

**Автономная некоммерческая организация профессионального образования  
«ПЕРМСКИЙ ГУМАНИТАРНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»  
(АНО ПО «ПГТК»)**

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ  
ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ  
ПО ДИСЦИПЛИНЕ**

**МДК.02.03 СЕРТИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ**

для специальности

**09.02.13 «Интеграция решений с применением технологий  
искусственного интеллекта»  
(код и наименование специальности)**

Квалификация выпускника

**Специалист по работе с искусственным интеллектом**

Форма обучения

**Очная**

Пермь 2026

Методические рекомендации по выполнению практических работ учебной дисциплины МДК.02.03 СЕРТИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ составлен в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.13 «Интеграция решений с применением технологий искусственного интеллекта»

Данные методические рекомендации помогут организовать самостоятельную деятельность студентов на основе деятельного и компетентного подходов к обучению, что соответствует ФГОС СПО по специальности 09.02.13 «Интеграция решений с применением технологий искусственного интеллекта».

Программа предназначена для студентов и преподавателей АНО ПО «ПГТК».

Автор – составитель: Могильникова Н.С., старший преподаватель.

Методические рекомендации по выполнению практических работ предназначен для оценивания достижений запланированных результатов

Методические рекомендации по выполнению практических работ представляет собой комплект материалов для проведения практических занятий (в форме практической подготовке) и осуществления контроля за выполнением работ.

Методические рекомендации по выполнению практических работ позволяет оценивать:

Код ОК, ПК	Уметь	Знать
ПК 2.1 Выявлять проблемы, возникающие в процессе эксплуатации баз данных. ПК 2.2 Осуществлять процедуры администрирования баз данных. ПК 2.3 Проводить аудит систем безопасности баз данных с использованием регламентов по защите информации. ПК 2.4 Формировать требования хранилищ банка данных для обучения. ПК 2.5 Подготавливать данные для базы знаний. ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам ОК 02 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач	Производить идентификацию проблем, связанных с нормальным функционированием базы данных; Принимать решения по локализации проблем, связанных с нормальным функционированием базы данных; Документировать внештатные ситуации связанные с нормальным функционированием базы данных; Осуществлять основные функции по администрированию баз данных; Настраивать политики безопасности при работе с сервером баз данных Дать независимую оценку уровня безопасности Производить регламентное обновление программного обеспечения Разрабатывать перечень рекомендаций по дальнейшей эксплуатации БД с максимальной защитой хранящейся информации. Производить формирование требований к обработке данных и их извлечению; Добавлять, удалять и изменять данные в базе данных; Производить операции по импорту и экспорту данных в различных форматах распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять её составные части определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы владеть актуальными методами работы в профессиональной и смежных сферах	Основные коды ошибок при работе с базой данных; Методы и средства устранения ошибок, возникающих при работе с базой данных; Тенденции развития банков данных; Технология установки и настройки сервера баз данных; Требования к безопасности сервера базы данных; Протоколы безопасности при работе с базой данных; Методы и средства защиты информации от несанкционированного доступа; Уровни угроз безопасности информации Формы документов, необходимых для формирования, ведения и использования банка данных Типы данных хранения информации в базе данных актуальный профессиональный и социальный контекст, в котором приходится работать и жить структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях основные источники информации и ресурсы для решения задач и/или проблем в профессиональном и/или социальном контексте методы работы в профессиональной и смежных сферах порядок оценки результатов решения задач профессиональной деятельности номенклатура информационных источников, применяемых в профессиональной деятельности приемы структурирования информации

профессиональной деятельности ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска оценивать практическую значимость результатов поиска применять средства информационных технологий для решения профессиональных задач использовать современное программное обеспечение в профессиональной деятельности использовать различные цифровые средства для решения профессиональных задач грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке проявлять толерантность в рабочем коллективе	формат оформления результатов поиска информации современные средства и устройства информатизации, порядок их применения программное обеспечение в профессиональной деятельности, в том числе цифровые средства психологические основы деятельности коллектива правила оформления документов правила построения устных сообщений особенности социального и культурного контекста
---	--	--


В результате текущей аттестации по учебной дисциплине МДК.02.03 Сертификация информационных систем осуществляется проверка сформированности умений и знаний, направленных на формирование соответствующих ФГОС СПО общих и профессиональных компетенций.

Практическое занятие «Настройка политики безопасности»

Цель: изучить процесс настройки политики безопасности на ПК

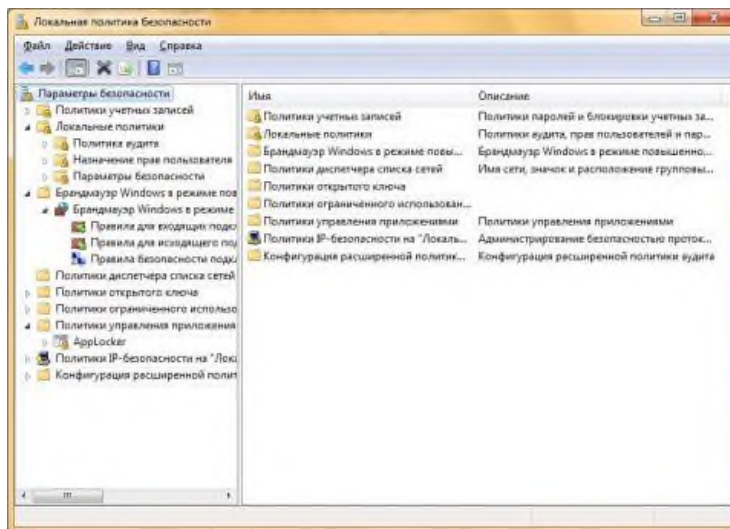
Теоретические сведения

Политика безопасности – это набор параметров, которые регулируют безопасность компьютера и управляются с помощью локального объекта GPO. Настраивать данные политики можно при помощи оснастки «Редактор локальной групповой политики» или оснастки «Локальная политика безопасности». Оснастка «Локальная политика безопасности» используется для изменения политики учетных записей и локальной политики на локальном компьютере, а политики учетных записей, привязанных к домену Active Directory можно настраивать при помощи оснастки «Редактор управления групповыми политиками». Перейти к локальным политикам безопасности, вы можете следующими способами:

1. Нажмите на кнопку «Пуск» для открытия меню, в поле поиска введите Локальная политика безопасности и [откройте приложение в найденных результатах](#);
2. Воспользуйтесь комбинацией клавиш  +R для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть» введите secpol.msc и нажмите на

кнопку «ОК»;

3. Откройте «Консоль управления MMC». Для этого нажмите на кнопку «Пуск», в поле поиска введите mmc, а затем нажмите на кнопку «Enter». Откроется пустая консоль MMC. В меню «Консоль» выберите команду «Добавить или удалить оснастку» или воспользуйтесь комбинацией клавиш Ctrl+M. В диалоге «Добавление и удаление оснасток» выберите оснастку «Редактор локальной групповой политики» и нажмите на кнопку «Добавить». В появившемся диалоге «Выбор объекта групповой политики» нажмите на кнопку «Обзор» для выбора компьютера или нажмите на кнопку «Готово» (по умолчанию установлен объект «Локальный компьютер»). В диалоге «Добавление или удаление оснасток» нажмите на кнопку «ОК». В оснастке «Редактор локальной групповой политики» перейдите в узел «Конфигурация компьютера», а затем откройте узел «Параметры безопасности».



В том случае, если ваш компьютер подсоединен к домену Active Directory, политика безопасности определяется политикой домена или политикой подразделения, членом которого является компьютер.

Применение политик безопасности для локального компьютера и для объекта групповой политики рабочей станции, подсоединенной к домену

При помощи следующих примеров вы увидите разницу между применением политики безопасности для локального компьютера и для объекта групповой политики рабочего компьютера, присоединенного к домену Windows Server 2008 R2.

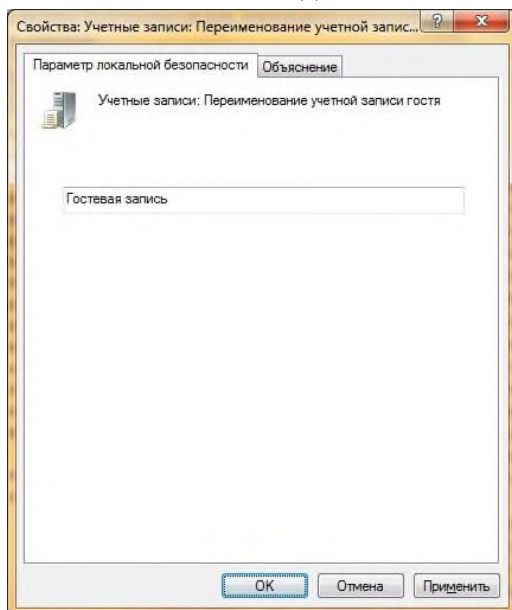
Применение политики безопасности для локального компьютера

Для успешного выполнения текущего примера, учетная запись, под [которой выполняются данные действия](#), должна входить в группу «Администраторы» на локальном компьютере. Если компьютер подключен к домену, то эти действия могут выполнять только пользователи, которые являются членами группы «Администраторы домена» или групп, с разрешенными правами на редактирование политик.

В этом примере мы переименуем гостевую учетную запись. Для этого выполните следующие действия:

1. Откройте оснастку «Локальные политики безопасности» или перейдите в узел «Параметры безопасности» оснастки «Редактор локальной групповой политики»;

2. Перейдите в узел «Локальные политики», а затем «Параметры безопасности»;
3. Откройте параметр «Учетные записи: Переименование учетной записи гостя» дважды щелкнув на нем или нажав на клавишу Enter;
4. В текстовом поле введите Гостевая запись и нажмите на кнопку «ОК»;



5. Перезагрузите компьютер.
6. После перезагрузки компьютера для того чтобы проверить, применилась ли политика безопасности к вашему компьютеру, вам нужно открыть в панели управления компонент «Учетные записи пользователей» и перейти по ссылке «Управление другой учетной записью». В открывшемся окне вы увидите все учетные записи, созданные на вашем локальном компьютере, в том числе переименованную учетную запись гостя:

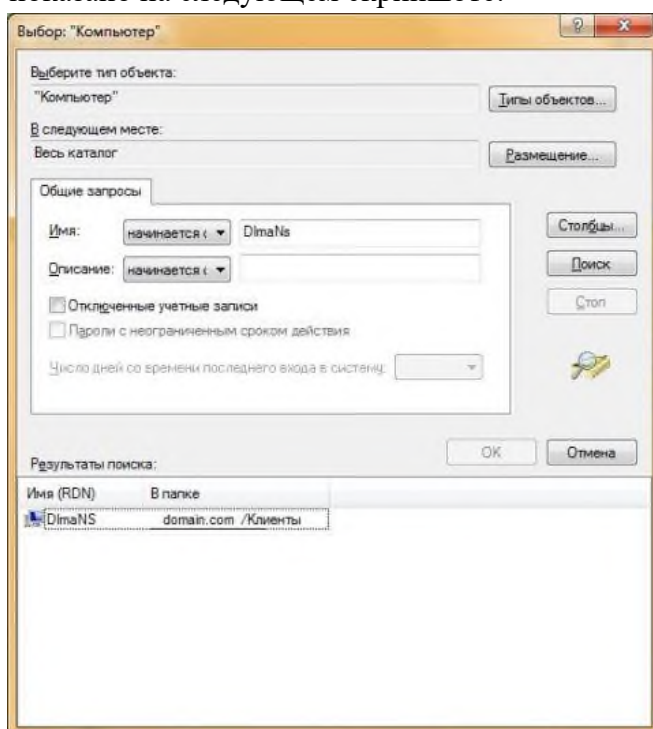


7. Применение политики безопасности для объекта групповой политики рабочей компьютер, присоединенного к домену Windows Server 2008 R2

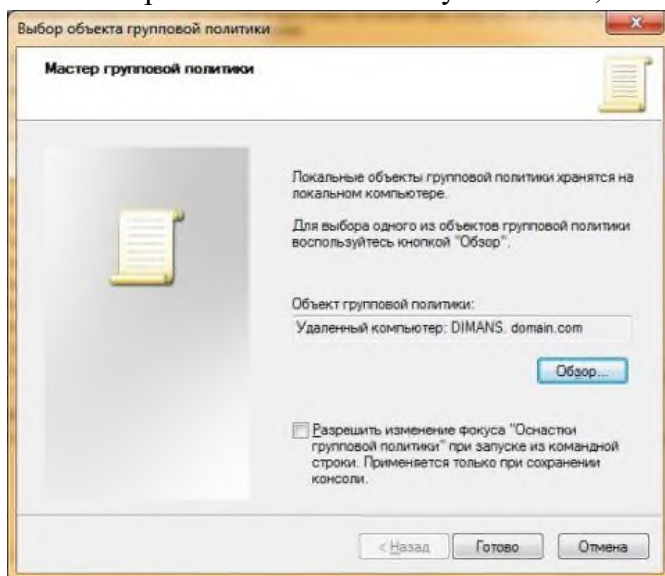
В этом примере мы запретим пользователю Test\_ADUser изменять пароль для учетной записи на своем компьютере. Напомню, что для выполнения следующих действий вы должны входить в группу «Администраторы домена». Выполните следующие действия:

1. Откройте «Консоль управления MMC». Для этого нажмите на кнопку «Пуск», в поле поиска введите mmc, а затем нажмите на кнопку «Enter»;
2. В меню «Консоль» выберите команду «Добавить или удалить оснастку» или воспользуйтесь комбинацией клавиш Ctrl+M;

3. В диалоге «Добавление и удаление оснасток» выберите оснастку «Редактор локальной групповой политики» и нажмите на кнопку «Добавить»;
4. В появившемся диалоге «Выбор объекта групповой политики» нажмите на кнопку «Обзор» для выбора компьютера и выберите нужный компьютер, как показано на следующем скриншоте:



5. В диалоге «Выбор объекта групповой политики» убедитесь, что выбрали нужный компьютер и нажмите на кнопку «Готово»;



6. В диалоге «Добавление или удаление оснасток» нажмите на кнопку «ОК»;
7. В оснастке «Редактор локальной групповой политики» перейдите в узел «Конфигурация компьютера», а затем откройте узел Параметры безопасности\Локальный компьютер\Параметры безопасности;
8. Откройте параметр «Контроллер домена: Запретить изменение пароля учетных записей компьютера» дважды щелкнув на нем или нажав на клавишу Enter;
9. В диалоге настроек параметра политики безопасности выберите опцию «Включить» и нажмите на кнопку «ОК»;



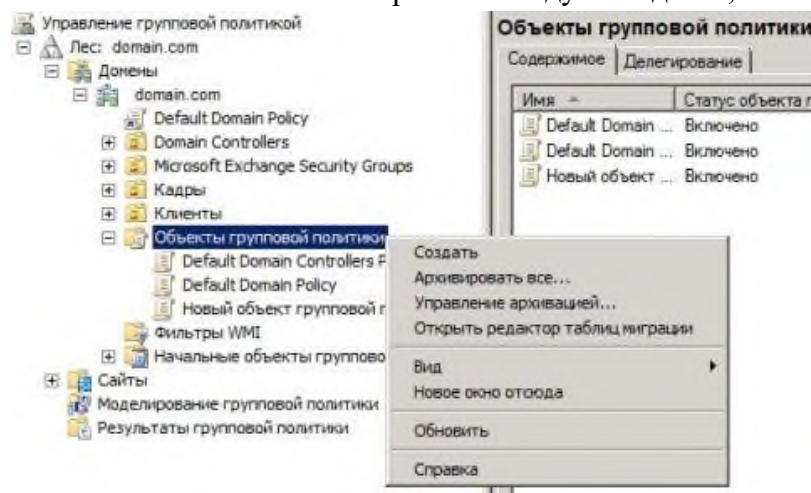
#### 10. Перезагрузите компьютер.

После перезагрузки компьютера для того чтобы проверить, применилась ли политика безопасности, перейдите на компьютер, над которым проводились изменения и откройте консоль управления MMC. В ней добавьте оснастку «Локальные пользователи и группы» и попробуйте изменить пароль для своей доменной учетной записи.

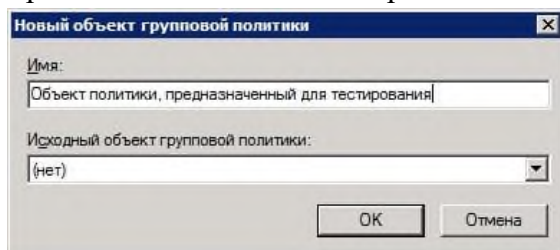
Применение политики безопасности для объекта групповой политики с контроллера домена Windows Server 2008 R2

При [помощи этого примера](#), изменим число новых уникальных паролей, которые должны быть назначены учетной записи пользователя до повторного использования старого пароля. Эта политика позволяет вам улучшать безопасность, гарантируя, что старые пароли не будут повторно использоваться в течении нескольких раз. Войдите на контроллер домена или используйте средства администрирования удаленного сервера. Выполните следующие действия:

1. Откройте консоль «Управление групповой политикой» - в диалоговом окне «Выполнить», в поле «Открыть» введите gpmmc.msc и нажмите на кнопку «ОК»;
2. В контейнере «Объекты групповой политики» щелкните правой кнопкой мыши и из контекстного меню выберите команду «Создать»;

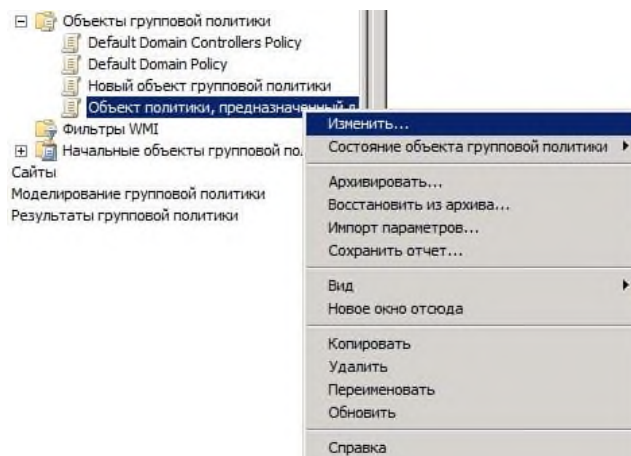


3. В поле «Имя» введите название объекта GPO, например «Объект политики, предназначенный для тестирования» и нажмите на кнопку «ОК»;

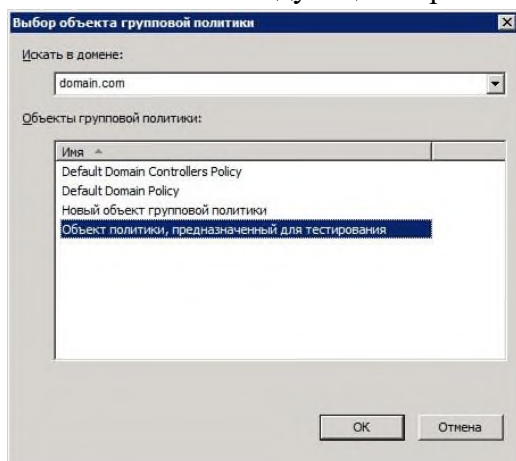


4. Щелкните правой кнопкой мыши на созданном объекте и из контекстного меню выберите команду «Изменить»;

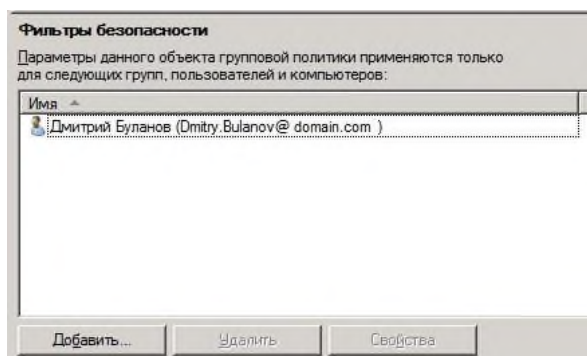




5. В окне «Редактор управления групповыми политиками» разверните узел Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей;
6. Откройте параметр «Вести журнал паролей» дважды щелкнув на нем или нажав на клавишу Enter;
7. В диалоге настройки параметра политики установите флажок на опции «Определить следующий параметр политики», в тестовом поле введите 5 и нажмите на кнопку «ОК»;
8. Закройте оснастку «Редактор управления групповыми политиками».
9. В консоли «Управление групповой политикой» нажмите правой кнопкой мыши на группе безопасности, для которой будут применяться изменения, и из контекстного меню выберите команду «Связать существующий объект групповой политики...». В диалоге «Выбор объекта групповой политики» выберите созданный вами объект, как показано на следующем скриншоте:



10. В фильтрах безопасности объекта политики выберите пользователя или группу, на которых будет распространяться указанные настройки.



11. Обновите параметры политики на клиентском компьютере при помощи команды `groupdate`.

Задание

1. Описать процесс настройки политики безопасности на ПК
2. Описать настройку Параметров безопасности на своем ПК

Контрольные вопросы

1. Перечислите этапы настройки политики безопасности
2. Где производится настройка политики безопасности системы?
3. Что такое политика безопасности?
4. В чем достоинства дискреционной политики безопасности?
5. В чем недостатки мандатной политики безопасности?
6. Кто определяет права доступа к папкам, файлам, принтерам при использовании дискреционной политики безопасности?
7. В чем отличие определения прав на доступ к файлам по сравнению с определением прав на доступ к папкам?
8. В чем отличие определения прав на доступ к принтерам по сравнению с определением прав на доступ к папкам и файлам?
9. В чем отличие определения прав на доступ к разделам реестра по сравнению с определением прав на доступ к папкам и файлам?

Содержание отчета

Отчет должен быть выполнен в соответствии с Общими требованиями к оформлению документов учебной деятельности обучающихся. Отчет должен содержать следующие разделы:

1. Наименование работы.
2. Цель работы.
3. Конечные результаты выполненной работы в виде скриншотов.
4. Ответы на контрольные вопросы.
5. Вывод.

Практические занятия «Создание резервных копий базы данных» и «Восстановление базы данных»

Цель работы: ознакомиться с основными конструкциями SQL, технологиями среды MS SQL Server Management, объектами SMO (среды MS Visual Studio) для резервного копирования и восстановления БД.

