипулятора «мышь» или клавиши **Tab** перейдите в поле **Truncate Logon Checkpoint** и установите в нем флажок.
8. Для завершения формирования контрольной точки нажмите последовательно кнопки **Apply (Применить)**, а затем **OK**.

Задание 2. Установите контрольную точку в базе данных, спроектированной в задании №1.

Методика и порядок выполнения задания 3

Методика выполнения задания 3 приведена в разделе «Теоретическое обоснование» данной лабораторной работы.

Задание 3. Используя инструкцию **SHRINKDATABASE (SHRINKDB)**, уменьшите размер базы данных.

Методика и порядок выполнения задания 4

1. Выполните загрузку **SQL Server 2000**, используя свой пароль.
2. Активизируйте спроектированную Вами базу данных.
3. Вызовите контекстное меню, выполнив щелчок правой кнопкой мыши.
4. В нем выполните следующую последовательность действий: **Task** → **ShrinkDatabase (Все задачи)** → **Уменьшение базы данных** и нажмите **Enter**.
5. В диалоговом окне **ShrinkDatabase - ...** укажите каким способом будет уменьшен размер базы данных. Способы уменьшения размеров базы данных приведены в разделе «Теоретическое обоснование» данной лабораторной работы.
6. Для завершения операции уменьшения размера базы данных с помощью **SQL Server Enterprise Manager** нажмите на кнопку **OK**.

Задание 4. Уменьшите размер базы данных, спроектированной в задании №1, с помощью механизмов управления **SQL Server Enterprise Manager**

Практическая работа №29. Мониторинг и обработка транзакций.

Цель работы: сформировать представление о том, что такое мониторинг и транзакции, сформировать умения по проведению мониторинга и обработки транзакций.

Оборудование, технические и программные средства: персональный компьютер, **SQL Server 2000**.

Теоретическое обоснование

Резервирование данных и журналов транзакций осуществляется путем записи дампа (*dump*) системы на дамповое устройство (*dump device*), которое **SQL Server** распознает как хранилище информации. Это может быть либо диск, и ленточное устройство.

Одни из лучших способов управления резервной копией информации предоставляется **SQL Server Enterprise Manager**. Для начала работы с системой резервирования выберите базу данных, которую требуется сохранить, правой кнопкой мыши и выполните команду **Tools | Backup Database** (или **Tasks | Backup Database**). Появится диалоговое окно **SQL Server Backup**, где расположены вкладки **General** и **Options**.

Основными видами резервирования в **SQL Server** являются:

- **Database – Complete (полная копия базы данных)**. В этом случае сохраняются любые действия над базой данных, производимые в процессе копирования, все незафиксированные транзакции и, естественно, все данные. Для создания первой копии необходимо выбрать именно этот вариант.

- **Database – Differential (дифференциальная копия)**. В этом случае **SQL Server** сохраняет только те части базы данных, которые изменились со времени создания полной копии и имеющиеся в журнале незафиксированные транзакции. В этом случае резервное копирование производится быстрее, чем в предыдущем, но полная копия должна существовать.

- **Transaction log (копия журнала транзакций)**. В этом случае сохраняются все изменения, произошедшие в базе данных.

- **Fileandfilegroup (копия файла или группы файлов).** В SQLServer реализована новая система хранения информации, которая базируется на таких понятиях, как «файл» и «группа файлов». В случае большой базы данных, когда требуется много времени на создание полной копии, можно включить в резервную копию только некоторые из составляющих ее файлов. Выбрав этот переключатель, вы получите доступ к кнопке с тремя точками, нажатием которой открывается диалоговое окно **SpecifyFilegroupupsandFiles**, где можно выбрать файлы для сохранения.

Следует отметить, что помимо основных типов резервных копий, также выделяют и типы резервирования, которые определяются параметрами системы или пользователем базы данных: 1) автоматическое – при установке флажка **Schedule**; 2) единовременное – при условии, что он снят. Единовременное резервирование еще называют ручным.

Для эффективной работы с базой данных, спроектированной в SQLServer, обязательно должны резервироваться следующие объекты:

- 1) главная база данных;
- 2) все базы данных, информацию из которых нельзя потерять;
- 3) все журналы транзакций для каждой базы данных, которые работают в системе или подвергаются тестированию.

Если база данных была повреждена в силу некорректных действий пользователя или вследствие сбоев в работе аппаратной и программной части системы, то необходимо провести восстановление системы. Основными действиями для её восстановления являются:

- 1) восстановление главной базы данных;
- 2) восстановление последней полной копии базы данных, если она была сделана;
- 3) восстановление журналов транзакций, которые были зарезервированы пользователем, начиная с момента получения последней резервной копии базы данных.

