Приложение

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
МДК 07.02 Сертификация информационных систем

09.02.07. Информационные системы и программирование

Паспорт (ФОС) для контроля освоения МДК 07.02 Сертификация информационных систем

ФОС предназначен для осуществления контроля и оценки результатов освоения обучающимися МДК 07.02 Сертификация информационных систем, относящегося к ПМ.07 Соадминистрирование баз данных и серверов. Предметом оценки являются умения, знания и практический опыт в соответствии с ФГОС специальности 09.02.07 Информационные системы и программирование, освоение которых направлено на формирование общих и профессиональных компетенций, предусмотренных этим же стандартом.

В частности, текущему контролю подлежат следующие умения, знания и практический опыт:

(Умения)

У. 1 проектировать и создавать базы данных;

У.2 выполнять запросы по обработке данных на языке SQL;

У.3 осуществлять основные функции по администрированию баз данных;

У. 4 разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных;

У. 5 владеть технологиями проведения сертификации программного средства.

(Знания)

3.1 модели данных, основные операции и ограничения;

3.2 технологию установки и настройки сервера баз данных;

3.3 требования к безопасности сервера базы данных;

3.4 государственные стандарты и требования к обслуживанию баз данных.

(Практический опыт)

ПО. 1 участии в соадминистрировании серверов;

ПО.2 разработке политики безопасности SQL сервера, базы данных и отдельных объектов базы данных;

ПО.3 применении законодательства Российской Федерации в области сертификации программных средств информационных технологий.

На основе перечисленных умений, знаний и практическом опыте у обучающегося должны быть сформированы следующие, предусмотренные ФГОС специальности СПО 09.02.07 Информационные системы и программирование, общие и профессиональные компетенции:

(Общие компетенции)

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

(Профессиональные компетенции)

ПК 7.1. Выявлять технические проблемы, возникающие в процессе эксплуатации баз данных и серверов.

ПК 7.2. Осуществлять администрирование отдельных компонент серверов.

ПК 7.3. Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов.

ПК 7.4. Осуществлять администрирование баз данных в рамках своей компетенции.

ПК 7.5. Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации.

Контроль и оценка осуществляются с использованием следующих форм и методов: традиционная дифференцированная система оценок в баллах («2» («неудовлетворительно»), «3» («удовлетворительно»), «4» («хороню»), «5» («отлично»)).

Задания для проведения текущего контроля по

МДК 07.02Сертификация информационных систем.

Практическая работа
Настройка политики безопасности

Цель работы: ознакомиться с методами ограничения доступа к информации

Теоретическая часть

Разграничение доступа является достаточно эффективным средством предупреждения возможного ущерба вследствие нарушения целостности или конфиденциальности информации. В том случае, если доступ к самому компьютеру или к его ресурсам может получить пользователь, который имеет злой умысел или недостаточный уровень подготовки, он может случайно или преднамеренно исказить информацию или уничтожить ее полностью или частично.

Это же обстоятельство может привести к раскрытию закрытой информации или несанкционированному тиражированию открытой, например, программ, баз данных, разного рода документации, литературных произведений и т. д. в нарушение прав собственников информации, авторских прав…

С точки зрения разграничения доступа, в информационных системах следует различать *субъекты доступа и объекты доступа*. В число *субъектов доступа* могут войти либо персонал информационной системы, либо посторонние лица. *Объектами доступа* являются аппаратно-программные элементы информационных систем. Чаще всего в качестве объектов доступа рассматриваются файлы (в том числе папки и файлы программ). Доступ к объекту может рассматриваться либо как чтение (получение информации из него), либо как изменение (запись информации в него). Тогда виды доступа определяются следующими возможными сочетаниями этих операций:

- ни чтение, ни изменение;
- только чтение;
- только изменение;

• и чтение, и изменение.

Очевидно, что различие функциональных обязанностей субъектов обусловливает необходимость предоставления им соответствующих видов доступа.