Задание №1. необходимо создать резервные копии базы данных «МММ» с использованием полного резервного копирования, разностного резервного копирования и резервного копирования журнала транзакций.

Ход работы:

1. Запустите SQL Server Management Studio (SSMS), подключитесь к своему экземпляру SQL Server, используя технологию 1.
2. Создайте папку с именем [c:\Student\ВашаПапка\test](#).
3. Откройте окно нового запроса. Измените контекст на базу данных master, используя технологию 6. Наберите и исполните следующую команду, чтобы создать полную резервную копию базы данных:

BACKUP DATABASE MMM TO DISK = '[C:\.....TEST\AW.BAK](#)'

Ознакомьтесь с результатами запроса – какая информация обработана, сколько страниц, сколько файлов.

4. Внесите изменение в таблицу «Модель» базы данных MMM. Добавьте одну запись (придумайте сами)/
5. Откройте окно нового запроса наберите и исполните следующую команду, чтобы создать резервную копию журнала транзакций и сохранить только что внесенное изменение:

BACKUP LOG MMM TO DISK = 'C:\.....[TEST\AW1.TRN](#)'

Ознакомьтесь с результатами запроса – какая информация обработана, сколько страниц, сколько файлов.

6. Внесите еще одно изменение в таблицу «Модель».
7. Откройте окно нового запроса наберите и исполните следующую команду, чтобы создать разностную резервную копию базы данных:

BACKUP DATABASE MMM TO DISK = 'C:\.....[TEST\AWDIFF1.BAK](#)' WITH DIFFERENTIAL

Ознакомьтесь с результатами запроса – какая информация обработана, сколько страниц, сколько файлов.

8. Внесите еще одно изменение в таблицу «Модель».
9. Откройте окно нового запроса наберите и исполните следующую команду, чтобы создать полную резервную копию базы данных в указанном месте на диске:

BACKUP LOG MMM TO DISK = 'C:\....[TEST\AW2.TRN](#)'

Ознакомьтесь с результатами запроса – какая информация обработана, сколько страниц, сколько файлов.

Задание №2. необходимо провести восстановление базы данных «MMM» из сделанных в задании №1 резервных копий.

Ход работы:

1. Если необходимо, запустите SSMS, подключитесь к своему экземпляру SQL Server, используя технологию 1.
2. Выполните восстановление БД из первой полной резервной копии (C:\...TEST\AW.BAK) средствами оболочки SSMS. Для этого выполните:
  - В обозревателе объектов вызовите контекстное меню на вашей БД и выберите задачу восстановления базы данных (см. рисунок 6).

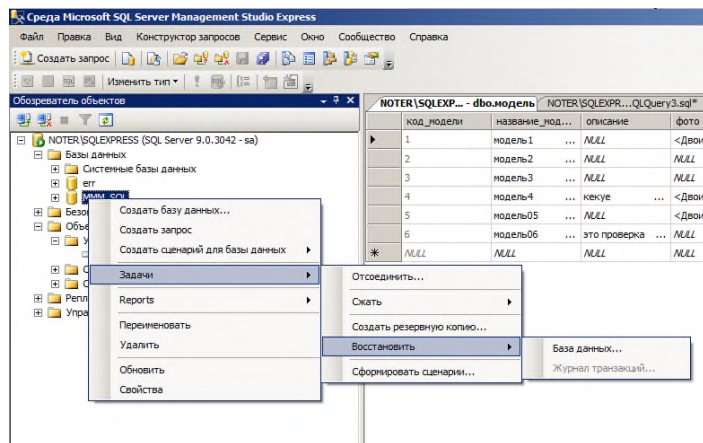


Рисунок 6 – Восстановление БД

- В открывшемся окне необходимо задать следующие параметры восстановления  
На закладке «Общие» необходимо выбрать:
  - а. Базу данных для восстановления (вашу МММ)
  - б. Выбрать источник набора данных для восстановления с устройства → файл C:\...TEST\AW.BAK
  - с. После определения файла-источника данных необходимо флажком выбрать базу данных для восстановления (рисунок 7).

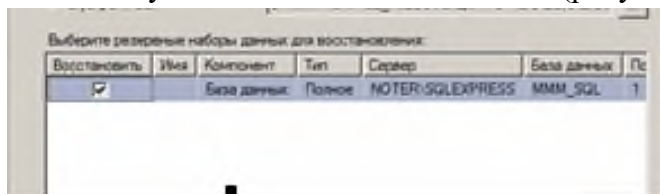


Рисунок 7- Выбор БД для восстановления

На закладке «Параметры»

- а. необходимо включить опцию «Перезаписать БД» и «оставить БД готовой к использованию», (рисунок 8).

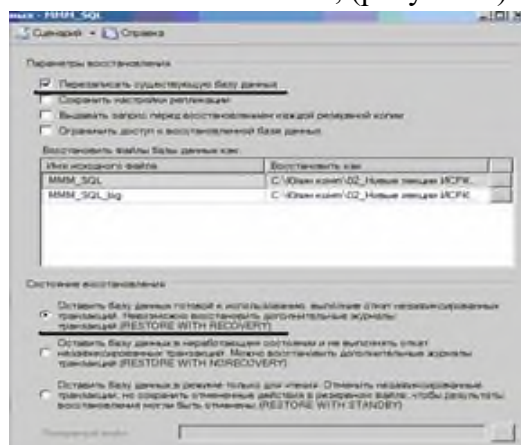


Рисунок 8 – Задание параметров восстановления

3. Нажмите ОК
4. После восстановления БД, откройте таблицу «Модель» и убедитесь, что она не содержит всех добавлений, вносимых вами в процессе выполнения упражнения, так как восстановление происходило из первой резервной копии (без изменений).

Задание №3. необходимо организовывать со стороны клиентского приложения, созданного в Visual Studio удаленное администрирование БД (резервное копирование).

Ход работы:

В Visual Studio

1. Создайте новый проект Windows Application и сохраните его в своей папке под именем Лабы\_МММ\_2 семестр.
2. В главную форму добавьте меню, изображенное на рисунке 9:

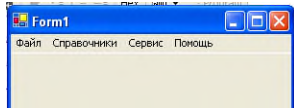


Рисунок 9 – Главное меню проекта

Файл (Открыть, Закрыть, Выход)

Справочники (Модель, Магазин, Дерево моделей)

Заказы (Работа с заказами)

Отчеты (Прайс-лист, Бланк заказов)

Администрирование БД (Резервное копирование, Безопасность)

Сервис (Калькулятор)

Помощь (Справка, О программе)

3. Добавьте новую форму в проект
4. Добавьте на только что созданную форму компоненты в соответствии с рисунком 10.

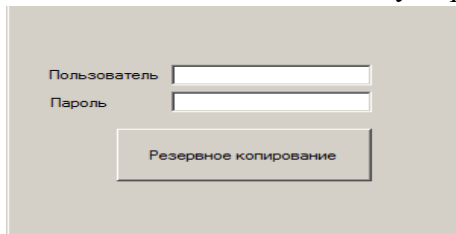


Рисунок 10 – Форма для подключения к серверу

5. Обеспечьте функциональную работу формы (напишите обработчик кнопки «Резервное копирование» с использованием объектов SMO. Описание объектов SMO, их свойств и методов см. в лекционном материале.)
6. Добавьте возможность открытия данной формы при выборе в главной форме пункта меню Администрирование БД → Резервное копирование
7. Запустите проект, проверьте работу формы.
8. Закройте проект
9. Убедитесь в появлении файла резервной копии на диске (файл, который указан в тексте программы).
10. Откройте SSMS. Добавьте в таблицу «Модель» новую строку данных (самостоятельно).
11. Средствами оболочки SSMS, выполните восстановление БД из резервной копии, созданной вашей программой
12. Убедитесь, что после восстановления добавленных строк в таблице «Модель» нет.

Задание №4. Ответьте на вопросы теста и представьте результаты преподавателю.

1. Вы выполняете разностное резервное копирование базы данных AdventureWorks каждые четыре часа, начиная с 04:00. полная резервная копия создается в полночь. Какие данные будут содержаться в разностной резервной копии сделанной в полдень?
  - a. А Страницы данных, измененные после полуночи.
  - b. В. Экстенды, измененные после полуночи.
  - c. С. Страницы данных, измененные после 08:00

- d. D. Экстенты, измененные после 08:00.
2. Вы выполняете полное резервное копирование базы данных Adventure Works, которое завершается в полночь. Разностное резервное копирование выполняется по расписанию каждые четыре часа, начиная с 04:00. Резервное копирование журнала транзакций происходит по расписанию каждые пять минут. Какую информацию будет содержать резервная копия журнала транзакций, созданная в 09:15?
- a. A. Все транзакции, начатые после 09:10.
  - b. B. Транзакции, завершённые после 09:10.
  - c. C. Страницы, изменённые после 09:10.
  - d. D. Экстенты, изменённые после 09:10.

Практическое занятие «Восстановление носителей информации» и «Восстановление удалённых файлов»

Цель работы: Изучить теоретические сведения и получить практический опыт настройки программы восстановления данных системы в Windows Server 2003.

#### Общие положения

Архивирование данных производится по двум основным причинам: для промежуточного сохранения записей и для сохранения файлов, необходимых при восстановлении системы после сбоя. Сохранение файлов, в зависимости от их назначения, имеет особенности. Все файлы можно разделить на системные и файлы данных. Системные файлы – это файлы, которые не изменяются в процессе работы информационной системы или изменяются, если изменяются версии приложений или операционных систем. Они могут архивироваться достаточно редко. Файлы данных, как правило, изменяются достаточно часто. К ним относятся файлы, созданные в текстовых редакторах, файлы баз данных, файлы электронных таблиц, файлы конфигурации (системный реестр, базы данных DHCP, DNS) и т.д. Указанные файлы требуют более частого архивирования.

Существует несколько типов архивирования, применение которых определяется тем, что копируется и как часто это производится.

1. “Архивное” архивирование. При данном архивировании в файлах заголовка, метках и записях указывается состояние бита архива, устанавливаемое в процессе копирования данных. Бит архива – это флаг, отражающий факт изменения данных. Состояние этого бита – “включен” (логическая 1) или “выключен” (логический 0) – указывает программам архивирования, что со времени последней такой операции файл соответственно был или не был изменен.
2. Копирующее архивирование. Это выполняемое “по случаю” копирование, при котором игнорируется состояние бита архива. Кроме того, после выполнения копирования бит архива не устанавливается. Такой вид архивирования полезен для быстрого получения копий в промежутках между процессами аварийно-восстановительных работ.
3. Ежедневное архивирование. Это простое архивирование файлов в тот же день, когда они были изменены. Такое архивирование возможно, когда объем изменяемых за день файлов невелик.
4. Стандартное архивирование. Это полное архивирование всех файлов, которое выполняется периодически. Полным называется архивирование, выполняемое в циклах по поддержанию готовности к аварийно-восстановительным работам. Во время полного архивирования копируются все файлы, а затем устанавливается бит архива, чтобы показать, что получены резервные копии файлов. Копирование и формируемая в его

процессе сопровождающая документация – единственные средства, позволяющие выполнить последующие операции добавочного или разностного архивирования.

5. Добавочное (дифференцированное) архивирование. Это архивирование всех файлов, которые были изменены со времени последнего полного или добавочного архивирования. При этом также устанавливается бит архива, который указывает на то, что выполнено архивирование данных. При применении схемы последовательного сохранения нескольких добавочных резервных копий для полного восстановления данных требуется использование всех носителей, на которых размещены последняя полная и все добавочные резервные копии.
6. Разностное архивирование. Работает точно так же, как и добавочное архивирование, за исключением того, что с архивным битом ничего не делается. Другими словами, файлы, прошедшие архивирование, не отмечаются.

Программа архивации помогает защитить данные от случайной утери в случае, если в системе возникнет сбой оборудования или носителя. Например, с помощью программы архивации можно создать резервную копию данных на жестком диске, а затем создать архив на другом устройстве хранения данных. Носителем архива может быть логический диск (например, жесткий диск), отдельное устройство (такое как съемный диск) или целая библиотека дисков или лент, управляемая сменщиком Robotic. При случайном удалении или замене исходных данных на жестком диске из-за его сбоя данные могут быть легко восстановлены из архивной копии.

Двумя наиболее распространенными задачами являются архивация файлов в файл или на ленту и восстановление файлов из файла или с ленты. Также можно архивировать данные из командной строки.

Чтобы защитить систему от серьезного сбоя, можно использовать средство архивации, чтобы регулярно создавать набор аварийного восстановления системы (ASR). Мастер аварийного восстановления системы создает архивацию, состоящую из двух этапов, которую можно использовать для восстановления системы после всех других неудачных попыток восстановления или после замены жесткого диска. ASR архивирует состояние системы, системные службы и все диски, связанные с компонентами операционной системы. Кроме того, он создает загрузочный диск, содержащий сведения об архивации, конфигурациях дисков (включая базовый и динамический тома) и инструкции по выполнению восстановления. Необходимо создавать новый набор ASR после любого значительного изменения в системе, а также регулярно в качестве части полного плана архивации.

Некоторыми наиболее распространенными задачами являются создание набора аварийного восстановления системы с помощью программы архивации и восстановление системы после сбоя с использованием средства аварийного восстановления системы.

Восстановление данных. Восстановлением называется процедура, которая выполняется для перемещения на жесткие диски компьютера вместо потерянного или испорченного файла, или набора файлов их работающей копии из архивных (резервных) данных.

При восстановлении используются следующие основные модели:

- простое восстановление,
- полное восстановление,
- массовое восстановление.

В простой модели восстановления данные могут быть восстановлены только на



момент последнего резервного копирования. Эта модель обеспечивает высокую эффективность выполнения массовых операций загрузки данных. Как следует из названия, простая модель копирования и восстановления наиболее легкая и удобная по сравнению с другими моделями. Максимально возможный объем данных, которые могут быть потеряны, определяется периодом времени между созданиями резервных копий.

В модели полного восстановления данные могут быть восстановлены в том виде, в котором она находилась вплоть до аварии. Модель поддерживает восстановление до контрольной точки, помеченной именованной транзакцией. Транзакция – это некоторое законченное, с точки зрения пользователя, действие в информационной системе. В модели полного восстановления массовые операции импорта протоколируются в журнал транзакций и, следовательно, могут быть полностью или частично восстановлены.

В модели массового восстановления операции импорта протоколируются в минимальном объеме. Это обеспечивает высокую производительность массовых операций загрузки, однако делает невозможным восстановление на любой заданный момент времени.

В зависимости от интервала времени, затрачиваемого на воссоздание информации, восстановление подразделяется на следующие виды.

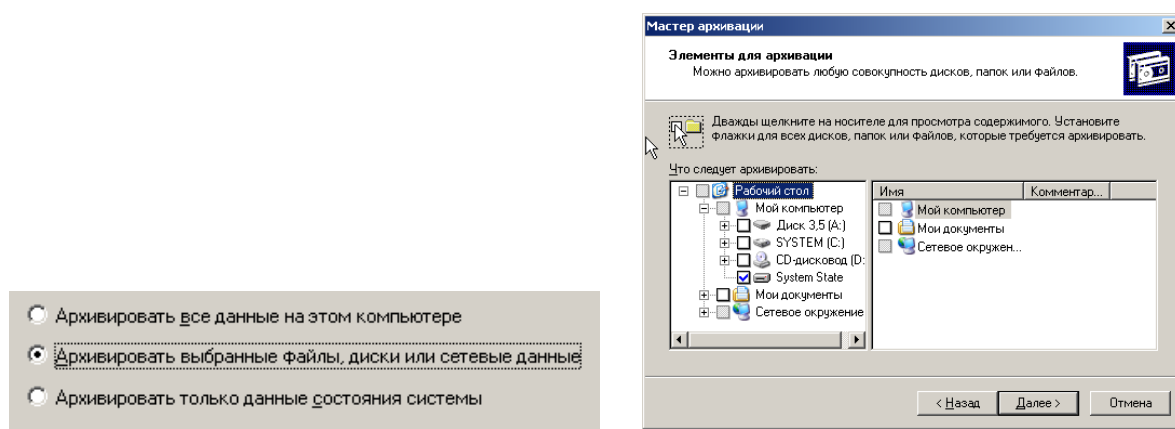
1. Восстановление в реальном времени (то есть сразу) или достаточно близко к нему. Данные, созданные не более чем несколько секунд назад, должны быть немедленно доступны пользователям и системам, даже если источник этих данных отключен. Это касается промышленных и медицинских систем, в которых задержка, определяемая восстановлением, допускается в течение долей и единиц секунд. Уровень времени в несколько секунд называется уровнем критического восстановления.
2. Если восстановление требуется в течение десяти минут, пока отключен первоначальный источник, то такое восстановление называется экстренным восстановлением.
3. Когда на восстановление можно затратить один час, оно называется срочным восстановлением.
4. Восстановление, требующее от одного до четырех часов, называется важным восстановлением.
5. Все другие восстановления, которые выполняются за интервал времени, больший предыдущих, называются небрежными.

#### Архивирование и восстановление состояния системы

Есть два варианта архивирования системных данных — архивирование состояния системы (System State) и создания набора для автоматического восстановления системы после аварии (Automated System Recovery).

- Архивирование и восстановление состояния системы

Для создания резервной копии состояния системы необходимо в утилите резервного копирования ntbackup при создании задания на архивирования отметить галочкой пункт



System State:

При этом будут архивироваться следующие данные:

- системный реестр;
- база данных зарегистрированных классов объектов (Class Registration);
- системные загрузочные файлы;
- база данных служб сертификатов (только на серверах, на которых установлена служба сертификатов);
- база данных Active Directory и папка SYSVOL (на контроллерах доменов).

Для архивирования состояния системы, а также для последующего восстановления, обязательно нужны права администратора данного компьютера. Восстановление Active Directory необходимо выполнять только при загрузке системы в режиме восстановления служб каталогов (запуск меню выбора режимы загрузки операционной системы выбираются в начальный момент загрузки нажатием клавиши F8).

- Автоматическое аварийное восстановление системы

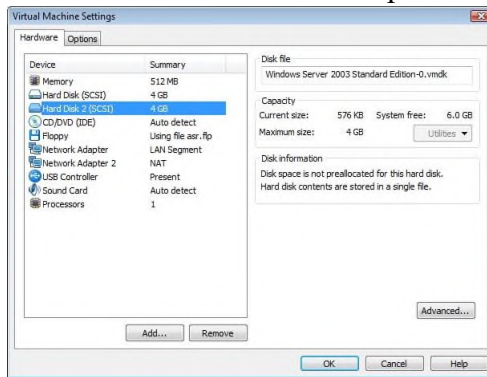
В отличие от резервного копирования состояния системы, при котором сохраняется только часть файлов операционной системы, резервное копирование для автоматического аварийного восстановления системы (ASR, Automated System Recover) архивирует больший объем информации — практически весь том, на котором установлена операционная система. И процедура восстановления системы становится более сложной.

- Создание ASR-копии

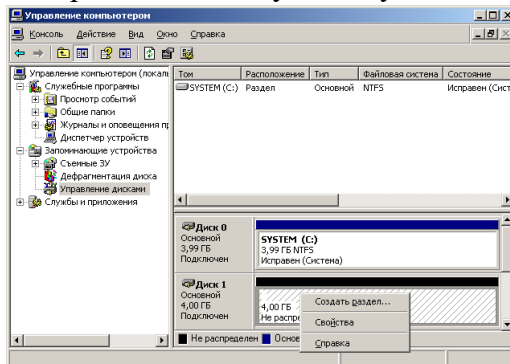
На данном этапе потребуется носитель для создания резервной копии системного тома (порядка нескольких гигабайт), причем в случае восстановления системы этот носитель должен быть доступен мастеру установки операционной системы (т.е. это либо ленточный накопитель с драйверами для контроллера и накопителя, либо дисковый накопитель с соответствующими драйверами), а также чистая отформатированная дискета для сохранения информации о конфигурации резервной копии.

1. Выберем вариант хранения данных на дополнительном дисковом накопителе. Для этого выполним следующие действия:
- Завершим работу нашего сервера;

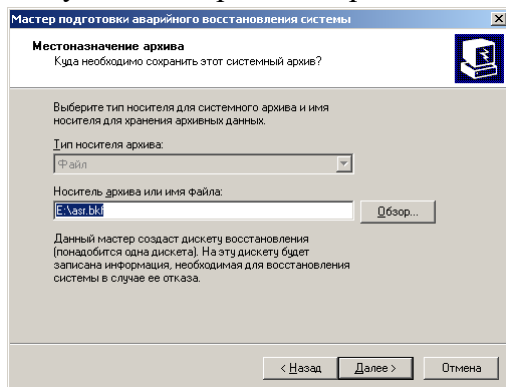
- В настройках данной ОС добавим новый SCSI-винчестер объемом 4Gb;



- Запустим ОС.
- Нажмем правой клавишей мыши на «Мой компьютер» и вызываем «Управление»;
- В управлении дисками инициализируем новый диск;
- Создаем на нем основной NTFS раздел по всему объему диска.



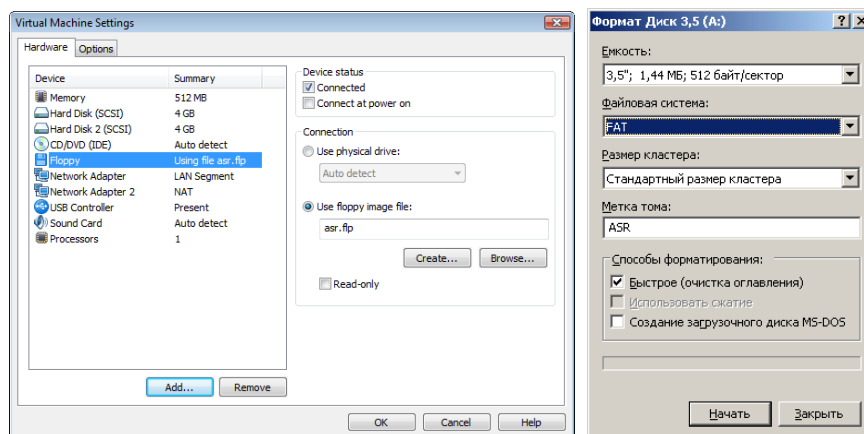
- Запустим утилиту резервного копирования ntbackup.
- Запустим «Мастер аварийного восстановления системы».
- Укажем путь для сохранения архива.