Методика и порядок выполнения работы

Методика и порядок выполнения задания 1

1. Запустите SQLServer 2000 и войдите в Ваш рабочий профиль, используя пароль.
2. В нем выберите базу данных, для которой нужно выполнить резервное копирование.
3. Выполните последовательность действий: **Tools** → **BackupDatabase** или **Tasks** → **BackupDatabase**.
4. В результате чего на экран будет выведено диалоговое окно **SQLServerBackup**, содержащее вкладки **General** и **Options**.
5. В поле **Database** укажите имя базы данных, подлежащей резервированию; в поле **Name** – имя ее резервной копии; **Description** – задается описание, использование которого облегчит работу с резервируемой базой данных.
6. С помощью клавиши **Tab** перейдите в область **Backup** и укажите тип создаваемой резервной копии.
7. Затем активизируйте область окна **Destination**, в которой указывается область диска или диск для размещения резервной копии базы данных.
8. Нажмите кнопку **Add** в группе **Destination**.
9. В диалоговом окне **ChooseBackupDestination** определите месторасположения резервной копии базы данных: в отдельном файле или на внешнем устройстве. Для сохранения резервной копии в отдельном файле достаточно указать полный путь доступа к нему; во втором случае – указывается и тип носителя, на котором будет сохраняться копия, и новое имя файла. Для возврата в диалоговое окно **SQLServerBackup** достаточно нажать кнопку **OK**.
10. Для автоматического резервирования базы данных установите флажок в поле **Schedule**, если он снят, то резервирование будет единовременным.
11. Для завершения операции резервирования достаточно нажать на кнопку **OK**.

Задание 1. Выполните резервирование базы данных спроектированной в задании 1 лабораторной работы № 6. В качестве методов резервирования выберите и автоматическое резервирование, и единовременное.

Методика и порядок выполнения задания 2

1. Запустите SQLServer 2000 и войдите в него с помощью известного Вам пароля.
2. В начале операции восстановления базы данных выполните следующую последовательность команд: **Tasks** → **RestoreBackup**.
3. После чего на экран будет выведено диалоговое окно **RestoreDatabase**, которое также содержит вкладки **General** и **Options**.

4. В этом диалоговом окне в поле **Usebackupsformdatabase** в начале выберите ту базу данных, о которой необходимо получить информацию и нажмите Enter. После чего SQL Server выведет всю информацию о тех базах данных, для которых было успешно завершено резервное копирование.

5. Затем из предлагаемого списка выберите тип восстановления базы данных.

6. После заполнения диалогового окна **RestoreDatabase** нажмите на кнопку OK. Если все параметры для восстановления базы данных указаны верно, то на экран будет выведено окно сообщений, в котором отображается процесс восстановления базы данных.

Задание 2. Проведите операцию восстановления базы данных. Базой данных, подлежащей восстановлению, считать базу данных, зарезервированную в предыдущем задании.

Отчет по лабораторной работе должен состоять из:

- 1) названия лабораторной работы;
- 2) ответов на контрольные вопросы;
- 3) формулировки заданий и порядка их выполнения.

Отчет о выполнении лабораторной работы в письменном виде сдается преподавателю.

Вопросы для защиты работы

1. Для чего необходимо выполнять резервирование баз данных?
2. Назовите основные типы резервирования и резервных копий.
3. Какие элементы подлежат резервированию в SQL Server?
4. Последовательность действий при выполнении резервирования баз данных в SQL Server.
5. Перечислите необходимые действия для восстановления системы.
6. Алгоритм восстановления системы в SQL Server.
7. Что такое контрольные точки?
8. Для чего они предназначены?
9. Каким образом можно установить контрольную точку?
10. Алгоритм установки контрольной точки с помощью флажка TruncateLogonCheckpoint.
11. Каким образом осуществляется проверка целостности базы данных в SQL Server?
12. Метод обеспечения наилучших результатов: режим одного пользователя.
13. Инструкция SHRINKDATABASE (SHRINKDB).
14. Последовательность действий для уменьшения дискового пространства с помощью SQL Server Enterprise Manager.

Практическая работа № 29. Восстановление информации в базе данных.

Цель работы: сформировать представление о восстановлении информации в базе данных, сформировать умения по проведению восстановления баз данных.