Управление доступом пользователей и глобальными параметрами на членах домена осуществляется на двух уровнях: локальной системы и домена. На отдельных компьютерах доступ пользователей конфигурируют на уровне локальной системы, а одновременно для нескольких систем или ресурсов, входящих в домен, — на уровне домена.

Права доступа пользователя определяются руководителем организации и прописываются на рабочей станции системным администратором (администратором домена).

Процедура проверки прав доступа включает авторизацию и аутентификацию. Авторизация предполагает проверку уровня доступа к объекту, а аутентификация — проверку подлинности пользователя. Для аутентификации обычно используются имя пользователя (login) и пароль (password). Системный администратор осуществляет разграничение прав доступа в соответствии с заданной системной политикой, которая предполагает:

• ограничения на минимальную длину, сложность и срок действия пароля;
• требование уникальности паролей;
• блокировку пользователя при неудачной аутентификации;
• ограничение времени и места работы пользователя.

Система разграничения доступа реализована так, что при повседневной работе пользователи не должны замечать, что любое обращение к любому объекту проходит проверку на соответствие установленным правам доступа. Списки прав доступа можно задавать на каждый документ отдельно. При создании документа автоматически задается такой доступ на него, чтобы создатель имел все права.

Система разграничения доступа предназначена для реализации определенных администратором защиты правил на выполнение операций пользователями над объектами хранилища.

Система ограничения прав доступа не может дать полной гарантии безопасности информации. Дело в том, что злоумышленник может получить или подобрать пароль легального пользователя. Кроме того, опытный специалист может обойти систему разграничения доступа. Средством обнаружения несанкционированного доступа к ресурсам служат системы аудита, которые автоматически фиксируют доступ к файлам и папкам и системные события.

Модели разграничения доступа

Наиболее распространенные модели разграничения доступа:

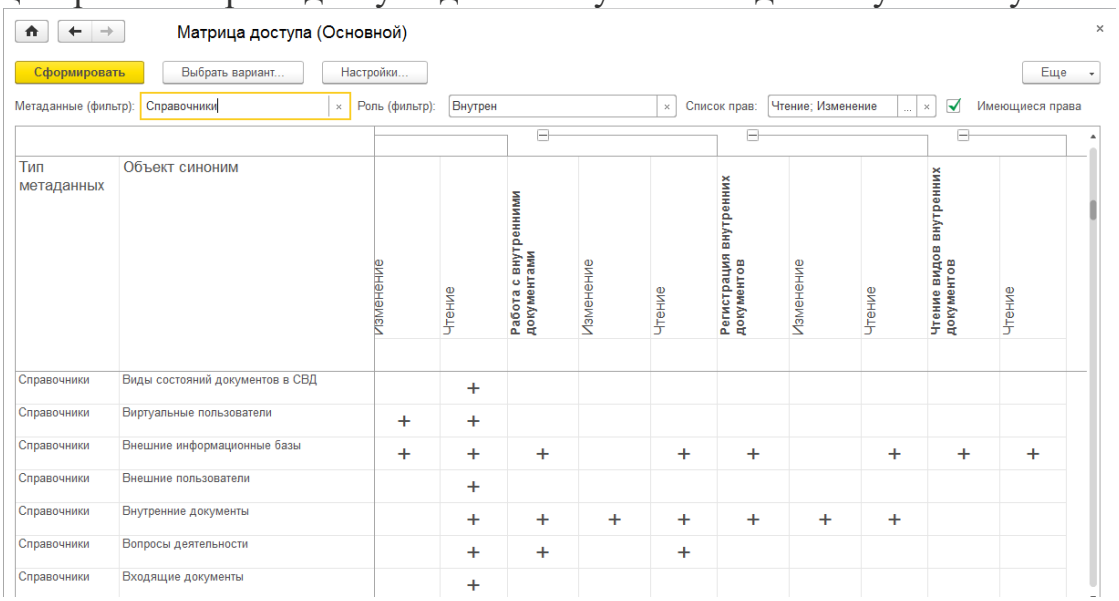
- *дискреционная* (избирательная) модель разграничения доступа;
- полномочная (*мандатная*) модель разграничения доступа.