- Нажмем кнопку «Готово». Утилита резервного копирования начнет создание резервной ASR-копии, в нужный момент будет сделан запрос вставить чистую дискету.

Работа с дисководом в WMware имеет определенную специфику. Будем использовать виртуальную дискету. Для этого в свойствах ОС сервера в WMware выберем дискету, выберем

«Использовать образ дискеты» и нажмем «Создать». Перед использованием дискеты отформатируйте ее.



После записи конфигурации резервной копии утилита попросит пометить дискету соответствующей информацией (название резервной копии и дата создания).

### Архивация файлов в файл или на ленту

Чтобы запустить архивацию, нажмите кнопку Пуск и выберите команды Все программы, Стандартные, Служебные и Архивация данных.

По умолчанию программы архивации и восстановления запускаются в режиме мастера (рис.1.), если этот режим не отключен. Имеется возможность использовать этот мастер или перейти на следующем шаге в Расширенный режим.

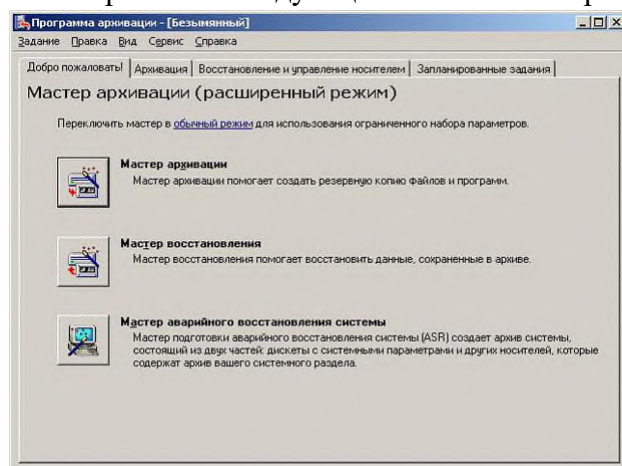


Рис. 1- Окно «Добро пожаловать»

Щелкните ссылку «Расширенный режим» в окне мастера архивации или восстановления.

Выберите вкладку Архивация, а затем в меню Задание выберите команду Создать.

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

В списке Место назначения архива выберите один из вариантов.

- Для архивации файлов или папок в файл выберите пункт Файл. Этот вариант выбран по умолчанию.
- Для архивации файлов и папок на ленту выберите накопитель на магнитной ленте. В поле Носитель архива или имя файла выполните одно из действий.
- Для архивации файлов и папок в файл введите путь и имя файла архива (.bkf) или нажмите кнопку Обзор, чтобы найти его.
- Для архивации файлов и папок на ленту выберите требуемую ленту.

Задайте параметры архивации — тип архива и тип файла журнала, выбрав в меню

Сервис команду Параметры. После этого нажмите кнопку ОК.

Нажмите кнопку Архивировать и внесите изменения в диалоговом окне Сведения о задании архивации.

Чтобы задать дополнительные параметры архивации, например, проверку данных или аппаратное сжатие, нажмите кнопку Дополнительно. Установив дополнительные параметры архивации, нажмите кнопку ОК.

Чтобы начать архивацию, нажмите кнопку Архивировать. Примечания:

- Для выполнения этой процедуры необходимо входить в группу Администраторы или Операторы архива на локальном компьютере или получить соответствующие полномочия путем делегирования. Если компьютер присоединен к домену, эту процедуру могут выполнять члены группы Администраторы домена. При этом по соображениям безопасности рекомендуется использовать команду Запуск от имени.
- Чтобы запустить архивацию, нажмите кнопку Пуск и выберите команды Все программы, Стандартные, Служебные и Архивация данных.
- Если мастер архивации или восстановления не запускается по умолчанию, для его использования выберите на вкладке Добро пожаловать! команду Режим мастера.
- Некоторые накопители на магнитной ленте могут не поддерживать аппаратное сжатие.
- Данные о состоянии системы включают большинство элементов конфигурации системы, но это не все сведения, которые могут потребоваться для восстановления системы после сбоя. Поэтому при архивации системы рекомендуется создавать резервные копии всех загрузочных и системных томов, включая данные о состоянии системы.
- Архивация данных о состоянии системы возможна только для локального компьютера. Данные состояния системы для удаленного компьютера архивировать нельзя.
- Файлы архива обычно имеют расширение .bkf. Можно использовать любое расширение, но рекомендуется использовать расширение .bkf, которое имеет сопоставления файлов, что обеспечит распознавание файла архива.
- Операторы архива и администраторы могут архивировать и восстанавливать зашифрованные файлы и папки, не расшифровывая их.

Восстановление файлов из файла или с ленты

Запустите приложение Архивация.

По умолчанию программы архивации и восстановления запускаются в режиме мастера, если этот режим не отключен.

Щелкните ссылку «Расширенный режим» в окне мастера архивации или восстановления.

Выберите вкладку Восстановление и управление носителем и в списке Установите флажки для всех объектов, которые вы хотите восстановить установите флажки для тех файлов и папок, которые требуется восстановить.

В списке Восстановить файлы выберите один из вариантов.

- Исходное размещение, если необходимо восстановить файлы и папки из архива в папку (или папки), где они находились до архивации. Перейдите к шагу 6.
- Альтернативное размещение, если необходимо восстановить файлы и папки из архива в указанную папку. Этот параметр позволяет сохранить структуру папок архивных данных. Все архивные папки и подпапки появятся в указанной дополнительной папке.
- Единственная папка, если необходимо восстановить файлы и папки из архива в указанную папку. При выборе этого параметра структура папок архивных данных не сохраняется.

Файлы будут восстановлены только в указанной папке.

Если выбран вариант Альтернативное размещение или Единственная папка, введите в поле Альтернативное размещение путь к нужной папке или нажмите кнопку Обзор, чтобы найти ее.

В меню Сервис выберите команду Параметры, перейдите на вкладку Восстановление и выполните одно из действий.

- Если в ходе восстановления не следует заменять файлы, уже имеющиеся на жестком диске, выберите вариант Не заменять файл на компьютере.
- Если в ходе восстановления требуется заменить старые файлы на диске новыми файлами из архива, выберите вариант Заменять файл на компьютере, только если он старше.
- Если в ходе восстановления требуется заменять файлы на локальном диске независимо от того как датированы файлы в архиве, выберите вариант Всегда заменять файл на компьютере.
- Нажмите кнопку ОК, чтобы принять заданные параметры восстановления. Нажмите кнопку Восстановить.

Если требуется изменить дополнительные параметры восстановления, например восстановление параметров безопасности и данных о точках соединений, нажмите кнопку Дополнительно. Завершив задание дополнительных параметров, нажмите кнопку ОК.

Нажмите кнопку ОК, чтобы начать восстановление. Внимание!

- Если выбран вариант Всегда заменять файл на компьютере, то при наличии в архиве текущего рабочего файла соответствующий файл на диске может быть заменен, а его данные утеряны.
- Программа архивации позволяет архивировать и восстанавливать данные томов FAT16, FAT32 и NTFS. Данные, полученные с тома NTFS, рекомендуется восстанавливать на томе NTFS той же версии, чтобы не допустить их потери. Некоторые файловые системы могут поддерживать не все возможности других файловых систем.

Примечания:

- Для выполнения этой процедуры необходимо входить в группу Администраторы или Операторы архива на локальном компьютере или получить соответствующие полномочия путем делегирования. Если компьютер присоединен к домену, эту процедуру могут выполнять члены группы Администраторы домена. При этом по соображениям безопасности рекомендуется использовать команду Запуск от имени.
- Чтобы запустить архивацию, нажмите кнопку Пуск и выберите команды Все программы, Стандартные, Служебные и Архивация данных.
- Восстановить файлы также можно с помощью мастера восстановления, выбрав в меню Сервис команду Мастер восстановления.
- Для архивации и восстановления файлов базы данных Microsoft SQL Server рекомендуется использовать встроенные служебные программы архивации и восстановления SQL.
- Для восстановления данных состояния системы контроллера домена необходимо предварительно запустить компьютер в режиме восстановления службы каталогов. Это позволит восстановить каталог SYSVOL и базу данных службы каталогов Active Directory.
- Восстановление данных состояния системы возможно только на локальном компьютере. Восстановить данные состояния системы на удаленном компьютере нельзя.
- Операторы архива и администраторы могут архивировать и восстанавливать зашифрованные файлы и папки, не расшифровывая их.

Создание набора аварийного восстановления системы с помощью программы

архивации

Запустите приложение Архивация.

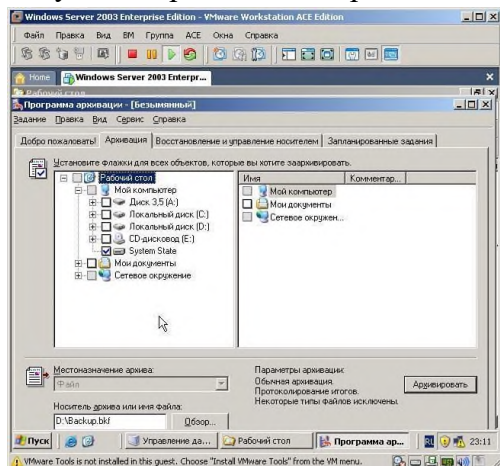


Рис. 2. Окно программы архивации вкладка «Архивация»

По умолчанию программы архивации и восстановления запускаются в режиме мастера, если этот режим не отключен. Можно использовать мастер архивации или мастер восстановления для создания набора аварийного восстановления системы (ASR), выбрав Всю информацию на данном компьютере в разделе Выберите объекты, которые следует архивировать. Иначе, можно перейти к следующему шагу, чтобы создать набор ASR, используя Расширенный режим.

Щелкните ссылку «Расширенный режим» в окне мастера архивации или восстановления.

В меню Сервис выберите команду Мастер аварийного восстановления системы. Следуйте инструкциям, появляющимся на экране.

Внимание! Необходимо иметь наготове дискету емкостью 1,44 Мбайт для сохранения параметров системы и носитель для хранения файлов архива.

Примечания:

- Для выполнения этой процедуры необходимо входить в группу Администраторы или Операторы архива на локальном компьютере или получить соответствующие полномочия путем делегирования. Если компьютер присоединен к домену, эту процедуру могут выполнять члены группы Администраторы домена. При этом по соображениям безопасности рекомендуется использовать команду Запуск от имени.
- В ходе выполнения этой процедуры будут заархивированы только системные файлы, необходимые для запуска операционной системы. Данные следует архивировать отдельно.
- После создания набора ASR следует пометить эту дискету и носитель архива и хранить их вместе. Чтобы использовать носитель архива, необходимо иметь дискету, которая была создана вместе с набором носителей. Невозможно использовать дискету, созданную в другое время или с другим набором носителей. Также для выполнения аварийного восстановления системы следует иметь установочный компакт-диск.
- Следует хранить набор ASR в безопасном месте. Набор ASR содержит сведения о конфигурации системы, которые можно использовать для причинения вреда системе.
- Если производится архивация кластера серверов, запустите мастер подготовки аварийного восстановления системы на всех узлах кластера и убедитесь, что служба кластеров работает при создании каждого архива ASR. Убедитесь, что один из узлов, на котором запущен мастер подготовки аварийного восстановления системы, является владельцем



ресурса кворума во время работы мастера.

Восстановление системы после сбоя с использованием средства аварийного восстановления системы

Перед началом процедуры восстановления убедитесь в наличии следующих элементов:

- предварительно созданной дискеты аварийного восстановления системы;
- предварительно созданного носителя архива;
- исходного установочного компакт-диска операционной системы;
- при наличии контроллера запоминающего устройства, для которого требуется отдельный файл драйвера (отличный от файлов, доступных с установочного компакт-диска), следует получить этот файл (на дискете) перед началом процедуры.

Вставьте исходный установочный компакт-диск операционной системы в CD-дисковод.

Перезагрузите компьютер. При появлении на экране приглашения нажать клавишу для загрузки с компакт-диска нажмите соответствующую клавишу.

Если имеется отдельный файл драйвера, как описано в шаге 1, используйте драйвер как часть программы установки, нажав клавишу F6 в ответ на соответствующее приглашение.

Нажмите клавишу F2 при появлении соответствующего приглашения в начале текстового этапа установки. Будет выведено приглашение вставить предварительно созданную дискету аварийного восстановления системы.

Следуйте указаниям, появляющимся на экране.

Если имеется отдельный файл драйвера, как описано в шаге 1, нажмите клавишу F6 (во второй раз) при появлении соответствующего приглашения после перезагрузки системы.

Следуйте указаниям, появляющимся на экране. Примечания:

- Наличие физического доступа к серверу снижает безопасность системы. Для создания более безопасной среды необходимо ограничить физический доступ ко всем серверам и сетевому оборудованию.
- При аварийном восстановлении системы файлы данных не восстанавливаются.
- При восстановлении кластера серверов, все узлы которого неисправны и диск кворума не может быть восстановлен из архива, следует использовать аварийное восстановление системы на каждом узле в исходном кластере для восстановления подписей дисков и разметки разделов дисков кластера (кворумные и некворумные).

Выполнение работы

Изучить возможности восстановления данных и работоспособности системы и ответить на вопросы:

1. Перечислите типы архивов резервного копирования данных.
2. Перечислите кнопки окна «Добро пожаловать» программы архивации.
3. Назовите варианты архивирования системных данных.
4. Какая информация представлена в отчете об архивации данных?
5. Какие основные причины отказа работоспособности системы?
6. Перечислите виды восстановления информации.
7. Опишите процедуру восстановления информации до момента сбоя в системе.

8. Почему достоверность информации, сохраняемой в копиях, зависит от интервала времени, через который производится архивирование?
9. Какая информация представлена в отчете о создании резервной копии состояния системы?

Практическое занятие «Мониторинг активности портов» и «Блокирование портов»

Цель работы: формирование умений и навыков блокировки и разблокировки портов подключения устройств

Основные положения

Понятие порта в компьютере многозначно. Самое общее определение: порт - это соединение (физическое или логическое), через которое принимаются и отправляются данные. Обмен данными между любыми устройствами возможен только при наличии утвержденного стандарта на интерфейс.

В состав аппаратного обеспечения порта входит специализированный разъём, предназначенный для подключения оборудования определённого типа. Часто этот специализированный разъём и называют портом, например USB-порт, но есть разъёмы, которые портами называть не принято, например, RJ11. Как правило, каждый порт имеет обозначение, которое размещается рядом с разъёмом.

Основные порты, используемые в компьютерах, ноутбуках:

- USB-порт;
- IEEE 1394 (FireWire) ;
- Порт eSATA и комбинированный порт USB/eSATA;
- Сетевой порт Ethernet;
- Порт SCSI;
- Последовательный порт RS-232;

· Порты для подключения внешних мониторов VGA, DVI, S-Video, HDMI, DisplayPort;

- Порт для док-станции и порт репликатор;
- Порты для модулей расширения PCMCIA, ExpressCard.

USB - Universal Serial Bus - универсальная последовательная шина. USB-порты являются своего рода стандартом для подключения внешних устройств, к которому стремятся все производители этих устройств. К портам USB подключаются: мыши, клавиатуры, принтеры, сканеры, модемы, кардридеры, флэш-накопители, фотоаппараты, сотовые телефоны, плееры, жёсткие диски, оптические дисководы и др.

IEEE 1394 - высокоскоростной последовательный порт для цифровых видеоустройств. Компания Apple продвигает стандарт IEEE 1394 под маркой FireWire, компания Sony – под маркой i.LINK. IEEE 1394 применяется для подключения видеокамер, цифровых фотоаппаратов и других мультимедийных устройств, а также принтеров, сканеров, внешних жестких дисков.

Основные преимущества по сравнению с USB 2.0 - более высокая скорость передачи, большая стабильность, большая длина кабеля до оконечного устройства.

eSATA - External Serial ATA (Advanced Technology Attachment - присоединение по передовой технологии) – последовательный интерфейс для подключения внешних устройств, поддерживающий режим «горячей замены». Стандарт eSATA предусматривает подключение внешних жестких дисков, оптических дисков, RAID-массивов. Скорость передачи данных гораздо выше, чем у USB 2.0 или IEEE 1394.

#### Недостатки eSATA:

- максимальная длина кабеля не превышает 2 метров;
- жёсткие диски, подключаемые через eSATA, потребуют дополнительного источника питания - это могут быть как разъёмы USB или 1394, так и розетка.

Порт Ethernet предназначен для подключения ноутбука к компьютерной сети с помощью сетевого кабеля через разъем RJ45 (RJ-45). Технология Ethernet описывается стандартами IEEE группы 802.3. Существует несколько стандартов технологии Ethernet. Стандарты различаются скоростью передачи данных и передающей средой. В ноутбуках обычно устанавливают порт Ethernet 10/100/1000, который поддерживает стандарты 10BASE-T, 100BASE-TX и 1000BASE-T для расстояний до 100 м. Стандарт 10BASE-T позволяет передавать данные со скоростью 10 Мбит/с. Для передачи используется 4 провода кабеля витой пары категории 3 или категории 5. По стандарту 100BASE-TX скорость передачи данных составляет 100 Мбит/с. Стандарт применяется для построения сетей топологии «звезда». Задействована витая пара категории 5, поддерживается дуплексная передача данных. Стандарт 1000BASE-T - гигабитный (Gigabit, Geth) Ethernet позволяет передавать данные со скоростью до 1 Гбит/с. Стандарт предусматривает использование витой пары категорий 5е.

RS-232 (англ. Recommended Standard) - стандарт последовательной асинхронной передачи двоичных данных между двумя устройствами на расстоянии до 15 метров. Порт RS-232 в последнее время не часто встречается в бизнес-ноутбуках, но может быть полезен в промышленных ноутбуках.

Он используется для реализации систем сбора данных в реальном времени, подключения научного ряда контактов. Карты Type III поддерживают 16- или 32-разрядный интерфейс. Они имеют толщину 10,5 мм, что позволяет устанавливать на карту стандартные разъёмы внешних интерфейсов и избавиться, таким образом, от дополнительных кабелей. Разъем имеет четыре ряда контактов. Разъем PCMCIA представляет собой щель шириной 54 мм, которая закрыта либо откидной шторкой, либо пластиковой заглушкой.

Разъем (слот) PCMCIA (вверху) и заглушка, внизу – кардридер.

Большинство ноутбуков оснащается лишь одним разъемом PCMCIA типа II. А современные ноутбуки уже обходятся и вовсе без этих разъемов.

Порт ExpressCard. Стандарт ExpressCard для карт расширения был разработан ассоциацией PCMCIA на смену стандарту PC Card. Новый стандарт был создан на базе новой скоростной последовательной шины PCI Express. Стандарт ExpressCard не только более производительный, чем PC Card, но и более универсальный. Через ExpressCard можно подключаться к шине USB. Карты ExpressCard бывают двух типов, отличающихся по ширине: 34 мм и 54 мм. Соответственно и разъёмы бывают двух типов ExpressCard/34 и ExpressCard/54. При этом карты 34 мм можно устанавливать как в разъем ExpressCard/34, так и в разъем ExpressCard/54. Через разъёмы ExpressCard подключают ТВ-тюнеры, звуковые карты, карты Wi-Fi, флеш-накопители (они часто подключаются через USB-составляющую интерфейса ExpressCard), модемы для работы в сотовых сетях и др.

Разъем RJ11(RJ-11 Registered jack) – разъем модема ноутбука. Используется для подключения к Интернету через модем по телефонной линии.

Сравнение средств мониторинга действий пользователей

Одной из важных особенностей современных корпоративных сетей является их размер, который зачастую исчисляется тысячами, а и иногда и десятками тысяч

компьютеров. При этом деятельность пользователей может быть распределена среди различных компьютеров, а одна и та же проблема часто решается группами пользователей. Важной задачей является контроль работы, как отдельных пользователей, так и групп пользователей.

Основными целями контроля являются: обеспечение информационной безопасности, выявление случаев некорректного, непрофессионального или нецелевого использования ресурсов, оценка характеристик функционирования корпоративной сети и параметров использования ресурсов.

Основной задачей обеспечения информационной безопасности является «раннее обнаружение» внутренних вторжений, т.е. выявление действий пользователей, которые могут предшествовать внутренним вторжениям. Чем крупнее организация, тем актуальнее является для нее проблема предотвращения внутренних вторжений, в частности кражи информации, так как именно кража является конечной целью большинства внутренних вторжений. Связано это с тем, что в больших организациях затрудняется контроль над обращением информации и существенно возрастает цена ее утечки. Указанные обстоятельства определяют высокий уровень озабоченности данной проблемой со стороны крупного бизнеса и правительственных организаций. Решение данной проблемы заключается в применении "жесткой" политики информационной безопасности в организации и использовании средств мониторинга действий пользователей.

#### Spector 360

Spector 360 включает в себя средства для автоматического развертывания и удаленного управления, осуществляет запись разнообразных действий, включая: Email, чаты, мгновенные сообщения, посещаемые веб-сайты, онлайн-поисковые запросы, нажимаемые клавиши и используемые программы. Spector 360 также включает в себя средство для записи образов экрана в режиме видеорекамера.

Все эти инструменты ведут запись одновременно, скрытно, под защитой тройного уровня безопасности. Приложение Recorder хорошо конфигурируется и может быть настроено для записи только интересующих Вас событий.

В дополнение к мониторингу и ведению записи Spector 360 обладает развитой системой определения и обнаружения ключевых слов, которая будет немедленно извещать о каждом случае, когда пользователь контролируемого ПК отклонится от допустимого использования ПК или Интернет.

Регистратор Spector 360 можно перевести в скрытый режим, который обеспечивает невозможность обнаружения программы неуполномоченными пользователями. В скрытом режиме Spector 360 не будет виден пользователю в системном меню задач, диспетчере задач или в меню установки/удаления программ панели управления.