Оборудование, технические и программные средства: персональный компьютер, СУБД Access.

Теоретическое обоснование

Основными методами обслуживания баз данных как администрирования являются восстановление, копирование и сжатие базы данных.

Восстановление базы данных как средство их администрирования используются в том случае, если она была повреждена, и эти повреждения не позволяют нормально работать с ней или даже открыть её.

Повреждение базы данных может быть вызвано следующими причинами: 1) воздействие компьютерных вирусов; 2) наличие дефектов (логических и физических) на дисках; 3) повреждениями во время эксплуатации.

Создание копий баз данных используется в том случае, если необходимо сохранить информацию от несанкционированного доступа и потерей. Копии баз данных создаются стандартными способами, причем они могут храниться в сжатом виде.

Сжатие файлов баз данных можно осуществлять стандартными программами – архиваторами. Сжатие баз данных средствами СУБД отличается от сжатия файлов баз данных при помощи программ – архиваторов. Оно состоит в следующем: на диске освобождается место для удаленных из базы данных записей.

Методика и порядок выполнения работы

Методика и порядок выполнения задания 1

Методика выполнения задания № 1 заключается в правильном использовании программ «файловых менеджеров»

Задание 1. Создайте резервную копию базы данных, разработанной Вами в задании 1 лабораторной работы № 1.

Методика и порядок выполнения задания 2

1. Запустите СУБД Access.
2. Если открытая Вами ранее база данных совершает непредсказуемые действия, то её вначале следует закрыть. В том случае, если база данных является сетевой, то её должны закрыть все пользователи, работающие с ней в данный момент.

3. Создайте резервную копию базы данных.

4. Для восстановления файла базы данных выполните следующую последовательность действий: **F10 → Сервис → Служебные программы → Восстановить → Ввод (F10 → Tools → DatabaseUtilities → RepairDatabase → Enter).**

5. В появившемся диалоговом окне укажите имя базы данных, которую необходимо восстановить и полный путь доступа к ней.

Задание 2. Выполните восстановление поврежденной базы данных. Перед выполнением данного задания допустите ошибки при загрузке базы данных, сформированной в задании 1 лабораторной работы № 1.

Методика и порядок выполнения задания 3

1. Загрузите СУБД Access. В нем откройте ранее сформированную базу данных.

2. Для сжатия базы данных выполните последовательность действий: **F10 → Сервис → Служебные программы → Сжать → Ввод (F10 → Tools → DatabaseUtilities → CompactDatabase → Enter).**

3. В диалоговом окне **CompactDatabase (база данных для сжатия)** выберите базу данных для сжатия, а затем нажмите кнопку **Compact (Сжать).**

Задание 3. Выполните операцию сжатия базы данных. В качестве исходной базы данных для сжатия выберите базу, спроектированную в задании 1 лабораторной работы № 1.

Отчет по лабораторной работе должен состоять из:

- 1) названия лабораторной работы;
- 2) ответов на контрольные вопросы;
- 3) формулировки заданий и порядка его выполнения.

Отчет о выполнении лабораторной работы в письменном виде сдается преподавателю.

Контрольные вопросы:

1. Перечислите и охарактеризуйте основные операции обслуживания баз данных как средства их администрирования.
2. Копирование баз данных.
3. Алгоритм восстановления базы данных.
4. Последовательность действий при сжатии баз данных.

Практическая работа №30. Технология управления базами данных средствами языка SQL

Цель работы: сформировать представление о технологии управления базами данных, сформировать умения по управлению базами данных средствами языка SQL.

Оборудование, технические и программные средства: персональный компьютер, СУБД Access.

Вам необходимо знать

Функциональные возможности языка SQL

Язык SQL (Structured Query Language) – это структурированный язык запросов для работы с базами данных.

Этот язык пригоден для использования многими СУБД на множестве современных компьютерных платформ. Пользователи, владеющие им, имеют огромные возможности доступа и применения данных разнообразных баз независимо от среды их создания.

В этом разделе рассматривается стандарт SQL-2, который в дальнейшем обозначается просто SQL.

Язык SQL имеет определенный набор команд, которые позволяют осуществлять:

- организацию данных;
- изменение данных;
- чтение данных;
- управление доступом к данным;
- совместное использование данных;
- обеспечение целостности данных;
- обращение к базам данных в прикладных программах.