При помощи Spector 360 вы можете сгенерировать высококачественные отчеты для руководства, которые могут регулярно распечатываться или рассылаться по почте.

Spector 360 разработан для коммерческих, образовательных и правительственных организаций, использующих сети на платформе Windows.

#### Security Curator

Security Curator – это система обеспечения информационной безопасности нового поколения, объединяющая в себе возможность наблюдения за деятельностью сотрудников, контроля их действий и блокировки потенциально опасных путей утечки информации.

Security Curator ведёт мониторинг в реальном времени практически всех действий сотрудников при работе за компьютером. Информация о действиях пользователей

обновляется в реальном режиме времени. При этом постоянно производится сохранение снимков экрана при совершении любых действий, также существует возможность наблюдения за рабочим столом пользователя в режиме он-лайн. В случае работы пользователем с USB-устройствами производится резервное копирование файлов.

Внедрение Security Curator позволяет ограничить доступ к нежелательным сайтам, программам и приложениям на определенный промежуток времени либо постоянно. Например, работодатель может разрешить сотрудникам посещать сайты ВКонтакте и Одноклассники только во время обеденного перерыва, а доступ к бухгалтерской программе 1С запретить после окончания рабочего дня и на выходных.

#### Activity Monitor

Этот мощный инструмент позволяет отслеживать любые действия в сети и предоставляет вам детальную информацию о том, что, как и когда делали ваши сотрудники. Будь то сеть библиотеки, университета или коммерческой организации, Activity Monitor поможет вам установить эффективный контроль над ней.

Приложение состоит из серверной и клиентской частей. Сервер Activity Monitor может быть установлен на любом компьютере в сети. Модуль-шпион (агент) устанавливается на всех компьютерах, действия на которых вы хотите отслеживать. Он может быть установлен даже удалённо с системы, на которой установлена серверная часть Activity Monitor.

Действия на сетевых компьютерах отслеживаются удалённо. Вы можете настроить программу таким образом, что она будет отслеживать и регистрировать действия на всех компьютерах в сети одновременно. Данные мониторинга могут быть использованы для более глубокого анализа и создания детальных отчётов.

Activity Monitor является эффективным средством повышения общей производительности труда в компаниях, использующих данную программу для мониторинга локальных сетей. Проще говоря, этот мощный инструмент от Softactivity экономит ваши деньги.

#### NetVizor

NetVizor — Программа для мониторинга сети. NetVizor позволяет наблюдать за всей локальной сетью из одного рабочего места. Программа может следить за рабочими станциями и индивидуальными пользователями, которые используют различные компьютеры, находящимся в сети.

Программа позволяет следить за сетевыми компьютерами, осуществлять фильтрацию контента и управлять сетевыми компьютерами дистанционно.

Существует возможность ведения журналов адресов посещенных сайтов, соединений с интернетом, открываемых файлов, чатов, пересылаемых сообщений электронной почты и так далее. NetVizor также обезвреживает шпионские программы и помогает следить за безопасностью.

Мониторинг	Spector 360	Security Curator	Activity Monitor	Net Visor
Экран	+	+	+	+
Снимки экрана	+	+	+	+

Запущенные процессы	+	+	+	+
Время запуска и выключения программ	+	+	+	+
Бесплатные сервисы электронной почты	+	-	+	+
Нажатие клавиш	+	+	+	+
E-mail	+	+	+	+
Посещенные сайты	+	+	+	+
Переписка в IM агентах	+	+	+	+
Социальные сети	+	+	+	+
Поисковые запросы	+	+	+	+
USB устройства	+	+	+	-
Обнаружение ключевых слов	+	-	-	+
Установка, удаление программ	+	+	+	+
Контроль рабочего времени	+	+	+	+
Загружаемые файлы	+	+	+	+
Доступ к файлам, папкам	+	+	+	+
Активность пользователя	+	+	+	+
FTP	+	+	+	+
Сетевые соединения	+	+	+	+

Выборочный мониторинг	+	+	+	+
Запись по расписанию	+	+	+	+
Контроль	Spector 360	Security Curator	Activity Monitor	Net Visor
Блокировка событий (запуск приложений, сайты, запрет файловых операций)	-	+	+	+
Блокировка запуска любых процессов	-	+	+	+
Блокировка подключения/отключения всех типов USB накопителей и устройств	-	+	-	-
Блокировка сетевых соединений (по порту, ip адресу)	+	+	+	+
Блокировка сайтов по домену	+	+	+	+
Блокировка чатов и Интернет пейджеров	+	+	+	+
Блокировка доступа в Интернет по протоколу или порту	+	+	+	+
Запрет действий с файлами/папками	-	+	+	+
Отчетность	Spector 360	Security Curator	Activity Monitor	Net Visor
Генерация отчетов с привязкой к отдельному пользователю	+	+	+	+
Поиск по ключевым словам	+	+	+	+
Генерация графических отчетов	+	+	+	+
Конвертация отчетов в PDF	+	+	-	+
Конвертация отчетов в HTML	+	+	+	+
Конвертация отчетов в CSV	+	+	+	+
Конвертация отчетов в Excel	+	-	+	-



Конвертация отчетов в Rich Text	+	-	-	-
Экспорт отчетов	+	-	-	-
Отправка отчетов по электронной почте	+	+	-	+
Отправка отчетов по FTP	+	+	-	-
Печать отчетов	+	+	+	+
Генерация отчетов по расписанию	+	+	-	-
Управление	Spector 360	Security Curator	Activity Monitor	Net Visor
Централизованное управление клиентами	+	+	+	+
Централизованное управление лицензиями	+	+	+	+
Централизованное конфигурирование безопасности	+	+	+	+
Централизованное конфигурирование сети	+	-	-	-
Централизованное конфигурирование WEB- фильтра	+	+	+	+
Резервирование и восстановление базы данных	+	-	-	-
Управление резервными копиями	+	-	-	-
Многопользовательский дискреционный контроль доступа к данным	+	-	-	+
Разделение доступа к функциям администрирования	+	-	-	+
Возможность группировки компьютеров	+	+	+	+
Возможность группировки пользователей	+	-	+	-
Безопасность	Spector 360	Security Curator	Activity Monitor	Net Visor

Контроль компьютеров в сети	+	+	+	+
Удаленная установка	+	+	+	+
Невидимый режим работы	+	+	-	+
Авторизация при запуске административного модуля	+	+	+	+
Стоимость	Spector 360	Security Curator	Activity Monitor	Net Visor
Цена за 1 лицензию (от 5 до 99 хостов)	~ 5200 руб.	~ 1800 руб.	~ 1400 руб.	~ 1600 руб.
Цена за 1 лицензию (от 100 до 249 хостов)	~ 4000 руб.	~ 1600 руб.	~ 700 руб.	~ 1100 руб.
Цена за 1 лицензию (от 250 до 1000 хостов)	~3500 руб.	~1500 руб.	~600 руб.	~200 руб.

Определенно, Spector 360 незаменим в крупных организациях, где решаются задачи оперативного мониторинга огромного количества рабочих станций.

Если делать акцент на возможность контроля и блокировки действий пользователей, тут подойдет Security Curator, NetVisor и Activity Monitor.

Рассмотрим два способа улучшения безопасности работы сети.

Шаг 1. Меняем учетную запись администратора (Пользователь Администратор с пустым паролем — это уязвимость) (убираем уязвимость 1)

При установке Windows XP в автоматическом режиме с настройками по умолчанию мы имеем пользователя Администратор с пустым паролем и любой User может войти в такой ПК с правами администратора. Чтобы решить проблему выполним команду Мой компьютер-Панель управления-Администрирование-Управление компьютером- Локальные пользователи-Пользователи (рис. 1).

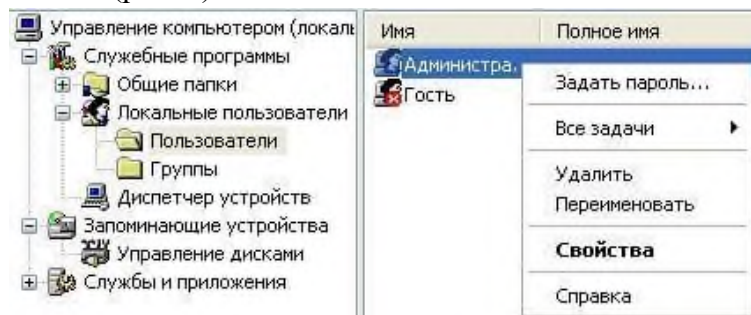


Рис. 1 - Окно Управление компьютером

Здесь по щелчку правой кнопкой мыши на Администраторы зададим администратору пароль, например, 12345. Теперь в окне Администрирование зайдем в Локальную политику безопасности. Далее идем по веткам дерева: Локальные политики-Параметры безопасности-Учетные записи: Переименование учетной записи Администратор (рис..2).

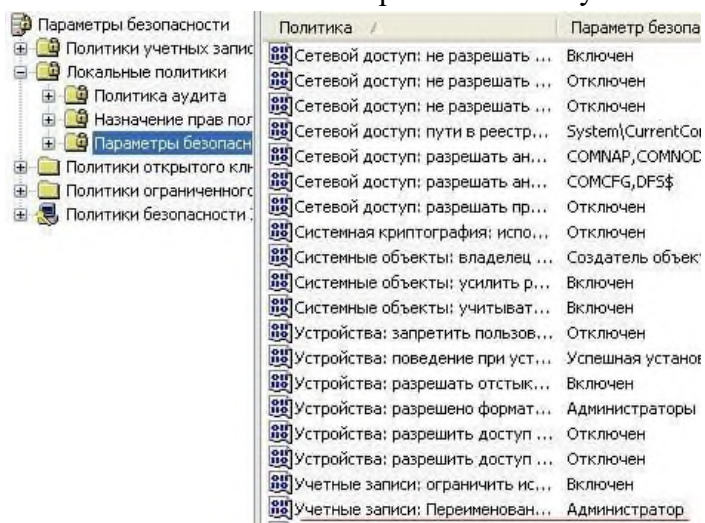


Рис. 2 - Находим в системном реестре запись Переименование учетной записи Администратор

Здесь пользователя Администратор заменим на Admin (рис. 3).

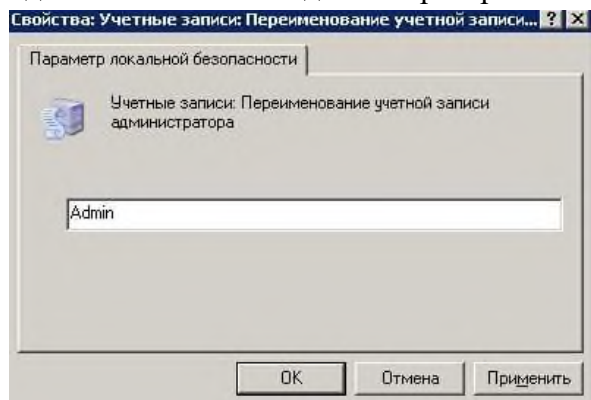


Рис. 3 - Пользователю Администратор присваиваем новое имя

Перезагружаем ОС. После наших действий получилась учетная запись Admin с паролем 12345 и правами администратора (рис. 4).

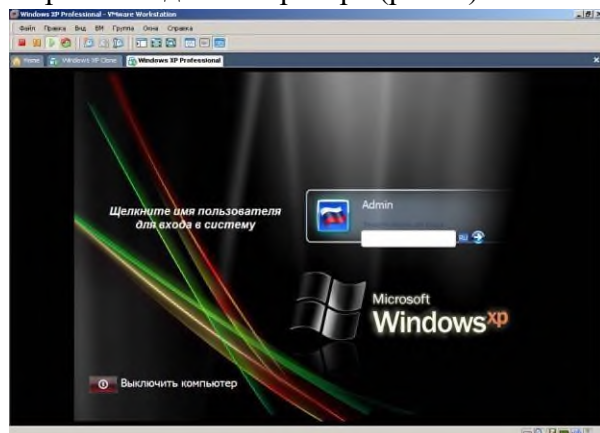


Рис. 4 - Окно входа в ОС Windows XP

Все, теперь мы имеем пользователя Администратор с паролем, одна из уязвимостей системы устранена.

Операцию по изменению имени пользователя и заданию пароля мы также могли бы выполнить без использования системного реестра, используя окно Учетные записи пользователей, что гораздо проще (рис. 5).

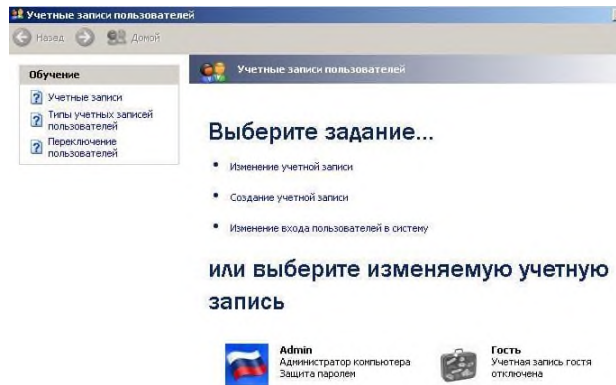


Рис. 5 - Окно Учетные записи пользователей

#### Примечание

Учетная запись Гость позволяет входить в ПК и работать на нем (например, в Интернет) без использования специально созданной учетной записи. Запись Гость не требует ввода пароля и по умолчанию заблокирована. Гость не может устанавливать или удалять программы. Эту учетную запись можно отключить, но нельзя удалить.

Шаг 2. Делаем окно приветствия пустым (убираем уязвимость 2)

У нас окно входа в систему содержит подсказку Admin, давайте ее уберем, сделав окно пустым. Для начала в окне Учетные записи пользователей жмем на кнопку Изменение входа пользователей в систему и уберем флажок Использовать страницу приветствия (рис. 6 и рис. 7).

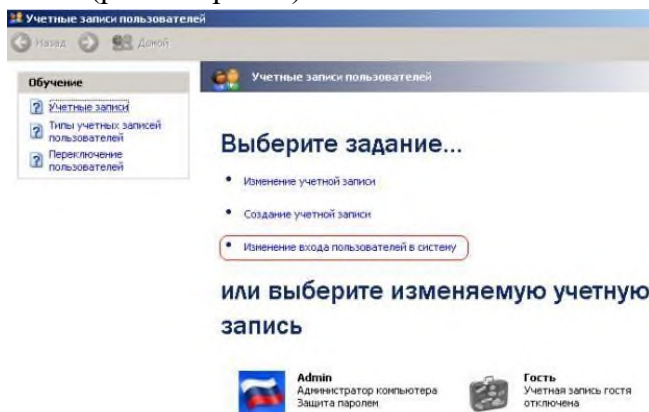


Рис. 6 - Окно Учетные записи пользователей

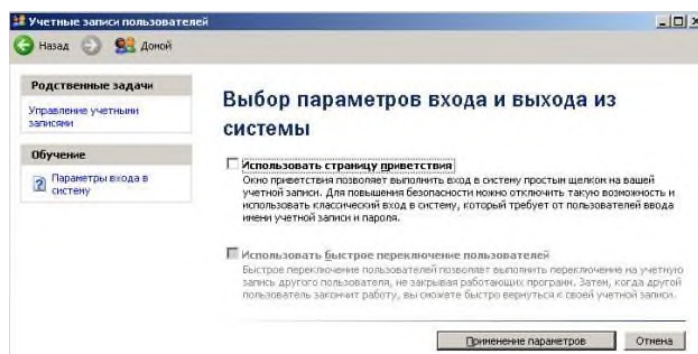


Рис. 7 - Убираем флажок Использовать страницу приветствия

Теперь повысим безопасность сети еще на одну условную ступень, сделав оба поля окна приветствия пустыми (рис. 8).



Рис. 8 - Обе строки данного окна сделаем пустыми

Выполним команду Панель управления - Администрирование – Локальные политики безопасности - Локальные политики - Параметры безопасности - Интерактивный вход: не отображать последнего имени пользователя. Эту запись необходимо включить (рис. 9).

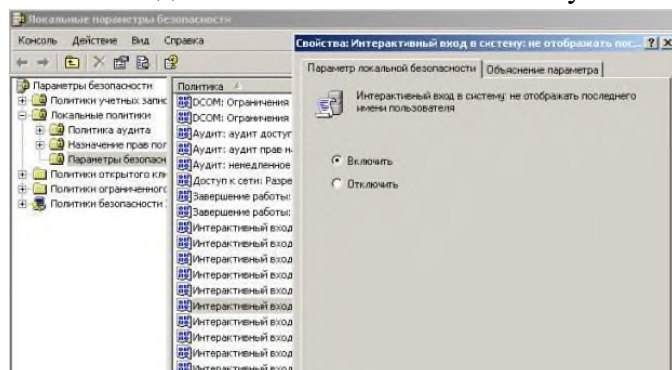


Рис. 9 - Активируем переключатель Включить

Теперь после завершения сеанса пользователь должен угадать не только пароль, но и имя пользователя (рис. 10).



Рис. 10 - Обе строки окна приветствия пусты

### Выявление сетевых уязвимостей сканированием портов ПК

Злоумышленники используют сканирование портов ПК для того, чтобы воспользоваться ресурсами чужого ПК в Сети. При этом необходимо указать IP адрес ПК и открытый port, к примеру, 195.34.34.30:23. После этого происходит соединение с удаленным ПК с некоторой вероятностью входа в этот ПК.

- TCP/IP port — это адрес определенного сервиса (программы), запущенного на данном компьютере в Internet. Каждый открытый порт — потенциальная лазейка для взломщиков сетей и ПК. Например, SMTP (отправка почты) — 25 порт, WWW — 80 порт, FTP — 21 порт.
- Хакеры сканируют порты для того, чтобы найти дырку (баг) в операционной системе. Пример ошибки, если администратор или пользователь ПК открыл полный доступ к сетевым ресурсам для всех или оставил пустой пароль на вход к компьютеру.

Одна из функций администратора сети - выявить недостатки в функционировании сети и устранить их. Для этого нужно просканировать сеть и закрыть (блокировать) все необязательные (открытые без необходимости) сетевые порты. Ниже, для примера, представлены службы TCP/IP, которые можно отключить:

- finger — получение информации о пользователях
- talk — возможность обмена данными по сети между пользователями
- bootp — предоставление клиентам информации о сети
- systat — получение информации о системе
- netstat — получение информации о сети, такой как текущие соединения
- rusersd — получение информации о пользователях, зарегистрированных в данный момент

### Просмотр активных подключений утилитой Netstat

Команда netstat обладает набором ключей для отображения портов, находящихся в активном и/или пассивном состоянии. С ее помощью можно получить список серверных приложений, работающих на данном компьютере. Большинство серверов находится в режиме LISTEN — ожидание запроса на соединение. Состояние CLOSE\_WAIT означает, что соединение разорвано. TIME\_WAIT — соединение ожидает разрыва. Если соединение находится в состоянии SYN\_SENT, то это означает наличие процесса, который пытается установить соединение с сервером. ESTABLISHED — соединения установлены, т. е. сетевые службы работают (используются).

Итак, команда netstat показывает содержимое различных структур данных, связанных с сетью, в различных форматах в зависимости от указанных опций. Для сокетов (программных



интерфейсов) TCP допустимы следующие значения состояния

- CLOSED — Закрыт. Сокет не используется.
- LISTEN — Ожидает входящих соединений.
- SYN\_SENT — Активно пытается установить соединение.
- SYN\_RECEIVED — Идет начальная синхронизация соединения.
- ESTABLISHED — Соединение установлено.
- CLOSE\_WAIT — Удаленная сторона отключилась; ожидание закрытия сокета.
- FIN\_WAIT\_1 — Сокет закрыт; отключение соединения.
- CLOSING — Сокет закрыт, затем удаленная сторона отключилась; ожидание подтверждения.
- LAST\_ACK — Удаленная сторона отключилась, затем сокет закрыт; ожидание подтверждения.
- FIN\_WAIT\_2 — Сокет закрыт; ожидание отключения удаленной стороны.
- TIME\_WAIT — Сокет закрыт, но ожидает пакеты, ещё находящиеся в сети для обработки

#### Примечание

Что такое «сокет» поясняет рис. 11. Пример сокета – 194.86.6..54:21

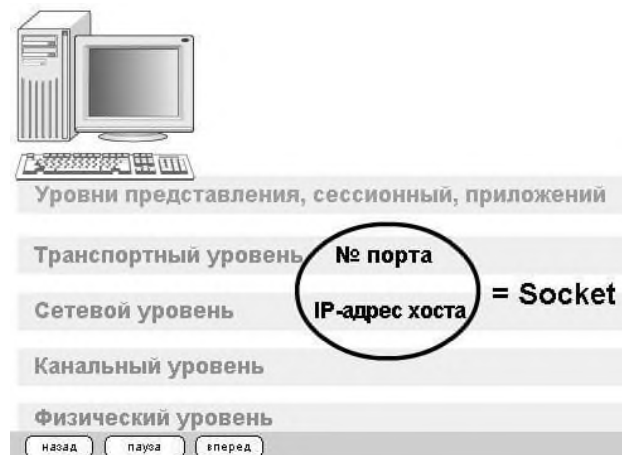


Рис. 11 - Сокет это № порта + IP адрес хоста

Практический пример. Обнаружение открытых на ПК портов утилитой Netstat

Для выполнения практического задания на компьютере необходимо выполнить команду Пуск-Выполнить. Откроется окно Запуск программы, в нем введите команду cmd (рис. 12).

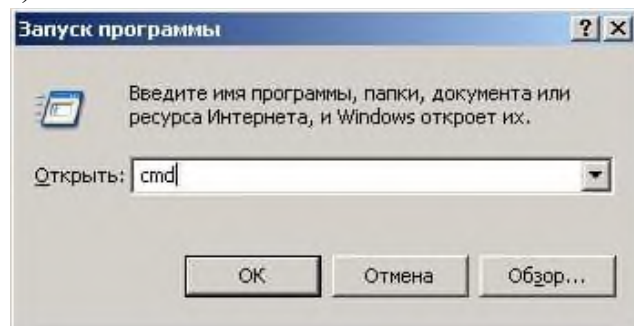


Рис. 12 - Окно Запуск программы

Чтобы вывести все активные подключения TCP и прослушиваемые компьютером порты



TCP/ UDP введите команду netstat (рис. 13). Мы видим Локального адреса (это ваш ПК) прослушиваются 6 портов. Они нужны для поддержки сети. На двух портах мы видим режим ESTABLISHED — соединения установлены, т. е. сетевые службы работают (используются). Четыре порта используются в режиме TIME\_WAIT — соединение ожидает разрыва.

```

Активные подключения
Имя      Локальный адрес      Внешний адрес      Состояние
TCP      D:3086               localhost:3087      ESTABLISHED
TCP      D:3087               localhost:3086      ESTABLISHED
TCP      D:3414               localhost:1110      TIME_WAIT
TCP      D:3416               localhost:1110      TIME_WAIT
TCP      D:3415               OSCP.AMS1.VERISIGN.COM:http TIME_WAIT
TCP      D:3417               OSCP.AMS1.VERISIGN.COM:http TIME_WAIT

D:\Documents and Settings\110>

```

Рис. 13 - Список активных подключений на тестируемом ПК

Запустите на вашем ПК Интернет и зайдите, например на [www.yandex.ru](http://www.yandex.ru). Снова выполните команду netstat (рис. 14). Как видим, добавилось несколько новых активных портов с их различными состояниями.

```

D:\Documents and Settings\110>netstat
Активные подключения
Имя      Локальный адрес      Внешний адрес      Состояние
TCP      D:1110               localhost:3433      TIME_WAIT
TCP      D:1110               localhost:3436      TIME_WAIT
TCP      D:1110               localhost:3441      TIME_WAIT
TCP      D:1110               localhost:3442      TIME_WAIT
TCP      D:1110               localhost:3443      TIME_WAIT
TCP      D:1110               localhost:3448      ESTABLISHED
TCP      D:1110               localhost:3452      TIME_WAIT
TCP      D:1110               localhost:3454      ESTABLISHED
TCP      D:1110               localhost:3456      TIME_WAIT
TCP      D:3430               localhost:3431      ESTABLISHED
TCP      D:3431               localhost:3430      ESTABLISHED
TCP      D:3432               localhost:1110      TIME_WAIT
TCP      D:3438               localhost:1110      TIME_WAIT
TCP      D:3440               localhost:1110      TIME_WAIT
TCP      D:3448               localhost:1110      ESTABLISHED
TCP      D:3450               localhost:1110      TIME_WAIT
TCP      D:3454               localhost:1110      ESTABLISHED
TCP      D:3458               localhost:1110      TIME_WAIT
TCP      D:3460               localhost:1110      TIME_WAIT
TCP      D:3461               localhost:1110      TIME_WAIT
TCP      D:3462               localhost:1110      TIME_WAIT
TCP      D:3434               addons-star.zlb.phx.mozilla.net:https TIME_WAIT
TCP      D:3445               static.yandex.net:http TIME_WAIT
TCP      D:3449               mc.yandex.ru:http   ESTABLISHED
TCP      D:3455               suggest.yandex.net:http ESTABLISHED
TCP      D:3463               suggest.yandex.net:http TIME_WAIT
TCP      D:3464               www.yandex.ru:http  TIME_WAIT
TCP      D:3465               yabs.yandex.ru:http TIME_WAIT

```

Рис. 14 - Активные подключения при работе ПК в Интернет

Команда netstat имеет следующие опции – табл. 1. Таблица 1 - Ключи для команды netstat

Опция (ключ)	Назначение
-a	Показывать состояние всех сокетов; обычно сокет, используемый серверными процессами, не показывается.
-A	Показывать адреса любых управляющих блоков протокола, связанных с сокетом; используется для отладки.
-i	Показывать состояние автоматически сконфигурированных (auto-configured) интерфейсов. Интерфейсы, статически сконфигурированные в системе, но

	не найденные во время загрузки, не показываются.
-n	Показывать сетевые адреса как числа. netstat обычно показывает адреса как символы. Эту опцию можно использовать с любым форматом показа.
-r	Показать таблицы маршрутизации. При использовании с опцией -s, показывает статистику маршрутизации.
-s	Показать статистическую информацию по протоколам. При использовании с опцией -r, показывает статистику маршрутизации.
-f семе йство адресов	Ограничить показ статистики или адресов управляющих блоков только указанным семейством_адресов, в качестве которого можно указывать:inet Для семейства адресов AF_INET,или unix Для семейства адресовAF_UNIX.
-I инте рфейс	Выделить информацию об указанном интерфейсе в отдельный столбец; по умолчанию (для третьей формы команды) используется интерфейс с наибольшим объёмом переданной информации с момента последней перезагрузки системы. В качестве интерфейса можно указывать любой из интерфейсов, перечисленных в файле конфигурации системы, например, emd1 или lo0.
-p	Отобразить идентификатор/название процесса создавшего сокет (-p, — programs display PID/Program name for sockets)

### Программа NetStat Agent

Представьте ситуацию: ваше Интернет-соединение стало работать медленно, компьютер постоянно что-то качает из Сети. Вам поможет программа NetStat Agent. С ее помощью вы сможете найти причину проблемы и заблокировать ее. Иначе говоря, NetStat Agent — полезный набор инструментов для мониторинга Интернет соединений и диагностики сети. Программа позволяет отслеживать TCP и UDP соединения на ПК, закрывать нежелательные соединения, завершать процессы, обновлять и освобождать DHCP настройки адаптера, просматривать сетевую статистику для адаптеров и TCP/IP протоколов, а также строить графики для команд Ping иTraceRoute (рис. 15).

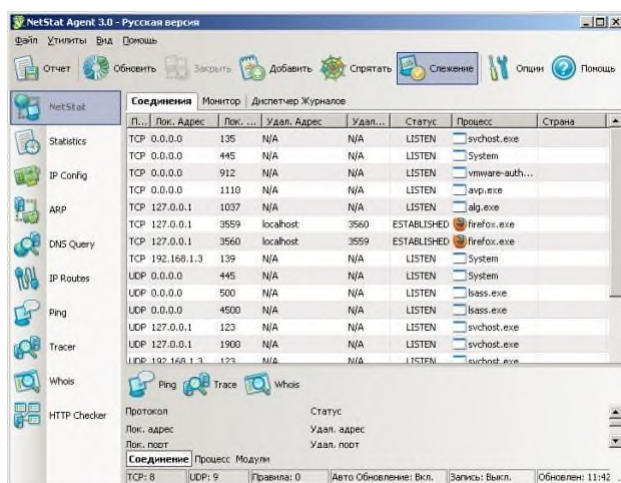


Рис. 15 - Главное окно программы NetStat Agent

В состав программы NetStat Agent вошли следующие утилиты:

- NetStat — отслеживает TCP и UDP соединения ПК (при этом отображается географическое местоположение удаленного сервера и имя хоста).
- IPConfig — отображает свойства сетевых адаптеров и конфигурацию сети.
- Ping — позволяет проверить доступность хоста в сети.
- TraceRoute — определяет маршрут между вашим компьютером и конечным хостом, сообщая все IP-адреса маршрутизаторов.
- DNS Query — подключается к DNS серверу и находит всю информацию о домене (IP адрес сервера, MX-записи (Mail Exchange) и др.).
- Route — отображает и позволяет изменять IP маршруты на ПК.
- ARP — отслеживает ARP изменения в локальной таблице.
- Whois — позволяет получить всю доступную информацию об IP-адресе или домене.
- HTTP Checker — помогает проверить, доступны ли Ваши веб-сайты.
- Statistics — показывает статистику сетевых интерфейсов и TCP/IP протоколов.

### Сканер портов Nmap (Zenmap)

Nmap — популярный сканер портов, который обследует сеть и проводит аудит защиты. Использовался в фильме «Матрица: Перегрузка» при взломе компьютера. Наша задача не взломать, а защитить ПК, поскольку одно и то же оружие можно использовать как для защиты, так и для нападения. Иначе говоря, сканером портов nmap можно определить открытые порты компьютера, а для безопасности сети пользователям рекомендуется закрыть доступ к этим портам с помощью брандмауэра (рис. 16).

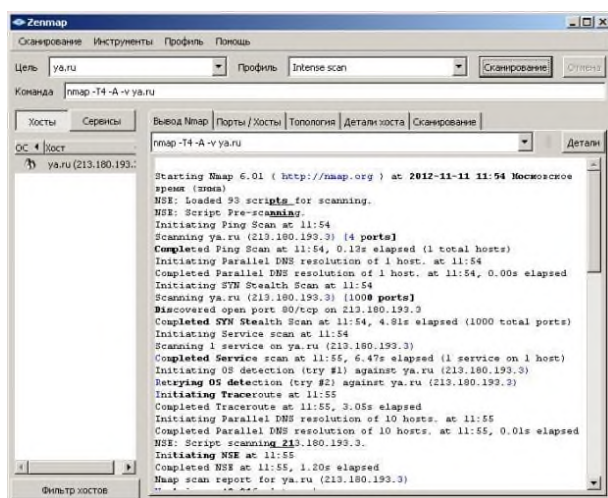


Рис. 16 - Интерфейс программы Nmap

Обычно для того, чтобы просканировать все порты какого-либо компьютера в сети вводится команда `nmap -p-65535 IP-адрес_компьютера` или `nmap -sV IP-адрес компьютера`, а для сканирования сайта — команда `nmap -sS -sV -O -P0 адрес сайта`.

### Монитор портов TCPView

TCPView — показывает все процессы, использующие Интернет-соединения. Запустив TCPView, можно узнать, какой порт открыт и какое приложение его использует, а при необходимости и немедленно разорвать соединение – рис. 17.

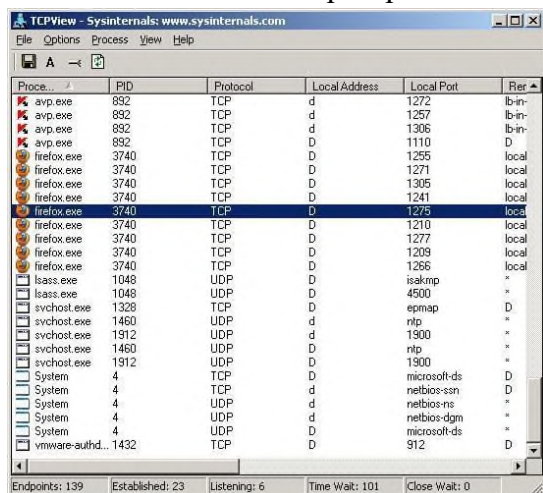


Рис. 17 - Главное окно программы TCPView

Просмотрите активные сетевые подключения локального ПК с помощью монитора портов `triview`. Определите потенциально возможные угрозы (какие порты открыты, и какие приложения их используют). При необходимости можно закрыть установленное приложение TCP-соединение или процесс правой кнопкой мыши.

### Выполнение работы

Изучить материал по мониторингу активности и блокированию портов и ответить на вопросы:

1. Какие виды мониторинга рабочих операций пользователя существуют?
2. Дайте характеристику современным программным средств мониторинга действий пользователей. Какое программное средство вы порекомендовали бы нашей

организации? Почему?

3. Какие уязвимости ОС Windows были устранены в данной работе и какими путями?
4. Как узнать закрытые порты? Как открыть нужный порт?
5. Для чего используется программа NetStat Agent? Nmap? TCPView?

### Практическое занятие «Проверка наличия и сроков действия сертификатов»

Цель работы: научиться проверять наличие и срок действия сертификатов

Для чего нужно продление SSL-сертификата

Шифрование данных актуально для любых сайтов, на которых пользователи вводят персональную информацию - то есть, в том числе и для любых интернет-магазинов и воронок. Использование SSL-сертификата добавляет дополнительную степень защиты, но сам сертификат имеет ограниченный срок службы. По окончании этого срока необходимо выпустить (зарегистрировать) новый SSL-сертификат.

Продление сертификата SSL крайне желательно выполнить до окончания срока действия предыдущего сертификата.

Стоит отметить, что то, что называется "продлением" - это, фактически, регистрация нового сертификата. Сертификаты никак не связаны между собой - можно покупать несколько сертификатов в день на один и тот же домен в день (хотя технически это не имеет смысла - к домену может быть физически привязан только один сертификат).

Как проверить срок действия SSL-сертификата

Рассмотрим, как узнать срок действия установленного на домен сертификата.

Откройте сайт по протоколу https (например, <https://site.ru>) в браузере. В левом углу, рядом с адресом, нажмите на иконку замочка и в выпадающем меню нажмите на пункт "Сертификат" (рис. 1).

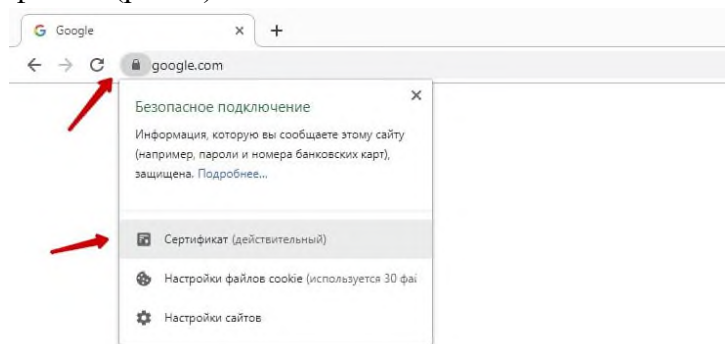


Рисунок 1.

Откроется окно с информацией о сертификате (рис. 2).

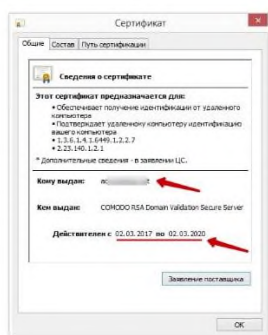


Рисунок 2.

В нём указан домен, для которого действует сертификат и даты начала/окончания его действия. Это и есть срок действия SSL сертификата.

Стоит отметить, что все новые сертификаты выдаются на 1 или 2 года. Сертификаты более, чем на 2 года не выпускаются с 2018 года по соображениям безопасности.

Что произойдет, если срок действия SSL-сертификат закончится

Если срок действия SSL-сертификат закончится, при попытке зайти на сайт в браузере отобразится сообщение об [ошибке](#) (рис. 3).

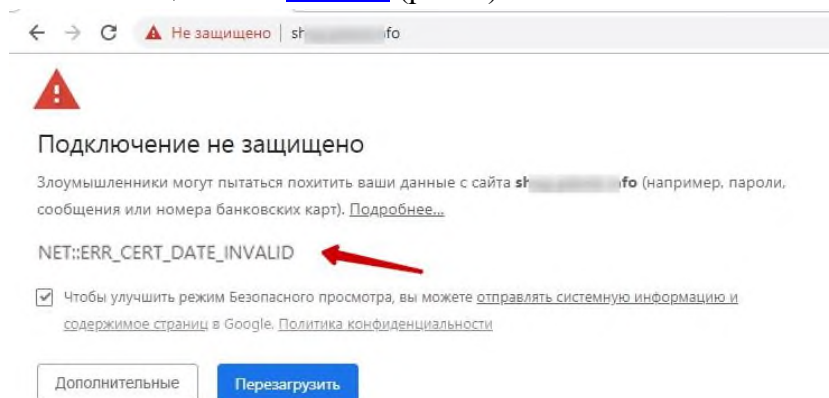


Рисунок 3

## Практическое занятие «Разработка политики безопасности корпоративной сети»

Цель работы: определить политику безопасности корпоративной сети

Информационные технологии, повсеместно применяемые для объединения компьютеров в сети, позволили значительно повысить производительность труда в организациях, с учетом, что сегодня в некоторых сферах деятельности просто невозможно обойтись без их использования. К таким сферам относятся: банковское дело, складские операции крупных компаний, электронные архивы библиотек и др. В этих сферах каждая отдельно взятая рабочая станция в не может хранить всей информации (в основном, по причине слишком большого ее объема). Сеть позволяет избранным (зарегистрированным на файл-сервере) пользователям получать доступ к той информации, к которой их допускает администратор сети.

Дальнейшее развитие и укрупнение предприятия, появление удаленных отделов и филиалов ставит новые задачи по объединению удаленных информационных ресурсов. Наряду с расширением IP-сетей в таких случаях, как правило, решаются дополнительные задачи:



объединение мини-АТС-филиалов, построение систем видеонаблюдения и видеоконференций, а также систем телемеханики (стандартные задачи дистанционного измерения, управления, индикации). Состав и объем дополнительных задач определяется основным видом деятельности предприятия.

Способы построения корпоративной сети.

В зависимости от поставленной задачи и цели, способы создания корпоративной сети могут быть разными. Чаще всего именно комбинация различных технологических решений позволяет добиться оптимального решения. У каждого из применяемых способов есть свои преимущества и недостатки. Объединение офисных локальных сетей в единую корпоративную сеть организации может осуществляться тремя методами.

1. Использование беспроводных сетей передачи данных. Применяется при построении корпоративной сети между рабочими площадками, расположенными в близко размещенных строениях.
2. Использование Internet в качестве транспортной среды передачи данных, с применением технологии построения VPN (Virtual Private Network) туннелей.
3. Использование арендованных каналов передачи данных. Возможно построение сети с применением технологии построения VPN туннелей или без.

При создании корпоративной сети методом VPN туннелей, для повышения безопасности VPN туннель должен быть зашифрованным.

Система защиты информации корпоративной сети с повышенной безопасностью должна обеспечивать:

- защиту информации от вмешательства посторонних нарушителей извне (через подключения к каналам связи внутри сети, через внешние системы, включая Интернет) и комплексную систему антивирусной защиты;
- разграничение доступа законных пользователей к ресурсам системы по уровням доступа (к рабочим местам, ресурсам вычислительной сети, к различным информационным системам, к средствам передачи информации, включая внутреннюю и внешнюю электронную почту, средства Интернет и другие);
- идентификацию и аутентификацию пользователей при работе в информационной сети (ИС);
- контроль над легитимностью действий пользователей и своевременное и соответствующее реагирование на нарушения;
- централизованный контроль целостности технических средств обработки информации;
- централизованное управление конфигурациями элементов корпоративной сети ИС, контроль целостности конфигураций;
- защиту целостности и конфиденциальности информации на всех этапах ее обработки, включая методы шифрования, использования электронной цифровой подписи и антивирусные средства;
- соответствующие изменения в организации защиты информации при совершенствовании технологий выполнения операций.

Безопасность в информационной сети.

Существуют три основных вида защиты сети:

- средства физической защиты, включающие средства защиты кабельной системы, систем

электропитания, средства архивации, дисковые массивы и т.д.

- программные средства защиты, в том числе: антивирусные программы, системы разграничения полномочий, программные средства контроля доступа.
- административные меры защиты, включающие контроль доступа в помещениях, разработку стратегии безопасности фирмы, планов действий в чрезвычайных ситуациях и т.д.

Кабельная система остается главной проблемой большинства ИС. По данным различных исследований, именно кабельная система является причиной более чем половины всех отказов сети, в связи с этим кабельной системе должно уделяться особое внимание с самого момента проектирования сети.

Наилучшим образом избежать себя от проблем по поводу неправильной прокладки кабеля является использование структурированных кабельных систем, использующих одинаковые кабели для передачи данных в локальной вычислительной сети, локальной телефонной сети, передачи видеоинформации или сигналов от датчиков пожарной безопасности или охранных систем.

Для защиты информационных ресурсов и обеспечения оптимальной работы информационных систем необходимо применение комплексной системы информационной безопасности, которая позволит эффективно использовать достоинства межсетевых экранов и компенсировать их недостатки с помощью других средств безопасности.

Использование межсетевых экранов позволяет организовать внутреннюю политику безопасности сети предприятия, разделив всю сеть на сегменты. Сегмент сети - логически или физически обособленная часть сети. Разбиение сети на сегменты осуществляется с целью оптимизации сетевого трафика и/или повышения безопасности сети в целом.

Это позволяет сформулировать основные принципы архитектуры безопасности корпоративной сети:

- введение  $N$  категорий секретности и создание соответственно  $N$  выделенных сетевых сегментов пользователей. При этом каждый пользователь внутри сетевого сегмента имеет одинаковый уровень секретности (допущен к информации одного уровня секретности). Данный случай можно сравнить с секретным заводом, где все сотрудники в соответствии со своим уровнем доступа имеют доступ только к определенным этажам. Эта структура объясняется тем, что ни в коем случае нельзя смешивать потоки информации разных уровней секретности. Не менее очевидным объяснением подобного разделения всех пользователей на  $N$ , изолированных сегментов является легкость осуществления атаки внутри одного сегмента сети;
- выделение в отдельный сегмент всех внутренних серверов компании. Эта мера также позволяет изолировать потоки информации между пользователями, имеющими различные уровни доступа;
- выделение в отдельный сегмент всех серверов компании, к которым будет предоставлен доступ из Интернета (создание демилитаризованной зоны для внешних ресурсов);
- создание выделенного сегмента административного управления;
- создание выделенного сегмента управления безопасностью.

Межсетевой экран пропускает через себя весь трафик, принимая относительно каждого проходящего пакета решение: дать ему возможность пройти или нет. Для того чтобы



межсетевой экран мог осуществить эту операцию, ему необходимо определить набор правил фильтрации.

Разновидностью программных средств обеспечения безопасности компьютерных сетей является защита от компьютерных вирусов. Наиболее распространенными методами защиты от вирусов по сей день остаются различные антивирусные программы. Однако в качестве перспективного подхода к защите от компьютерных вирусов в последние годы все чаще применяется сочетание программных и аппаратных методов защиты. Среди аппаратных устройств такого плана можно отметить специальные антивирусные платы, которые вставляются в стандартные слоты расширения компьютера.

В компьютерных сетях при организации контроля доступа и разграничения полномочий пользователей используется комбинированный подход - пароль + идентификация пользователя по персональному “ключу”. В качестве “ключа” может использоваться пластиковая карта (магнитная или со встроенной микросхемой - smart- card) или различные устройства для идентификации личности по биометрической информации - по радужной оболочке глаза или отпечатков пальцев, размерам кисти руки и так далее. Оснатив сервер или сетевые рабочие станции, например, устройством чтения смарт-карточек и специальным программным обеспечением, можно значительно повысить степень защиты от несанкционированного доступа.