Структура SQL-команды

Каждая команда SQL начинается с ключевого слова – глагола, описывающего действие, выполняемое командой, например, CREATE (создать). В команде может быть одно или несколько предложений. Предложение описывает данные, с которыми работает команда, или содержит уточняющую информацию о действии, выполняемом командой. Каждое предложение начинается с ключевого слова, например, WHERE (где). Одни предложения в команде являются обязательными, а другие – нет. Некоторые предложения могут содержать дополнительные ключевые слова, выражения. Многие предложения включают имена таблиц или полей. Имена должны содержать от 1 до 18 символов, начинаться с буквы и не содержать пробелы и специальные символы пунктуации. В качестве имен нельзя использовать ключевые слова.

Пример SQL - команды:



Для выполнения операций над данными в SQL существуют выражения. Выражения представляют собой определенную последовательность полей, констант, функций, соединенных операторами.

В полях могут храниться данные определенных типов. Некоторые из них перечислены в табл. 8.1.

Таблица 8.1

Тип данных	Описание
CHAR(длина)	Строки символов постоянной длины
CHARACTER(длина)	
INTEGER	Целые числа
INT	Малые целые числа
SMALLINT	

В выражениях могут использоваться константы.

Примеры констант с фиксированной запятой: 21 -375.18 62.3

Примеры констант с плавающей запятой: 0.5E7 -3.14E9 2.5E-6

Примеры строковых констант: 'New York', 'пр. Скорини, 28-4'.

Обработка отсутствующих значений может осуществляться с помощью константы отсутствующее значение (NULL). Например, значение NULL в поле "Дата рождения" означает, что дата рождения студента неизвестна, а значение NULL в поле "Оценка" – что студент не сдавал экзамен.

Функции задают выполнение определенных операций. Например, функция Now() возвращает текущее значение даты и времени.

В выражениях можно использовать следующие операторы:

- 1) арифметические: + (сложение), - (вычитание), * (умножение), / (деление);
- 2) сравнения: = (равно), > (больше), < (меньше), >= (больше или равно), <= (меньше или равно), <> (не равно);
- 3) логические: AND (логическое "И"), OR (логическое "ИЛИ"), NOT (отрицание "НЕТ");
- 4) специальные:
 - IN - определяет множество, которому может принадлежать значение;
 - BETWEEN - задает границы, в которых должно находиться значение;
 - LIKE - применяется для поиска по шаблону;
 - IS NULL - используется для поиска NULL-значений.

Соглашения по записи форматов SQL-команд

Формирование запросов на языке SQL предполагает ввод команд с клавиатуры в строгом соответствии с их форматами. Для записи форматов команд (иногда усеченных) будем использовать следующие соглашения:

- <> (угловые скобки). То, что в них указано, определяет пользователь;
- [] (квадратные скобки). Выделяют те части команды, которые могут отсутствовать;
- { },... Заключенная в фигурные скобки часть команды может быть повторена несколько раз, причем повторы разделяются запятыми;
- ½ (вертикальная черта). Означает альтернативный выбор.

А Для выполнения последующих заданий создать в Access файл базы данных в своей папке с именем ПРИМЕРЫ-SQL.

8.1. Организация данных

Задание 8.1. Создать структуру таблицы СВЕДЕНИЯ, представленной в табл. 8.2, используя SQL-команду.

Таблица 8.2

СВЕДЕНИЯ				
Номер зачетной книжки	Ф.И.О. студента	Год рождения	Пол	
200101	ИВАНОВ И. И.	1985	МУЖ	
200102	ПЕТРОВ П. П.	1986	МУЖ	
200103	СИДОРОВ С. С.	1985	МУЖ	
200104	МАЛКО М. М.	1987	ЖЕН	
200201	ИЛЬИНА И. И.	1986	ЖЕН	
200202	ФЕДОРОВ Ф. Ф.	1985	МУЖ	

С учетом типа, размера и свойств данных таблицы СВЕДЕНИЯ, а также требований языка SQL к описанию данных, можно описать поля этой таблицы как в табл. 8.3.

Таблица 8.3

Описание полей таблицы СВЕДЕНИЯ				
	Номер зачетной книжки	Ф.И.О. студента	Год рождения	Пол
Имя поля	НОМЗ	ФИО	ГОД	ПОЛ
Тип данных	Целые числа	Строки символов постоянной длины	Целые числа	Строки символов постоянной длины
Размер поля	-	15	-	3
Ограничения на поле	Обязательно для заполнения. Ключевое поле.	Обязательно для заполнения	-	-

Запрос на создание структуры таблицы на языке SQL реализуется с помощью команды **CREATE TABLE**, имеющей следующий формат:

```
CREATE TABLE <имя таблицы>
( (<имя поля> <тип данных> [<размер>]
  [<ограничения на поле>]
  [<значение поля по умолчанию>]),...
  [<ограничения на таблицу>] )
```

Приведем некоторые из ограничений на поля:

- **NOT NULL** – поле, для которого указано это ограничение, не допускает значений NULL;
- **UNIQUE** – поле, для которого указано это ограничение, не допускает повторяющихся значений;
- **PRIMARY KEY** – поле, для которого это ограничение задано, должно выступать в роли первичного ключа;

Значение поля по умолчанию указывается при помощи ключевого слова **DEFAULT**.

Ограничения на таблицу применяются к группам, состоящим из нескольких полей. Они задаются при помощи ключевого слова **CHECK**.

Выполнение задания

Откройте окно Конструктора запроса, выполнив действия:

окно *База данных* ▶ объект *Запросы* ▶ [Создать] ▶

окно *Новый запрос* ▶ выбрать *Конструктор* ▶

окно *Добавление таблицы* ▶ [Закрыть]

Затем выполните следующее:

- перейдите в режим **SQL**, введя команду

Вид/Режим SQL

В результате появится окно SQL-запроса, в котором можно формировать запрос на языке SQL и редактировать его, используя для этого привычную технологию редактирования в текстовом редакторе. Вид окна SQL-запроса приведен на рис. 8.1;

- в окне SQL-запроса наберите команду для создания структуры таблицы СВЕДЕНИЯ:

```
CREATE TABLE СВЕДЕНИЯ (НОМЗ INT NOT NULL PRIMARY KEY, ФИО CHAR(15) NOT NULL, ГОД INT, ПОЛ CHAR(3))
```

Эта команда сформирована с учетом формата команды **CREATE TABLE** и описания полей таблицы СВЕДЕНИЯ, произведенного в табл. 8.3;

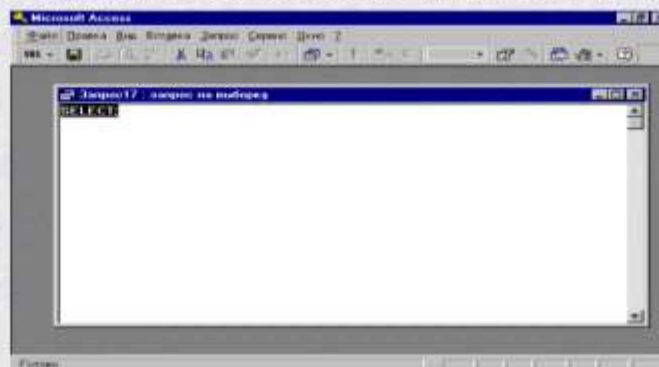



Рис. 8.1. Вид окна Конструктора запроса в режиме SQL

Примечание. Набор SQL-команд можно осуществлять, используя прописные и строчные русские и английские буквы. Но для ускорения работы целесообразно его производить на одном регистре, например, полностью прописными буквами.

- выполните запрос по команде

Запрос/Запуск

или при помощи кнопки  (Запуск);

- сохраните запрос с именем **СозданиеСВЕДЕНИЯ**, закрыв окно SQL-запроса или выполнив команду

Файл/Сохранить

- активизируйте объект Таблицы и убедитесь в наличии таблицы СВЕДЕНИЯ.

Примечание. Выполнение SQL-запроса из окна базы данных производится при помощи кнопки [Открыть].

Задание 8.2. Создать структуру таблицы УСПЕВАЕМОСТЬ, представленной в табл. 8.4, используя SQL-команду.

Таблица 8.4

УСПЕВАЕМОСТЬ				
Номер зачетной книжки	Группа	Оценка по математике	Оценка по информатике	
200101	M-1	5	5	
200102	M-1	4	5	
200103	M-1	4	3	
200104	M-2	2	4	
200201	M-2	3	4	
200202	M-2	4	-	

С учетом типа, размера данных таблицы УСПЕВАЕМОСТЬ, а также требований языка SQL к описанию данных, можно описать поля этой таблицы как в табл. 8.5.