Существуют следующие службы безопасности:

- аутентификация;
- обеспечение целостности;
- засекречивание данных;
- контроль доступа;
- защита от отказов.

Наиболее надежным средством предотвращения потерь информации является: установка источников бесперебойного питания (при кратковременном отключении электроэнергии) и организация надежной системы архивации данных.

В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер. Хранение архивной информации, представляющей особую ценность, должно быть организовано в специальном охраняемом помещении. Рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании, на случай пожара или стихийного бедствия.

Дополнительными требованиями к организации корпоративной информационной сети, где хранящаяся в ней информация является секретной, также является максимальная изолированность сети от внешнего внедрения (отсутствие беспроводного подключения, в частности использования технологий Wi-Fi для построения сети, а также прокладка кабельной сети в недоступных для посторонних людей местах) и лицензирование используемого в ней программного обеспечения. К организациям с подобными требованиями к безопасности сети можно отнести федеральные и государственные организации (пенсионный фонд, налоговая служба, полиция и т.п.), а также банки и подобные им коммерческие предприятия.

Практическое занятие «Получение сертификата»

Цель: Изучить основные понятия сертификации. Сертификация ПО.

Сертификации в переводе с латыни означает «сделано верно». Для того чтобы убедиться в том, что продукт «сделан верно», надо знать, каким требованиям он должен соответствовать и каким образом возможно получить достоверные доказательства этого соответствия. Общепризнанным способом такого доказательства служит сертификация соответствия.

Термин «соответствие», указывает, что это процедура, даёт уверенность в том, что продукция (процесс, услуга) соответствуют заданным требованиям.

К объектам сертификации относятся продукция, услуги, работы, системы качества, персонал, рабочие места и пр.

В сертификации продукции, услуг и иных объектов (далее – продукция) участвуют первая, вторая, третья стороны.

Третья сторона – лицо или орган, признаваемые независимыми от участвующих сторон в рассматриваемом вопросе.

Участвующие стороны представляют собой, как правило, интересы поставщиков (первая сторона) и покупателей (вторая сторона).

Сертификация может иметь обязательный и добровольный характер.

Перечни продукции, подлежащей обязательной сертификации, утверждаются Правительством Российской Федерации.

Сертификация продукции (далее – сертификация) – процедура подтверждения соответствия, посредством которой независимая от изготовителя (продавца, исполнителя) и потребителя (покупателя) организация удостоверяет в письменной форме, что продукция соответствует установленным требованиям.

Система сертификации – совокупность участников сертификации, осуществляющих сертификацию по правилам, установленным в этой системе.

Систему сертификации составляют: центральный орган, который управляет системой, проводит надзор за её деятельностью и может передавать право на проведение сертификации другим органам; правила и порядок проведения сертификации; нормативные документы, на соответствие которым осуществляется сертификация; процедура (схемы) сертификации; порядок инспекционного контроля. Системы сертификации могут действовать на национальном, региональном и международном уровнях. Если система сертификации занимается доказательством соответствия определённого вида продукции (процесса, услуг) – это система сертификации однородной продукции, которая в своей практике применяет стандарты, правила и процедуру, относящиеся именно к данной продукции.

Сертификат соответствия (далее сертификат) – документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям.

Декларация о соответствии – документ в котором изготовитель (продавец, исполнитель) удостоверяет, что поставляемая (продаваемая) им продукция соответствует установленным требованиям.

Таким образом, подтверждение соответствия проводится посредством не только сертификата, но и декларации о соответствии. Перечни продукции, соответствие которой

может быть подтверждено декларацией о соответствии, утверждаются постановлением Правительства Российской Федерации. Декларация о соответствии имеет юридическую силу наравне с сертификатом.

Знак соответствия – за зарегистрированный в установленном порядке знак, которым по правилам данной системы сертификации подтверждается соответствие маркированной им продукции установленным требованиям.

Основные цели и принципы сертификации Сертификация направлена на достижение следующих целей:

- содействие потребителям в компонентном выборе продукции (услуги);
- защита потребителя от недобросовестности изготовителя (продавца, исполнителя);
- контроль безопасности продукции (услуги, работы), для окружающей среды, жизни, здоровья и имущества;

- подтверждение показателей качества продукции, работы), заявленных изготовителем (исполнителем);

- создание условий для деятельности организации и предпринимателей на едином товарном рынке России, а также для участия в международном экономическом, научно-техническом сотрудничестве и международной торговле.

При проведении сертификации необходимо руководствоваться следующими принципами.

Законодательная основа сертификации. (Деятельность по сертификации в РФ основана на Законах РФ «О сертификации продукции и услуг», «О защите прав потребителей» и других нормативных актах».

Открытость системы сертификации. (В работах по сертификации участвуют предприятия, учреждения, организации независимо от форм собственности (в том числе других стран), признающие и выполняющие её правила).

Гармонизация правил рекомендаций по сертификации с международными нормами и правилами. (Гармонизация является условием признания сертификатов и знаков соответствия за рубежом, тесного взаимодействия с международными, региональными и национальными системами сертификации других стран).

Открытость и закрытость информации. (При сертификации должно осуществляться информирование всех её участников – изготовителей, потребителей, органов по сертификации, а также всех других заинтересованных сторон – общественных организаций, предприятий, отдельных лиц – о правилах и результатах сертификации.

С другой стороны, при сертификации должна соблюдаться конфиденциальность информации, составляющей коммерческую тайну). Обязательная и добровольная сертификация

В соответствии с Законом РФ «О сертификации продукции и услуг» сертификация может иметь обязательный о добровольный характер.

Обязательная сертификация – подтверждение уполномоченным на то органом соответствия продукции обязательным требованиям, установленным законодательством.

Наиболее универсальными, т.е. применимыми к большинству товаров и услуг, являются требования: назначения, безопасности, экологичности, надёжности, эргономики,

ресурсосбережения, технологичности, эстетичности.

Обязательная сертификация является формой государственного контроля за безопасностью продукции. Её осуществление связано с определёнными обязанностями, налагаемыми на предприятия, в том числе материального характера. Поэтому она может осуществляться лишь в случаях, предусмотренных законодательными актами РФ, т.е. законами и нормативными актами Правительства РФ.

В соответствии с Законом РФ «О защите прав потребителей» перечни товаров (работ, услуг), подлежащих обязательной сертификации, утверждаются Правительством РФ. На основании этих перечней разрабатывается и вводится в действие постановлением Госстандарта России «Номенклатура продукции и услуг (работ) в отношении которых законодательными актами Российской Федерации предусмотрена их обязательная сертификация».

При обязательной сертификации действие сертификата соответствия и знака соответствия распространяется на всей территории РФ.

Организация и проведение работ по обязательной сертификации возлагаются на специально уполномоченный федеральный орган исполнительной власти в области сертификации – Госстандарт России, а в случаях, предусмотренных законодательными актами РФ в отношении отдельных видов продукции, и на другие федеральные органы исполнительной власти. В России в 1999 г. действовало 16 систем обязательной сертификации. Самая представительная и известная – Система обязательной сертификации ГОСТ Р, образованная и возлагаемая Госстандартом России. В рамках этой системы действуют системы сертификации однородной продукции (пищевой продукции и продовольственного сырья, игрушек, посуды, товаров лёгкой промышленности и др.) и однородных услуг (услуг общественного питания, туристских услуг и услуг гостиниц и др.). Добровольная сертификация проводится по инициативе юридических или физических лиц на добровольных условиях между заявителем и органом по сертификации в системах добровольной сертификации. Допускается проведение добровольной сертификации в системах обязательной сертификации органами по обязательной сертификации. Нормативный документ, на соответствие которому осуществляются испытания при добровольной сертификации, выбирается, как правило, заявителем. Заявителем может быть изготовитель, поставщик, продавец, потребитель продукции. Системы добровольной сертификации чаще всего объединяют изготовителей и потребителей продукции, заинтересованных в развитии торговли на основе долговременных партнёрских отношений.

В отличие от обязательной сертификации, объекты которой и подтверждение их соответствия связаны с законодательством, добровольная сертификация касается видов продукции (процессов, услуг), не включённых в обязательную номенклатуру и определяемых заявителем (либо в договорных отношениях). Правила и процедуры системы добровольной сертификации определяются органом по добровольной сертификации.

Однако так же, как и в системах обязательной сертификации, они базируются на рекомендациях международных и региональных организаций в этой области. Решение о добровольной сертификации связано с проблемами конкурентоспособности товара, продвижением товаров на рынок (особенно зарубежный); предпочтениями покупателей, всё больше ориентирующихся в своём выборе на сертифицированные изделия. Как правило, развитие добровольной сертификации поддерживается государством. В настоящее время в России преобладает обязательная сертификация, за рубежом добровольная, заинтересованы в добровольной сертификации лишь российские эксперты. По мере ужесточения конкуренции на рынке будет возрастать потребность в добровольной сертификации.

#### Участники сертификации

Участниками сертификации являются изготовители и исполнители услуг (первая сторона), заказчики – продавцы (первая либо вторая сторона), а также организации, представляющие третью сторону - органы по сертификации, испытательные лаборатории (центры), специально уполномоченные федеральные органы исполнительной власти.

Основные участники – заявители, органы по сертификации (ОС) и испытательные лаборатории (ИЛ). Именно они участвуют в процедуре сертификации каждого конкретного объекта на всех этапах этой процедуры.

Изготовители (продавцы, исполнители) при проведении сертификации обязаны:

- реализовать продукцию, исполнять услуги только при наличии сертификата, выданного или признанного уполномоченным на то органом или декларации о соответствии (принятой в установленном порядке);
- обеспечивать соответствие реализуемой продукции (услуги) требованиям НД, на соответствие которым она была сертифицирована, и маркирование её знаком соответствия;
- указывать в сопроводительной технической документации сведения о сертификате или декларации о соответствии и НД, которым она должна соответствовать и обеспечивать доведение этой информации до потребителя (покупателя, заказчика);
- обеспечивать беспрепятственное выполнение своих полномочий должностным лицам, осуществляющим контроль за сертифицированной продукцией (услугой);
- приостанавливать или сокращать реализацию продукции (предоставление услуги): если она не отвечает требованиям НД; после истечения срока действия или отмены решением ОС; по истечении срока действия декларации о соответствии; по истечении срока годности или срока службы продукции;
- извещать ОС о тех изменениях, которые влияют на характеристики, проверяемые при сертификации.

Орган по сертификации выполняет следующие функции:

- сертифицирует продукцию (услуги), выдаёт сертификаты и лицензии на применение знака соответствия;
- осуществляет инспекционный контроль за сертифицированной продукцией (услугой);
- приостанавливает либо отменяет действие выданных им сертификатов; - предоставляет заявителю необходимую информацию.

ОС несёт ответственность за обоснованность и правильность выдачи сертификата соответствия, за соблюдение правил сертификации.

Аккредитованные испытательные лаборатории (ИЛ) осуществляют испытания конкретной продукции или конкретные виды испытаний и выдают протоколы испытаний для целей сертификации.

ИЛ несёт ответственность за соответствие проведённых ею сертификационных испытаний требованиями НД, а также за достоверность и объективность результатов.

Если орган по сертификации аккредитован как ИЛ, то его именуют сертификационным центром.

Правовые основы сертификации

Закон «О защите прав потребителей»

Сертификация в России организуется и проводится в соответствии с общегосударственными законами РФ: «О защите прав потребителей», «О сертификации продукции и услуг», «О стандартизации», а также с законами РФ, относящимися к определённым отраслям: «О ветеринарии», «О пожарной безопасности», «О санитарноэпидемиологическом благополучии населения», иными правовыми актами Российской Федерации, направленными на решение отдельных социально-экономических задач.

Закон «О защите прав потребителей», принятый в 1992г., установил ряд принципиально новых положений: закрепил права потребителей – право на безопасность товаров, работ, услуг для жизни и здоровья; право на надлежащее качество приобретаемых товаров, выполняемых работ и оказываемых услуг; право на возмещение ущерба и судебную защиту прав и интересов потребителя; предусмотрел механизм защиты потребителей, права которых нарушены при продаже недоброкачественных товаров либо при ненадлежащем выполнении работ оказании услуг.

Все законодательные акты, действующие на территории РФ, приведены в соответствии с Законом «О защите прав потребителей».

На основании отдельных статей закона Правительство РФ утверждает разного рода подзаконные акты, правила по договорам купли-продажи, по продаже отдельных видов товаров, выполнению отдельных видов работ и т.д.

В целях обеспечения безопасности товаров (работ, услуг) Закон «О защите прав потребителей» вводит обязательную сертификацию, Сертификация подтверждает соответствие качества товара обязательным требованиям государственных стандартов.

На основании Закона обязательной сертификации подлежат:

- товары (работы, услуги), на которые в законодательных актах, государственных стандартах установлены требования, направленные на обеспечение безопасности жизни, здоровья потребителей и охраны окружающей среды, а также на предотвращение причинения вреда имуществу потребителей;
- средства, обеспечивающие безопасность жизни и здоровья потребителей.

Партия товара, реализуемого через розничную торговую сеть, или каждая единица товара должна сопровождаться сертификатом соответствия, который продавец обязан

предъявить покупателю по его требованию.

Реализация товаров (в том числе импортных), выполнение работ и оказание услуг без сертификата соответствия, подтверждающего их соответствие обязательным требованиям стандартов безопасности, Законом запрещена. Товары могут сопровождаться сертификатом, выданным национальными органами по сертификации, а также зарубежными сертификатами, признанными в России.

На товарах, прошедших сертификацию и удостоверенных сертификатом (или на сопроводительной документации, на таре или упаковке), должен быть знак соответствия, установленный государственным стандартом. Ответственность за наличие сертификата и знака соответствия несёт продавец (изготовитель).

В первоначальной редакции Закон действовал четыре года. Но практика показала, что не все его статьи позволяют однозначно толковать их содержание. В 1996г. был принят Федеральный закон «О внесении изменений и дополнений, а Закон Российской Федерации «О защите прав потребителей» и Кодекс РСФСР об административных правонарушениях». Ряд изменений коснулся непосредственно вопросов обязательной сертификации.

Так, в новой редакции уточняется сущность понятия, «потребитель» которое трактуется как «гражданин, имеющий намерение заказать или приобрести либо заказывающий, приобретающих или использующий товары (работы, услуги) исключительно для личных

«бытовых» нужд, не связанных с извлечением прибыли». Таким образом, к числу потребителей Закон не относит индивидуальных предпринимателей, приобретающих товар для своей деятельности, связанной с извлечением прибыли. Однако, предпринимателю не запрещено обращаться в Общество по защите прав потребителей с жалобами на качество товара.

Закон предусматривает систему мер, предотвращающих поступление в продажу товаров, в отношении которых известны факты причинения вреда человеку и окружающей среде, не смотря на соблюдение потребителем правил пользования, хранения и транспортировки. При поступлении сигналов от обществ по защите прав потребителей, государственных и общественных организаций, судебных органов Закон обязывает изготовителя приостановит производство (реализацию) товаров, работ, услуг и устранить причины, вызывающие несоответствие. Закон определяет и другие меры.

Чтобы иметь возможность защитить свои права в случае их нарушения, потребитель обязательно должен располагать информацией об изготовителе, поэтому Закон «О защите прав потребителей» предусматривает право потребителя на информацию о предприятии – изготовителе товара, продавце товара, а также предпринимателе, который производит и продаёт товар.

Некоторые сведения об изготовителе потребитель может почерпнуть из торговых марок, товарных знаков. Товарные знаки крупнейших фирм всегда обеспечивают доверие покупателей к их продукции, основанное не на наличии сертификата соответствия, а на высоком и стабильном качестве, которое гарантируется высокоэффективными системами управления качеством продукции на предприятиях этих фирм.

Сертификат соответствия вправе потребовать от изготовителя и продавца покупатель, что рассматривается законом «О защите прав потребителей» как гарантия права на

безопасность потребляемых товаров. Безопасность изделий, процессов, услуг, определяемая Законом, как основной аспект сертификации, характеризуется конкретными параметрами и требованиями к ним.

В этой связи законом усилена государственная защита прав потребителей путём расширения полномочий таких федеральных органов управления, как: Министерство РФ по антимонопольной политике и поддержке предпринимательства, Госстандарт РФ, Минздрав РФ и др. Они получили право в пределах своей компетенции:

- осуществлять контроль за соблюдением изготовителями (продавцами) требований к безопасности продукции (работ, услуг);
- требовать устранения недостатков или снимать подобные товары с производства, запрещать реализацию продукции и услуг, предписывать прекращение работ;
- предписывать запрещение реализации товаров с истекшим сроком годности, а также при отсутствии достоверной информации о них.

За нарушение правил сертификации органами по сертификации, испытательными лабораториями (центрами) установлен штраф в размере двукратной стоимости работ по сертификации. Если же товары реализуются с нарушениями правил по сертификации, то штрафом облагаются изготовители (продавцы) в размере стоимости реализованных товаров. Ответственность за подобные нарушения несут также и руководители предприятий-изготовителей и органов по сертификации. Обязанности по координации деятельности федеральных органов, осуществляющих контроль за безопасностью товаров, Закон возлагает на Госстандарт РФ.

В области сертификации Законом определены следующие обязанности Госстандарта РФ:

- определение порядка сертификации и номенклатуры товаров (работ, услуг), подлежащих обязательной сертификации;
- аккредитация органов по сертификации контрольных видов товаров (работ, услуг) и испытательных лабораторий (центров), а также предоставление права проведения аккредитации другим юридическим лицам;
- осуществление контроля за правильностью проведения сертификации;
- введение Государственного реестра сертифицированных товаров, аккредитованных органов по сертификации и испытательных лабораторий;
- принятие решений о признании сертификатов, выданных зарубежными и международными организациями;
- представление России во взаимодействиях с зарубежными странами и в международных организациях по вопросам сертификации.

В более широком аспекте правовые основы сертификации обеспечивает Закон РФ «О сертификации продукции и услуг».

Закон «О сертификации продукции и услуг»

Закон «О сертификации продукции и услуг» был принят в 1993г., в новой редакции – в 1995г., а в 1998г. вступил в силу Федеральный закон «О внесении изменений и дополнений» в Закон Российской Федерации «О сертификации продукции и услуг», содержащий новые положения, касающиеся различных аспектов сертификации.



Новые изменения и дополнения создают законодательную основу для более глубокой гармонизации российских систем сертификации с международными правилами и нормами, что необходимо для выполнения требований «Всемирной торговой организации» (ВТО).

Принята новая редакция определения термина «сертификация» с учётом Руководства 2 ИСО/МЭК от 1996г.: сертификация – это деятельность по подтверждению соответствия установленным требованиям независимой от изготовителя (продавца, исполнителя) и потребителя (покупателя) организации. Соответствие удостоверяется в письменной форме, т.е. документом. Таким документом является сертификат соответствия.

Дополнение устанавливает, что «при обязательной сертификации действие сертификата соответствия и знака соответствия распространяется на всей территории Российской Федерации». Такое уточнение вызвано незаконной практикой субъектов РФ, которые принимали нормативные акты, обязывающие поставщиков товаров проводить повторную сертификацию, если сертификат соответствия был получен ими в другом регионе России.

Закон однозначно трактует право на создание системы сертификации: «система сертификации создаётся государственными органами управления, предприятиями, учреждениями и организациями и представляет собой совокупность участников сертификации», которые проводят сертификацию по тем правилам и в том порядке, как это принято в данной системе и в соответствии с положениями Закона «О сертификации продукции и услуг». В Законе установлены общие положения о сертификате и знаке соответствия, об обязанностях Госстандарта РФ по разработке правил их регистрации и применения.

Закон предусматривает, что система сертификации может создаваться только юридическими лицами. Форма собственности юридического лица и организационная форма не регламентируются.

Согласно Закону, к участникам сертификации могут быть отнесены: государственные органы; организации, которые создают систему сертификации; испытательные лаборатории; центральные органы системы сертификации, определяемые в необходимых случаях для организации и координации работ в системах сертификации однородной продукции; а также изготовители (продавцы) и потребители (могут привлекаться представители обществ по защите прав потребителей).

В законе уточняется право участия в обязательной сертификации организаций независимо от их «организационно-правовых форм и форм собственности, если они не являются изготовителями (продавцами, исполнителями) и потребителями (покупателями) сертифицируемой ими продукции, при условии их аккредитации в установленном порядке и наличии лицензии на проведение работ по обязательной сертификации».

Пересмотрены положения статей Закона, касающихся аккредитации. Теперь право аккредитации предоставлено не только Госстандарту, но и другим федеральным органам исполнительной власти, на которые законодательными актами РФ возложена организация обязательной сертификации. В их обязанности вменяется не только проверка компетентности, но выявление независимости от изготовителей, продавцов, потребителей. Лицензия должна выдаваться только после получения аккредитуемой организацией аттестата аккредитации.

Таким образом, новая редакция указанного положения приведена в полное соответствие с требованиями документа Европейской Комиссии Генерального Директората III «Перечень мероприятий, которые должны быть приняты Российской Федерацией».

Формы обязательной сертификации устанавливает Госстандарт либо другие уполномоченные на то органы, причём все они должны учитывать сложившуюся зарубежную и международную практику.

Закон установил положение, касающееся рекламной деятельности: запрещается рекламирование товара, если он подлежит обязательной сертификации, но не имеет сертификата соответствия.

Существенные изменения внесены в положения Закона, относящиеся к добровольной сертификации. Отмечены ограничения, которые запрещали добровольную сертификацию продукции, если она подлежала обязательной сертификации. Отменено положение, которое предусматривало проведение добровольной сертификации только тем требованиям к товару, которые не отнесены к обязательным. Добровольная сертификация проводится на условиях договора между заявителем и органом по сертификации по инициативе заявителя.

Цель добровольной сертификации - подтверждение соответствия продукции требованиям стандартов, технических условий, рецептур и других документов, определяемых заявителем.

Однако Закон предусматривает, что добровольная сертификация продукции, подлежащей обязательной сертификации, не заменяет обязательную сертификацию этой продукции. Таким образом, если даже изготовитель осуществил добровольную сертификацию на соответствие тем показателям, которые являются аспектом обязательной сертификации, он всё равно обязан провести обязательную сертификацию.

Весьма важным дополнением к Закону о сертификации продукции и услуг является подтверждение соответствия:

«Подтверждение соответствия может также проводится посредством принятия изготовителем (продавцом, исполнителем) декларации о соответствии. Декларация о соответствии является документом, в котором изготовитель (продавец, исполнитель) удостоверяет, что поставляемая (продаваемая) им продукция соответствует требованиям. Перечни продукции, соответствие которой может быть подтверждено декларацией о соответствии, требования к декларации о соответствии и порядок её принятия утверждаются Правительством Российской Федерации.

Декларация о соответствии, принятая в установленном порядке, регистрируется в органе по сертификации и имеет юридическую силу наравне с сертификатом».

Принятое дополнение соответствует требованиям по присоединению России к ВТО, положениям ГАТТ и зарубежной практике подтверждения соответствия согласно Руководству 2 ИСО/МЭК.

Организационно-методические принципы сертификации

Правила сертификации

В качестве органа по сертификации (ОС) или испытательных лабораторий (ИЛ) допускаются организации независимо от их организационно-правовых форм и форм собственности, если они не являются изготовителями (продавцами, исполнителями) и

потребителями (покупателями сертифицированной ими продукции), при условии их аккредитации в установленном порядке и наличии лицензии на проведение работ по сертификации.

Аккредитацию ОС и ИЛ организует и осуществляет Госстандарт России, федеральные органы исполнительной власти в пределах своей компетенции на основе результатов их аттестации, как правило, комиссиями. Результаты аккредитации оформляют аттестатом аккредитации.

Если в системе аккредитации несколько ОС одной и той же продукции (услуги), то заявитель в праве провести сертификации в любом из них.

Сертификация отечественной и импортируемой продукции проводится по одним и тем же правилам.

Сертификаты и аттестаты аккредитации в системах обязательной сертификации вступают в силу с даты их регистрации в Государственном Реестре.

Государственный реестр содержит сведения о ЦОС, ОС, ИЛ, утверждённых системах сертификации однородной продукции (группы услуг), знаках соответствия, Аттестованных экспертах, документах, содержащих правила и рекомендации по сертификации.

Официальным языком является русский. Все документы (заявки, протоколы, акты, аттестаты, сертификаты и т.п.) оформляются на русском языке.

При возникновении спорных вопросов в деятельности участников сертификации заинтересованная сторона может подавать апелляцию в ОС, ЦОС, Госстандарт России, другие федеральные органы, проводящие работы по сертификации. Указанные органы рассматривают вопросы, связанные с деятельностью участников работ по сертификации, применению знаков соответствия, выдачи и отмены сертификатов и аттестатов аккредитации. Сертификация проводится по схемам, установленным системами сертификации однородной продукции или группы услуг.

Схемы сертификации продукции

Схема сертификации – определённая совокупность действий, официально принимаемая в качестве доказательства соответствия продукции заданным требованиям (таблица 2).

Таблица 2- Схемы сертификации

Но мер схемы	Испытания в аккредитованных испытательных лабораториях и другие способы доказательства соответствия	Проверка производства (системы качества)	Инспекционный контроль сертифицированной продукции (системы качества, производства)
1	Испытания типа	-	-
1a	Испытания типа	Анализ состояния производства	-

2	Испытания типа	-	Испытания образцов, взятых у продавца
2а	Испытания типа	Анализ состояния производства	Испытания образцов, взятых у продавца. Анализ состояния производства
3	Испытания типа	-	Испытание образцов, взятых у изготовителя
3а	Испытание типа	Анализ состояния производства	Испытание образцов, взятых у изготовителя. Анализ состояния производства
4	Испытание типа	-	Испытания образцов, взятых у продавца. Испытание образцов, взятых
			у изготовителя
4а	Испытание типа	Анализ состояния производства	Испытания образцов, взятых у продавца. Испытание образцов, взятых у изготовителя. Анализ состояния производства
5	Испытания типа	Сертификация производства или сертификация системы качества	Контроль сертифицированной системы качества (производства). Испытания образцов взятых у продавца и (или) у изготовителя
6	Рассмотрение декларации соответствия (с прилагаемыми документами)	Сертификация системы качества	Контроль сертифицированной системы качества
7	Испытание партии	-	-
8	Испытание каждого образца	-	-

9	Рассмотрение декларации о соответствии(с прилагаемыми документами)	-	-
9а	Рассмотрение декларации о соответствии(с прилагаемыми документами)	Анализ состояния производства	-
10	Рассмотрение декларации о соответствии(с прилагаемыми документами)		Испытание образцов, взятых у изготовителя и у продавца
10а	Рассмотрение декларации о соответствии(с прилагаемыми документами)	Анализ состояния производства	Испытания образцов, взятых у изготовителя и у продавца. Анализ состояния производства

Из таблицы видно, что в качестве способов доказывания используют: 1) испытание, 2) проверку производства, 3) инспекционный контроль, 4) рассмотрение декларации о соответствии (с прилагаемыми документами).

Один или совокупность нескольких способов доказательства определяют содержание схемы определённого номера.

В схемах 1-5 производится испытание типа, т.е. одного или нескольких образцов, являющихся её типовыми представителями. Испытание в схеме 7 - это уже контроль качества партии путём испытания средней пробы (выборки), отбираемой от партии путём испытания средней пробы (выборки), отбираемой от партии с использованием метода статистического контроля. В схеме 8 испытанию подвергается каждая единица продукции. Таким образом,

жесткость испытаний, а значит, надёжность и стоимость испытаний возрастают по направлению 1-7-8.

Второй способ доказательства - проверка производства применяется тогда, когда для объективной оценки качества недостаточно испытаний, а необходим анализ технологического процесса для оценки стабильности качества продукции. Для оценки производства скоропортящейся продукции этот способ доказательства является главным (схема 6), так как сроки годности продукции меньше времени, необходимого для организации и проведения испытаний в ИЛ.

Проверка производства проходит также с различным уровнем жесткости. При проверке в форме «анализ состояния производства» (схемы 1а, 2а, 4а, 9а, 10а) проверяется два элемента качества. Предусмотренные ГОСТ Р ИСО 9001 – 96. В схеме 5, предусматривающей сертификацию производства, проверяются 10 элементов качества. При сертификации системы качества (схемы 5,6) проверяются 20 элементов, причём проверку производства имеют право проводить эксперты, аккредитованные в области проверки систем качества.

Таким образом, жесткость проверки производства, а значит, надёжность проверки стабильности качества будет наиболее высокой при сертификации системы качества.

Инспекционный контроль (ИК) предусмотрен в большинстве схем. Его проводят после выдачи сертификата. Он может проводиться в форме испытания образцов (схемы 2, 2а, 3, 3а, 4, 4а) либо в форме контроля сертифицированной системы качества (производства). В последнем случае порядок ИК регламентирован ГОСТ Р 40.005, касающимся сертифицированных систем качества (производства).

Рассмотрение декларации о соответствии (рисунок 1) - это способ доказательства, который представляет первая сторона-изготовитель. Этот способ введён недавно и заимствован из практики сертификации в ЕС. Он заключается в том, что руководитель предприятия представляет в ОС заявление-декларацию, прилагая к последнему протоколы испытаний, а также информацию об организации на предприятии контроля качества продукции.

Схемы 1-6 и 9а-10а применяются при сертификации серийно выпускаемой продукции, схемы 7,8,9 – при сертификации выпущенной партии или единичного экземпляра. Схему 1 рекомендуется использовать при ограниченном объёме реализации и выпуска продукции. Как видно, вышеуказанные рекомендации даны, исходя из такого критерия, как объём производства продукции. Другой критерий - требования к качеству. Так, схемы 1а, 2а, 3а, 4а, 9а и 10а рекомендуется применять (вместо соответствующих схем 1, 2, 3, 9 и 10), если у ОС нет информации о возможности изготовителя данной продукции обеспечить стабильность её характеристик, подтверждённых испытаниями. Схема 5 является наиболее жесткой. Её применяют в случае, если установлены повышенные требования к стабильности характеристик выпускаемой продукции (потенциально опасные изделия техники, продукция на экспорт).

Схемы 3а, 4а, и 5 используют также при проведении работ по добровольной сертификации продукции на соответствие требованиям государственных стандартов.

Схемы 9-10а введены недавно. С введением подобных схем российская система сертификации ещё больше приблизилась к европейской системе качества. Если полученные вне сертификации документы прямо или косвенно подтверждают соответствие продукции

установленным требованиям, то ОС может выдать поставщику сертификат соответствия на основании этих документов и декларации о соответствии.

Безусловно, важным критерием выбора схемы является специфика продукции.

Схемы сертификации устанавливаются в системах (правилах) сертификации однородной продукции. Конкретную схему определяет ОС или заявитель.

При наличии у изготовителя сертификата на систему качества ему достаточно представить на конкретную продукцию декларацию о соответствии (рисунок 1).

Порядок проведения сертификации продукции

Сертификация продукции проходит по следующим основным этапам:

- подача заявки на сертификацию;
- рассмотрение и принятие решения по заявке;
- отбор, идентификация образцов и их испытания;
- проверка производства (если предусмотрена схемой сертификации);
- анализ полученных результатов, принятие решения о возможности выдачи сертификата;
- выдача сертификата и лицензии (разрешения) на применение знака соответствия;
- инспекционный контроль за сертифицированной продукцией в соответствии со схемой сертификации.

При сертификации по отдельным схемам некоторые этапы могут не предусматриваться. Рассмотрим содержание каждого этапа.

1. Для проведения сертификации заявитель направляет заявку в соответствующий ОС.

При наличии нескольких ОС по сертификации данной продукции заявитель вправе направить заявку в любой из них.

## ДЕКЛАРАЦИЯ О СООТВЕТСВИИ

---

наименование организации-изготовителя, продавца (далее заявителя)

---

код ОКПО или номер регистрационного документа индивидуального предпринимателя

---

Юридический адрес\_

---

Телефон\_\_\_\_\_Факс\_\_\_\_\_Телекс\_\_\_\_\_в лице\_\_\_\_\_

фамилия, имя, отчество организации (продавца)

\_\_\_\_\_ заявляет, что продукция \_\_\_\_\_

---

тип, марка, КОД ОК 005 (ОКП) и (или) ТИ ВЭД СНГ выпускаемая по \_\_\_\_\_  
наименование и обозначение

---

документация изготовителя (стандарт, ТУ, КД, образец-эталон)

---

серийный выпуск, или партия определённого размера, или единица продукции  
соответствует требованиям \_\_\_\_\_  
наименование и обозначение

---

нормативного документа, номера пунктов Дополнительные сведения \_\_\_\_\_  
документа подтверждающие соответствие продукции

---

требованиям нормативных документов Руководитель организации \_\_\_\_\_  
подпись                      инициалы фамилия

М. П, Дата

Рисунок 1 – Форма декларации о соответствии (как способа доказательства соответствия в отдельных схемах сертификации).

Напомним, что заявителем может быть любое юридическое лицо (или индивидуальный предприниматель), представляющее продукцию на сертификацию, признающие правила системы сертификации и обязывающееся оплатить расходы на её проведение.

При обязательной сертификации по схеме с использованием декларации о соответствии заявитель подаёт в ОС вместе с заявкой и декларацию о соответствии.

2. ОС рассматривает заявку и (не позднее 15 дней) сообщает заявителю решение. В решении содержатся все основные условия сертификации, в частности: схема сертификации (если заявитель сам её предложил); перечень необходимых документов, перечень аккредитованных ИЛ; перечень органов, которые могут провести сертификацию производства или системы качества (если это предусмотрено



схемой сертификации). Выбор конкретной ИЛ, ОС для сертификации системы качества (производства) осуществляет заявитель.

В соответствии с «Положением о системе сертификации ГОСТ Р» к сертификации допускается продукция, пригодная для использования по назначению, имеющая необходимую маркировку и техническую документацию, содержащую информацию о продукции в соответствии с законодательством РФ (по товарам – в соответствии с Законом РФ «О защите прав потребителей»).

3. Отбор образцов для испытаний осуществляет, как правило, ИЛ. Испытания проводят на образцах, конструкция, состав и технология изготовления которых должны быть такими же, как у продукции, поставляемой потребителю (заказчику).

Количество образцов, порядок их отбора и хранения устанавливаются в соответствии с НД или организационно-методическими документами по сертификации.

Осуществляемая на данном этапе идентификация должна подтвердить подлинность продукции, в частности соответствие наименованию, номеру партии, указанному на маркировке.

Испытания проводятся в ИЛ, аккредитованных на право проведения тех испытаний, которые предусмотрены в НД, используемых при сертификации данной продукции. Протоколы испытаний представляются заявителю и в ОС. Копии протоколов испытаний и испытанные образцы подлежат хранению в течение срока действия сертификата.

4. В зависимости от схемы сертификации могут производиться анализ состояния производства (схемы 2а, 4а, 9а, 10а), сертификация производства и системы качества (схемы 5 и 6).

5. ОС после анализа протоколов испытаний, проверки производства осуществляет оценку соответствия продукции установленным требованиям. В случае положительных результатов ОС оформляет сертификат и регистрирует его. Сертификат действителен только при наличии регистрационного номера. При обязательной сертификации сертификат выдаётся, если продукция соответствует всем требованиям всех НД, установленных для данной продукции. Обязательной составной частью сертификата соответствия является сертификат пожарной безопасности.

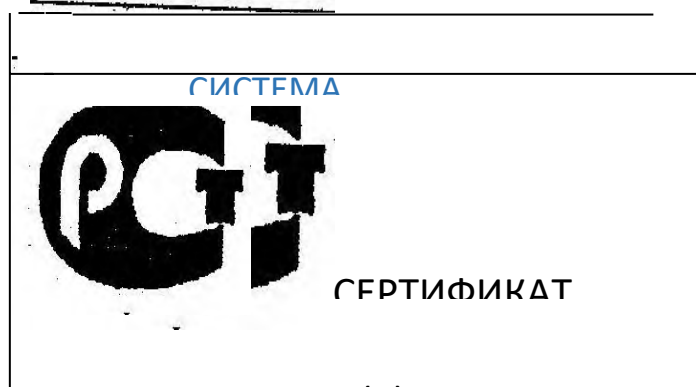
Поскольку проверка подлинности и правильности заполнения сертификата является одной из форм входного контроля качества продукции, поступающей в организации сферы услуг (магазины, предприятия общепита и пр.), то коммерческие работники должны знать требования к форме сертификата соответствия и правила его заполнения (рисунок 2).

При отрицательных результатах обязательной сертификации выпускаемой продукции ОС должен уведомить об этом соответствующий территориальный орган государственного контроля и надзора по месту расположения изготовителя (продавца, исполнителя работ и услуг) для принятия необходимых мер по предупреждению реализации данной продукции или выполнения работ (оказания услуг).

Срок действия сертификата устанавливает ОС, но не более чем на три года. Действие сертификата на партию продукции, имеющей срок годности, должно распространяться на срок не более срока годности продукции.

Для серийно выпускаемой продукции, реализуемой изготовителем в течение срока действия сертификата, последний действителен при её поставке, продаже в течение срока службы.

В сопроводительной технической документации, прилагаемой к сертифицированной продукции (Руководство по эксплуатации, паспорт, этикетка и др.), а также в товарносопроводительной документации делается запись о проведённой сертификации (номере сертификата, сроке его действия, органе, его выдавшем).



(1)

---

Сам знак представляет сочетание РСТ и означает аббревиатуру названия стандарта – Р [оссийский] СТ [андарт] . Он указывает на национальную принадлежность знака соответствия. Маркирование продукции знаком соответствия осуществляет изготовитель (продавец).

Изготовителю (продавцу) право маркирования знаком соответствия предоставляется лицензией, выдаваемой ОС. В лицензии устанавливается обязательство изготовителя (продавца) обеспечить соответствие всей продукции, маркированной знаком соответствия, стандартам и испытанному образцу.

Знак соответствия ставится на изделие и (или) тару, сопроводительную техническую документацию. Знак соответствия наносят на тару при невозможности нанесения его непосредственно на продукцию (например, для газообразных, жидких и сыпучих материалов и веществ).

Инспекционный контроль (ИК) за сертифицированной продукцией проводится (если это предусмотрено схемой сертификации) в течение всего срока действия сертификата и лицензии не реже одного раза в год в форме периодических и внеплановых проверок, включающих испытания образцов продукции, анализ состояния производства и пр. Цель инспекционного контроля, как это уже указывалось выше, - подтверждение соответствия реализуемой продукции установленным требованиям.

Внеплановые проверки могут проводиться в случаях поступления информации о претензиях к качеству продукции от потребителей, торговых организаций, а также надзорных органов.

Результаты ИК оформляют актом. По результатам ОС может приостановить или отменить действие сертификата и аннулировать лицензию на право применения знака соответствия в случае несоответствия продукции требованиям НД. ИК осуществляют, как правило, ОС, проводящие сертификацию данной продукции.

## **2.2. Перечень вопросов и заданий для промежуточной аттестации**

Контрольные вопросы.

1. Законодательство Российской Федерации в области защиты информации. Требования безопасности к серверам баз данных. Классы защиты
2. Основные группы методов противодействия угрозам безопасности в корпоративных сетях
3. Программно-аппаратные методы защиты процесса обработки и передачи информации. Политика безопасности, настройка политики безопасности
4. Виды неисправностей систем хранения данных
5. Резервное копирование: цели, методы, концепции, планирование, роль журнала транзакций. Виды резервных копий
6. Утилиты резервного копирования
7. Восстановление базы данных: основные алгоритмы и этапы
8. Восстановление носителей. Воссоздание утраченных файлов. Полное восстановление. Неполное восстановление
9. Мониторинг активности и блокирование
10. Автоматизированные средства аудита
11. Брандмауэры. Уровни качества программной продукции
12. Требования к конфигурации серверного оборудования и локальных сетей. Оформление

требований. Техническое задание.

13. Объекты информатизации, требующие обязательной сертификации программных средств и обеспечения
14. Сертификаты безопасности: виды, функции, срок действия. Проверка наличия сертификата безопасности
15. Системы сертификации. Процедура сертификации.
16. Платформы и центры сертификации. Сертификат разработчика. Процесс подписи и проверки кода

SSL сертификат: содержание, формирование запроса, проверка данных с помощью сервисов

## **1. Методические рекомендации по написанию реферата**

Реферат – первая и наиболее частая для студентов с первых курсов обучения форма работы, которая наилучшим образом, обогащает знания и развивает аналитические способности, т.е. способствует формированию профессиональных компетенций, а в воспитательном плане – формирует ответственность и сочетание личного интереса с общественной необходимостью, то есть качества необходимые для будущего специалиста.

Структура работы

Структура работы, соотношение объема работ по главам в каждом конкретном случае определяются в зависимости от темы, объекта, предмета и целевой направленности исследования.

Типовая структура включает следующие разделы:

1. Титульный лист.
2. Оглавление.
3. Введение.
4. Главы основной части.
5. Заключение.
6. Список используемой литературы и информационных источников.
7. Приложения.

Титульный лист - первая страница работы (на данной странице номер не ставится).

Оглавление - помещается после титульного листа, в нем приводятся пункты работы с указанием страниц (на данной странице номер не ставится).

Введение - кратко обосновывается актуальность выбранной темы, цель и содержание поставленных задач, формулируется объект и предмет исследования, указывается избранный метод исследования. Дается характеристика работы – относится ли она к теоретическим исследованиям или к прикладным, сообщается, в чем заключается значимость и прикладная ценность полученных результатов, приводится характеристика источников для написания работы и краткий обзор имеющейся по данной теме литературы.

Основная часть - подробно приводится методика и техника исследования, даются сведения об объеме исследования, излагаются и обсуждаются полученные результаты. Содержание основной части должно точно соответствовать теме работы и полностью ее раскрывать.

Заключение - содержит основные выводы, к которым автор пришел, в процессе анализа материала (при этом должна быть подчеркнута самостоятельность, новизна, теоретическое и практическое значение полученных результатов).

Список используемой литературы и информационных источников - приводится в конце работы, в алфавитном порядке сначала указываются источники используемой литературы, затем интернет-источники. Допускается использовать в списке литературы источники не позднее 5-летней давности.

Приложение - помещают вспомогательные или дополнительные материалы. В случае необходимости можно привести дополнительные таблицы, рисунки, графики и т.д., если они помогут лучшему пониманию полученных результатов.

Требования к оформлению работы

Объем работы должен быть 20-30 страниц.

Текст набирается в текстовом редакторе MS Word: шрифт TimesNewRoman, размер – 14 пт, цвет шрифта черный, междустрочный интервал – полуторный (или 1,15), отступ первой строки (абзацный отступ) – 1,25 см, выравнивание текста – по ширине, расстановка переносов по тексту – автоматическая, в режиме качественной печати. Оглавление должно быть сформировано автоматически. Текст распечатывается на принтере.

Заголовки разделов печатаются строчными буквами с абзацного отступа.

Заголовки подразделов печатаются строчными буквами (кроме первой прописной), располагаются с абзацного отступа. Заголовки пунктов печатаются строчными буквами (кроме первой прописной), с использованием шрифтового выделения (полужирный шрифт), начиная с абзаца. Если заголовок состоит из двух или более предложений, их разделяют точкой. Заголовки подпунктов печатают строчными буквами (кроме первой прописной), начиная с абзаца в подбор к тексту.

В конце заголовков структурных частей, наименований разделов и подразделов точка не ставится. Расстояние между заголовком структурной части (за исключением заголовка пункта) и подразделом должно быть равно 2 интервалам.

Разделы должны иметь порядковую нумерацию в пределах всего текста. Номер раздела указывается перед его названием, после номера раздела точка не ставится, перед заголовком оставляют пробел. Наименования разделов печатаются строчными буквами с абзацного отступа, выделяются полужирным шрифтом размером 16 пт, точка в конце наименования раздела не ставится. Разделы работы оформляются, начиная с новой страницы.