Таблица 8.5

Имя поля	Описание полей таблицы УСПЕВАЕМОСТЬ			
	Номер зачетной книжки	Группа	Оценка по математике	Оценка по информатике
Имя поля	НОМЗ	ГРУП	ОМАТЕМ	ОИНФ
Тип данных	Целые числа	Строки символов постоянной длины	Целые числа	Целые числа
Размер поля	-	6	-	-
Ограничения на поле	Обязательно для заполнения. Не допускаются повторяющиеся значения	-	-	-

Выполнение задания

Откройте окно SQL-запроса и выполните следующее:

- в окне SQL-запроса наберите команду для создания структуры таблицы УСПЕВАЕМОСТЬ:
CREATE TABLE УСПЕВАЕМОСТЬ (НОМЗ INT NOT NULL UNIQUE, ГРУП CHAR(6), ОМАТЕМ INT, ОИНФ INT)
- выполните запрос;
- сохраните запрос с именем СозданиеУСПЕВАЕМОСТЬ;
- активизируйте объект Таблицы и убедитесь в наличии таблицы УСПЕВАЕМОСТЬ.

8.2. Изменение данных

Задание 8.3. Добавить в таблицу СВЕДЕНИЯ запись с данными, представленными в табл. 8.1, используя SQL-команду.

Добавление записей в таблицу осуществляется с помощью команды **INSERT** следующего формата:

```
INSERT INTO <имя таблицы>[((<имя поля>),...)]
VALUES (<значение>),...
```

Если имена полей не указаны, то значениями заполняются поля, состав и порядок которых был описан командой **CREATE TABLE**. Значения полей задаются константами (выражения не допустимы).

Выполнение задания

Откройте окно SQL-запроса и выполните следующее:

- наберите команду для добавления в таблицу СВЕДЕНИЯ запись с данными из первой строки табл. 8.1:
INSERT INTO СВЕДЕНИЯ VALUES (200101, 'ИВАНОВ И. И.', 1985, 'МУЖ')
- выполните запрос;
- сохраните запрос с именем ПЕРВАЯ СТРОКА;
- активизируйте объект Таблицы, откройте таблицу СВЕДЕНИЯ и убедитесь в наличии первой записи;
- аналогично набирайте в окне SQL-запроса команду для добавления записи с данными из второй строки табл. 8.1, выполните запрос, сохраняйте его с именем ВТОРАЯ СТРОКА и т.д.

Задание 8.4. Добавить в таблицу УСПЕВАЕМОСТЬ запись с данными, представленными в табл. 8.4, используя SQL-команду.

Выполнение задания

Выполните это задание аналогично заданию 3. Для добавления записи с данными из последней строки таблицы, в которой оценка по информатике не определена, УСПЕВАЕМОСТЬ выполните следующий запрос:

```
INSERT INTO УСПЕВАЕМОСТЬ VALUES (200202, 'M-2', 4, NULL)
```

Задание 8.5. Изменить с помощью SQL-команды в таблице СВЕДЕНИЯ фамилию студентки ИЛЬИНОЙ И.И., у которой номер зачетной книжки 200201, на фамилию КРАВЦОВА.

Запрос на изменение значений полей таблицы реализуется с помощью команды **UPDATE**, имеющей следующий формат:

```
UPDATE <имя таблицы>
SET {<имя поля>=<выражение>}...
[WHERE <условие>]
```

Условие задается выражением типа сравнения или логическим выражением. Если предложение **WHERE** отсутствует, то изменения выполняются во всех записях таблицы.

Выполнение задания

Откройте окно SQL-запроса и выполните следующее:

- наберите команду на изменение фамилии студентки с номером зачетной книжки 200201:
UPDATE СВЕДЕНИЯ
 SET ФИО = 'КРАВЦОВА И. И.'
 WHERE НОМЗ=200201
- выполните запрос,
- сохраните его с именем ЗАМЕНА;
- откройте таблицу СВЕДЕНИЯ и убедитесь в произведенном изменении.

Задание 5.6. Удалить с помощью SQL-команды из таблицы СВЕДЕНИЯ данные о студентке, у которой номер зачетной книжки 200201.

Запрос на удаление записей из таблицы формируется с помощью команды DELETE следующего формата:

```
DELETE FROM <имя таблицы>  
  [WHERE <условие>]
```

Если предложение **WHERE** отсутствует, то удаляются все записи таблицы.

Выполнение задания

Откройте окно SQL-запроса и выполните следующее:

- наберите команду на удаление сведений о студентке с номером зачетной книжки 200201:
DELETE FROM СВЕДЕНИЯ
 WHERE НОМЗ=200201
- выполните запрос,
- сохраните его с именем УДАЛЕНИЕ;
- откройте таблицу СВЕДЕНИЯ и убедитесь в произведенном удалении.

http://bseu.by/it/tohod/praktikum8_2.htm