Иллюстрации обозначают словом «Рисунок» и нумеруют последовательно в пределах раздела реферата или сквозной нумерацией. Номер иллюстрации может состоять из номера раздела и порядкового номера иллюстрации, разделенных точкой. Например: «Рисунок 1.2» (второй рисунок первого раздела). Номер иллюстрации, ее название и поясняющие подписи помещают последовательно под иллюстрацией. Если в работе приведена одна иллюстрация, то ее не нумеруют и слово «Рисунок» не пишут. Иллюстрации должны иметь наименование, которое дается после номера рисунка. Точка после номера рисунка и наименования иллюстрации не ставится.

Каждая таблица должна иметь название, которое следует помещать над таблицей слева, без абзацного отступа в одну строку с ее номером через тире. Расстояние от текста до таблицы и от таблицы до последующего текста равно одной строке. Между наименованием таблицы и самой таблицей не должно быть пустых строк.

*Пример.*

Таблица (номер) – Название таблицы


Приложения оформляют как продолжение реферата на последующих страницах, располагая их в порядке появления ссылок в тексте.

Каждое приложение следует начинать с нового листа (страницы) с указанием наверху справа страницы слова «Приложение», напечатанного строчными буквами. Приложение должно иметь содержательный заголовок, расположенный в следующей строке по центру. Если в реферате более одного приложения, их нумеруют последовательно цифрами, например, Приложение 1, Приложение 2 и т.д.

Критерии оценки реферата

К *общим критериям* можно отнести:

соответствие реферата теме.

глубина и полнота раскрытия темы.

адекватность передачи первоисточника.

логичность, связность.

доказательность.

структурная упорядоченность (наличие введения, основной части, заключения, их оптимальное соотношение).

оформление (наличие оглавления, списка литературы, культура цитирования, сноски и т.д.).  
языковая правильность.

Общая оценка за реферат выставляется следующим образом: если студент выполнил от 65% до 80% указанных выше требований, ему ставится минимальный балл – 3 (удовлетворительно); 80-90% — средний балл – 4 (хорошо); 90-100% — максимальный балл – 5 (отлично).

## 2. Методические рекомендации по созданию презентации

В оформлении презентаций выделяют два блока: оформление слайдов и представление информации на них. Для создания качественной презентации необходимо соблюдать ряд требований, предъявляемых к оформлению данных блоков.

Оформление слайдов:

Стиль	<ul style="list-style-type: none"><li>- Соблюдайте единый стиль оформления</li><li>- Избегайте стилей, которые будут отвлекать от самой презентации.</li><li>- Управляющие кнопки не должны преобладать над основной информацией (текстом, иллюстрациями).</li><li>- Для фона и заголовка используйте контрастные цвета. Не используйте на одном слайде больше трех цветов.</li></ul>
Фон и цвет	<ul style="list-style-type: none"><li>- Для фона предпочтительны холодные тона</li><li>- На одном слайде рекомендуется использовать не более трех цветов: один для фона, один для заголовка, один для текста.</li><li>- Для фона и текста используйте контрастные цвета.</li><li>- Обратите внимание на цвет гиперссылок.</li></ul>
Анимационные эффекты	<ul style="list-style-type: none"><li>- Используйте возможности компьютерной анимации для представления информации на слайде.</li><li>- Не стоит злоупотреблять различными анимационными эффектами, они не должны отвлекать внимание от содержания информации на слайде.</li></ul>

Представление информации:

Содержание информации	<ul style="list-style-type: none"><li>- Используйте короткие слова и предложения.</li><li>- Минимизируйте количество предлогов, наречий, прилагательных.</li><li>- Заголовки должны привлекать внимание аудитории.</li></ul>
Расположение информации на странице	<ul style="list-style-type: none"><li>- Предпочтительно горизонтальное расположение информации.</li><li>- Наиболее важная информация должна располагаться в центре экрана.</li><li>- Если на слайде располагается картинка, надпись должна располагаться под ней.</li></ul>
Шрифты	<ul style="list-style-type: none"><li>- Для заголовков – не менее 24.</li><li>- Для информации не менее 18.</li><li>- Шрифты без засечек легче читать с большого расстояния.</li><li>- Нельзя смешивать разные типы шрифтов в одной презентации.</li><li>- Для выделения информации следует использовать жирный шрифт, курсив или подчеркивание.</li><li>- Нельзя злоупотреблять прописными буквами.</li></ul>
Способы выделения информации	<p>Следует использовать:</p> <ul style="list-style-type: none"><li>- рамки; границы, заливку;</li><li>- штриховку, стрелки;</li></ul>

	- рисунки, диаграммы, схемы для иллюстрации наиболее важных фактов.
Объём информации	- Не стоит заполнять один слайд слишком большим объемом информации: люди могут одновременно запомнить не более трех фактов, выводов, определений. - Наибольшая эффективность достигается тогда, когда ключевые пункты отображаются по одному на каждом отдельном слайде.
Виды слайдов	Для обеспечения разнообразия следует использовать разные виды слайдов: - с текстом; - с таблицами, диаграммами.

#### Критерии оценки презентации

Общая оценка за презентацию выставляется следующим образом: если студент выполнил от 65% до 80% указанных выше требований, ему ставится минимальный балл – 3 (удовлетворительно); 80-90% — средний балл – 4 (хорошо); 90-100% — максимальный балл – 5 (отлично).

### 3. Методические рекомендации по написанию доклада

Доклад должен быть подготовлен на русском языке. Объем текста от 8 до 12 стр. (от 5000 до 30000 знаков без учета пробелов)

Для набора текста использовать программу Microsoft Word версии не выше 2003, для набора формул – Microsoft Equation 3.0.

В тексте статьи нужно использовать только международную систему единиц измерений (СИ).

Поля:

верхнее – 25мм;

нижнее – 20 мм;

левое – 30 мм;

правое – 20 мм;

красная строка 12,5 мм.

Бумага белая для офисной техники формата 210 x 297.

Качество печати – высокое.

В целях обеспечения унификации текстов в сборнике трудов конференции необходимо при оформлении доклада соблюсти следующие требования:

а) Название работы должно удовлетворять следующим требованиям: шрифт - Times New Roman, размер шрифта – 14, стиль – обычный, масштаб – 100%, интервал – обычный, смещение – нет, всё название должно быть написано жирным шрифтом и буквы должны быть прописными. Тип распределения текста на странице – по центру. Заголовки разделов оформляются аналогично названию работы, но только с одной заглавной, остальные буквы строчные.

б) После названия работы должны быть перечислены инициалы и фамилии авторов, а также с новой строки - название учреждения, которое данные авторы представляют. Требования к написанию: шрифт - Times New Roman, размер шрифта – 14, стиль – обычный, масштаб – 100%, интервал – обычный, смещение – нет, должно быть написано курсивом. Тип распределения текста на странице – по ширине.

в) Между названием и данными об авторе должна быть одна пустая строка.

г) Весь основной текст доклада набирается со следующими параметрами: шрифт - Times New Roman, размер шрифта – 14, стиль – обычный, масштаб – 100%, интервал – обычный, смещение – нет. Тип распределения текста на странице – по ширине.

д) Междустрочные интервалы принять одинарными.

е) При необходимости набора формул должен быть использован формульный редактор – Microsoft Equation 3.0:

шрифт Times New Roman или Symbol;

кегель -12;

надстрочные и подстрочные индексы кегель – 9.

положение по горизонтали должно совпадать с положением текста соответствующей строки

формулы, записанные в отдельной строке, должны располагаться по центру, а номер их – подогнан к правой границе листа.

ж) Надписи на рисунках и подрисуночные надписи, обозначения физических величин и их единиц, другие данные, помещаемые в таблицы, а также заголовки таблиц граф – шрифту 14.

з) Номера рисунков как в основном тексте так и в подрисуночной надписи приводить к виду – Рис. ....(№. Рисунок). Подрисуночная надпись должна располагаться вне “тела” рисунка.

и) Иллюстративный материал представляется только черно-белый.

Графические иллюстрации - в формате \*.wmf (векторная графика) или \*.tif (с глубиной цвета 1 бит), фотографии - в растровом формате \*.tif. При этом все элементы на иллюстрациях должны быть четкими, а надписи - свободно читаемыми; располагаться в центре листа.

к) Подрисуночная надпись аналогично располагается в центре листа. Номер таблицы указывается в виде – Таблица №, располагается по правой границе листа над самой таблицей, между таблицей и её номером должна быть одна пустая строка.

л) Список использованной литературы должен быть составлен по порядку ссылок в тексте. Необходимо представлять полный список, касающийся рассматриваемой темы. Настоятельно рекомендуется исключать самоцитирование.

Критерии оценки доклада

К *общим критериям* можно отнести:

соответствие доклада теме.

глубина и полнота раскрытия темы.

адекватность передачи первоисточника.

логичность, связность.

доказательность.

структурная упорядоченность (наличие введения, основной части, заключения, их оптимальное соотношение).

оформление (наличие оглавления, списка литературы, культура цитирования, сноски и т.д.).

языковая правильность.

Общая оценка за доклад выставляется следующим образом: если студент выполнил от 65% до 80% указанных выше требований, ему ставится минимальный балл – 3 (удовлетворительно); 80-90% — средний балл – 4 (хорошо); 90-100% — максимальный балл – 5 (отлично).

#### **4. Методические рекомендации по заполнению таблиц**

Таблица (из лат. *tabula* «доска») — способ передачи содержания, заключающийся в организации структуры данных, в которой отдельные элементы помещены в ячейки, каждой из которых сопоставлена пара значений — номер строки и номер колонки. Таким образом, устанавливается смысловая связь между элементами, принадлежащими одному столбцу или одной строке.

Таблицы являются удобной формой для отображения информации. Но таблицы выполняют лишь тогда свою цель, когда между строчками и столбцами имеется смысловая связь, то есть информацию в них можно рассортировать неким образом, например, по дате или алфавиту.

Алгоритм заполнения таблицы.

Прочтите названия оглавлений таблицы.

Прочтите текст учебника и с помощью карандаша, укажите в нем материалы к каждой графе.



3. Запишите в соответствующие графы таблицы указанные материалы из текста в сокращенном виде.

Критерии оценки результата

Уровни освоения	Характеристика уровня
Допустимый (удовлетворительно)	- Таблица заполнена верно на 50%
Высокий (хорошо)	- Таблица заполнена верно более чем на 50%
Оптимальный (отлично)	- Таблица заполнена в полном объеме.

## 5. Методические рекомендации по составлению схем

Схемы как графические документы (графическая модель системы), на которых в виде условных обозначений или изображений показаны составные части некоторой системы и связи между ними.

Алгоритм составления схем

Прочтите предложенный текст и запишите его название

Укажите карандашом в книге основные разделы, из которых состоит текст и дайте им названия.

Проведите от названия текста стрелки вниз и подпишите возле каждой из них названия разделов текста.

Дополните схему примерами.

Критерии оценки результата

Уровни освоения	Характеристика уровня
Допустимый (удовлетворительно)	- все элементы присутствуют, отсутствует логика составления
Высокий (хорошо)	- схема составлена с небольшими упущениями
Оптимальный (отлично)	- схема составлена логически верно.

## 6. Методические рекомендации по составлению конспекта

Конспект - это последовательная фиксация информации, отобранной и обдуманной в процессе чтения.

Конспект:

подразумевает объединение плана, выписок и тезисов;

показывает внутреннюю логику изложения;

содержит основные выводы и положения, доказательства, приемы;

отражает отношение составителя к материалу;

может использоваться не только самим автором (составителем), но и другими читателями.

Основные требования к написанию конспекта: системность и логичность изложения материала, краткость, убедительность и доказательность.

При составлении конспекта необходимо избегать многословия, излишнего цитирования, стремления сохранить систематическую особенность текста в ущерб его логике.

Виды конспектов графически представлены на рис. 1.



Рис. 1. Виды конспектов

Общий алгоритм конспектирования состоит в следующем:

Общий алгоритм конспектирования состоит в следующем:

прочитать текст, отметить в нём новые слова, непонятные места, имена, даты; составить перечень основных мыслей, содержащихся в тексте, составить простой план, который поможет группировать материал в соответствии с логикой изложения;

выяснить в словаре значение новых непонятных слов, выписать их в тетрадь или словарь в конце тетради;

вторично прочитать текст, сочетая чтение с записью основных мыслей автора и их иллюстраций. Запись ведется своими словами, не переписывая текст. Важно стремиться к краткости, пользуясь правилами записи текста;

прочитать конспект ещё раз, доработать его.

Вместе с тем существуют некоторые особенности создания конспектов различных видов. Остановимся кратко на этом вопросе.

*Конспектирование* - процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста.

*Выделение главной мысли* - одна из основ умственной культуры при работе с текстом. «Отбирать полезнейшее, - писал великий чешский педагог XVII века Я.А.Коменский, - дело такой важности, что немыслим толковый читатель, без умения отбирать. Единственно надежный плод чтения - усвоение прочитанного, выбор полезного. Поистине только это держит ум в напряжении, запечатляет воспринятое в памяти и озаряет ум все более ярким светом. Не пожелать выделить из книги ничего, значит все пропустить».

*Результат конспектирования* - запись, позволяющая конспектирующему немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в

перевод с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других.

План-конспект - это сжатый в форме плана пересказ прочитанного или услышанного.

Характеристика конспекта: краток, прост, быстро составляется и заполняется. Положительной чертой этого вида конспектов является то, что он учит выбирать главное, чётко и логично излагать мысли, даёт возможность усвоить материал ещё в процессе его изучения. Всё это делает его незаменимым при быстрой подготовке доклада, выступления. Однако работать с ним через некоторое время трудно, так как плохо восстанавливается в памяти содержание материала.

Этапы работы:

Составь план прочитанного текста или воспользуйся готовым.

Разъясни кратко и доказательно каждый пункт плана, выбери разумную и эффективную форму записи.

Сформулируй и запиши вывод.

План-конспект может выглядеть как таблица. Например:

Основные вопросы	Раскрытие вопросов
1. Сущность, содержание, основные характеристики бренда.	<p>Бренд — это атрибуты фирмы или товара, которые отражают их индивидуальность, привлекают внимание клиентов, создают имидж фирме, репутацию, способствуя продвижению товара на рынках.</p> <p>Российскими авторами бренд трактуется как раскрученная торговая марка.</p> <p>Символ бренда должен:</p> <ul style="list-style-type: none"> <li>наиболее точно и полно отражать содержание товара;</li> <li>обеспечить максимальное отличие от конкурентных брендов;</li> <li>сформировать у потребителя убеждения, что этот бренд уникальный.</li> </ul> <p>Уникальность символа бренда – главное требование при формировании бренда</p>
2. Взаимосвязь бренда с экономическими категориями «потребность», «спрос», «предложение».	
3. Технологии.	
4. Управление активами бренда	
и др.	

Ключевые слова	Суть, основная мысль	Раскрытие основной мысли	Заключение, вопросы, личные отношения

Задание для работы при этом может быть сформулировано следующим образом:

Вариант 1. Внимательно прочтите предложенный текст (тексты) в учебнике (учебниках или распечатке). Представьте его в виде конспекта. На его основе составьте тезисы и план.

Вариант 2. Внимательно прочтите предложенный текст в учебнике или распечатке. Законспектируйте его, используя предложенный преподавателем план. Оформите план-конспект.

Вариант 3. Внимательно прочтите предложенный текст в учебнике или распечатке. Законспектируйте его, используя вид конспекта - тематический обзорный (раскрывает конкретную тему использованием нескольких источников).

Цитатный конспект — это конспект, созданный из цитат.

Характеристика конспекта: строится из высказываний тора, из изложенных им фактов. Чаще всего этот вид конспекта используется для работы с первоисточником. К нему студент может

обращаться неоднократно. Но он не способствует актив мыслительной работе, поэтому, как правило, служит только люстрацией к изучаемой теме.

Этапы работы:

Прочитать текст, отметить в нём основное содержание, главные мысли, выделить те цитаты, которые войдут в конспект.

Пользуясь правилами сокращения цитат, выписать их в тетрадь. Форма записи может быть разной, например:

... (цитата);

... (цитата); (вывод);

основные вопросы; доказательства (цитаты); выводы.

Прочитать написанный текст, сверить его с оригиналом.

Сделать общий вывод.

Опорный конспект — это отражение изложения информации заложенной в тексте в виде опорных сигналов - слов, условных знаков, рисунков.

Характеристика конспекта: краток, учит выбирать главное, наглядно отражает причинно-следственные связи, развивает логическое мышление и образное умение моделировать информацию. Незаменим при повторении материала к зачёту, экзамену.

Этапы работы:

Прочитать внимательно текст.

Разделить его на смысловые части - блоки.

Поставить к каждой части вопрос.

Ответить на поставленный вопрос опорными сигналами, расположив их в виде логической схемы.

Свободный конспект — это сочетание выписок, цитат, тезисов.

Характеристика конспекта: он требует серьёзных усилий от студента при составлении, так как требует умений активного использования всех типов записей: планов, тезисов, выписок. Однако именно этот вид конспектов в высшей степени способствует прочному усвоению учебного материала.

Этапы работы:

Используя имеющиеся источники, выбрать материал по интересующей теме, изучить его и глубоко осмыслить.

Сделать необходимые выписки основных мыслей, цитат, составить тезисы.

Используя подготовленный материал, сформулировать основные положения по теме.

Тематический конспект — это конспект ответа на поставленный вопрос или конспект учебного материала по определенной теме.

Характеристика конспекта: он может быть обзорным и хро. но логическим; учит анализировать различные точки зрения на один и тот же вопрос, привлекать имеющиеся знания и личный опыт; используется в процессе работы над докладом, сообщением, рефератом.

Этапы работы:

Изучить несколько источников и сделать из них выборку материала по определённой теме или хронологии.

Мысленно оформить прочитанный материал в виде плана.

Пользуясь этим планом, кратко своими словами изложить осознанный материал.

Критерии результатов знаний и умений

«5» - уровень освоения студентом учебного материала достаточно высок, студент умеет использовать теоретические знания при выполнении практических задач с практикой, подтверждает сформированность общих и профессиональных компетенций;

«4» - студент полно освоил учебный материал, владеет понятийным аппаратом, ориентируется в изученном материале, осознанно применяет знания для решения практических задач, грамотно излагает ответ, но содержание и форма ответа имеют отдельные неточности;

«3» - студент знает и понимает основные положения учебного материала, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических задач не умеет доказательно обосновать свои суждения;

«2» - студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, искажает их смысл, беспорядочно и неуверенно излагает материал, не может применять знания для решения практических задач.

## **Критерии результатов знаний и умений**

### **1. Практические занятия.**

Оценка «отлично» ставится в том случае, если учащийся:

- выполнил работу в полном объеме с соблюдением необходимой
- последовательности проведения опытов и измерений;
- самостоятельно и рационально выбрал и подготовил для занятия необходимое оборудование, все работы провел в условиях и режимах, обеспечивающих получение результатов и выводов с наибольшей точностью;
- в представленном отчете правильно и аккуратно выполнил все записи, таблицы, рисунки, чертежи, графики, вычисления и сделал выводы;
- соблюдал требования безопасности труда.

Оценка «хорошо» ставится в том случае, если выполнены требования к оценке «5», но:

- было допущено два-три недочета, или не более одной негрубой ошибки и одного недочета.

Оценка «удовлетворительно» ставится, если работа выполнена не полностью, но объем выполненной части таков, что позволяет получить правильные результаты и выводы, или если в ходе проведения работы и измерений были допущены следующие ошибки:

- задание проводилось в нерациональных условиях, что привело к получению результатов с большим количеством ошибок,
- или в отчете были допущены в общей сложности не более двух ошибок (в записях единиц, измерениях, в вычислениях, графиках, таблицах, схемах, анализе погрешностей и т. д.), не принципиального для данной работы характера, но повлиявших на результат выполнения,
- или не выполнен совсем или выполнен неверно анализ погрешностей;
- или работа выполнена не полностью, однако объем выполненной части таков, что позволяет получить правильные результаты и выводы по основным, принципиально важным задачам работы.

Оценка «неудовлетворительно» ставится в том случае, если:

- работа выполнена не полностью, и объем выполненной части работы не позволяет сделать правильных выводов,
- или в ходе работы и в отчете обнаружилось в совокупности все недостатки,
- отмеченные в требованиях к оценке «3».

### **2. Практические занятия.**

Контрольная работа.

Оценка отлично ставится если обучающийся

- полно раскрыл содержание материала в объеме, предусмотренном рабочей программой,
- изложил материал грамотным языком в определенной логической последовательности, точно используя специальную терминологию;
- правильно выполнил рисунки, чертежи, сопутствующие ответу;
- отвечал самостоятельно без наводящих вопросов преподавателя. Возможны одна-две неточности при освещении второстепенных вопросов или в выкладках, которые студент легко исправил по замечанию преподавателя.

Оценка хорошо ставится если обучающийся

- в изложении допущены небольшие пробелы, не исказившие содержание ответа;
- допущены один – два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя;
- допущена ошибка или имеется более двух недочетов при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию преподавателя.

Оценка удовлетворительно ставится если обучающийся

- неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса;
- имелись затруднения или допущены ошибки в определении понятий, использовании терминологии и выкладках (определениях), исправленные после нескольких наводящих вопросов преподавателя;
- при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

Оценка неудовлетворительно ставится если обучающийся

- не раскрыл основное содержание учебного материала;
- обнаружено незнание или непонимание студентом большей или наиболее важной части учебного материала;
- допущены ошибки в определении понятий, при использовании терминологии, в выкладках, которые не исправлены после нескольких наводящих вопросов преподавателя.

Тестовое задание

- Оценка отлично ставится если обучающийся ответил более чем на 85% вопросов.
- Оценка хорошо ставится если обучающийся ответил на 75-84% вопросов.
- Оценка хорошо ставится если обучающийся ответил на 74-60% вопросов.
- Оценка хорошо ставится если обучающийся ответил менее чем на 59% вопросов.

**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

<b>№ п.п.</b>	<b>Содержание изменения</b>	<b>Дата, номер протокола заседания кафедры, подпись зав.кафедрой</b>
1	2	3
1		
2		
3		
4		