Дискреционная модель характеризуется следующими правилами:

- ❖ любой объект имеет владельца;
- ❖ владелец имеет право произвольно ограничивать доступ субъектов к данному объекту;

- для каждого набора субъект – объект – метод право на доступ определен однозначно;
- наличие хотя бы одного привилегированного пользователя (например, администратора), который имеет возможность обращаться к любому объекту с помощью любого метода доступа.

В дискреционной модели определение прав доступа хранится в матрице доступа: в строках перечислены субъекты, а в столбцах – объекты. В каждой ячейке матрицы хранятся права доступа данного субъекта к данному объекту.



Тип метаданных	Объект синоним	Изменение	Чтение	Работа с внутренними документами	Изменение	Чтение	Регистрация внутренних документов	Изменение	Чтение	Чтение видов внутренних документов	Чтение
Справочники	Виды состояний документов в СВД		+								
Справочники	Виртуальные пользователи	+	+								
Справочники	Внешние информационные базы	+	+	+		+	+		+	+	+
Справочники	Внешние пользователи		+								
Справочники	Внутренние документы		+	+	+	+	+	+	+		
Справочники	Вопросы деятельности		+	+		+					
Справочники	Входящие документы		+								

Полномочная модель характеризуется следующими правилами:

- каждый объект обладает грифом секретности. Гриф секретности имеет числовое значение: чем оно больше, тем выше секретность объекта;
- у каждого субъекта доступа есть уровень допуска. Допуск к объекту в этой модели субъект получает только в случае, когда у субъекта значение уровня допуска не меньше значения грифа секретности объекта.

Преимущество полномочной модели состоит в отсутствии необходимости хранения больших объемов информации о разграничении доступа. Каждым субъектом выполняется хранение лишь значения своего уровня доступа, а каждым объектом – значения своего грифа секретности.

Методы разграничения доступа

Виды методов разграничения доступа:

1. **Разграничение доступа по спискам**

Суть метода состоит в задании соответствий: для каждого пользователя задается список ресурсов и права доступа к ним или для каждого ресурса определяется список пользователей и права доступа к этим ресурсам. С помощью списков возможно установление прав с точностью до каждого пользователя. Возможен вариант добавления прав или явного запрета доступа. Метод доступа по спискам используется в подсистемах безопасности операционных систем и систем управления базами данных.

2. **Использование матрицы установления полномочий**

При использовании матрицы установления полномочий применяется матрица доступа (таблица полномочий). В матрице доступа в строках записываются идентификаторы субъектов, которые имеют доступ в компьютерную систему, а в столбцах – объекты (ресурсы) компьютерной системы. В каждой ячейке матрицы может содержаться имя и размер ресурса, право доступа (чтение, запись и др.), ссылка на другую информационную структуру, которая уточняет права доступа, ссылка на программу, которая управляет правами доступа и др. Данный метод является достаточно удобным, так как вся информация о полномочиях сохраняется в единой таблице. Недостаток матрицы – ее возможная громоздкость.

3. **Разграничение доступа по уровням секретности и категориям**

Разграничение по степени секретности разделяется на несколько уровней. Полномочия каждого пользователя могут быть заданы в соответствии с максимальным уровнем секретности, к которому он допущен. При разграничении по категориям задается и контролируется ранг категории пользователей. Таким образом, все ресурсы компьютерной системы разделены по уровням важности, причем каждому уровню соответствует категория пользователей.

4. **Парольное разграничение доступа**

Парольное разграничение использует методы доступа субъектов к объектам с помощью пароля. Постоянное использование паролей приводит к неудобствам для пользователей и временным задержкам. По этой причине методы парольного разграничения используются в исключительных ситуациях.

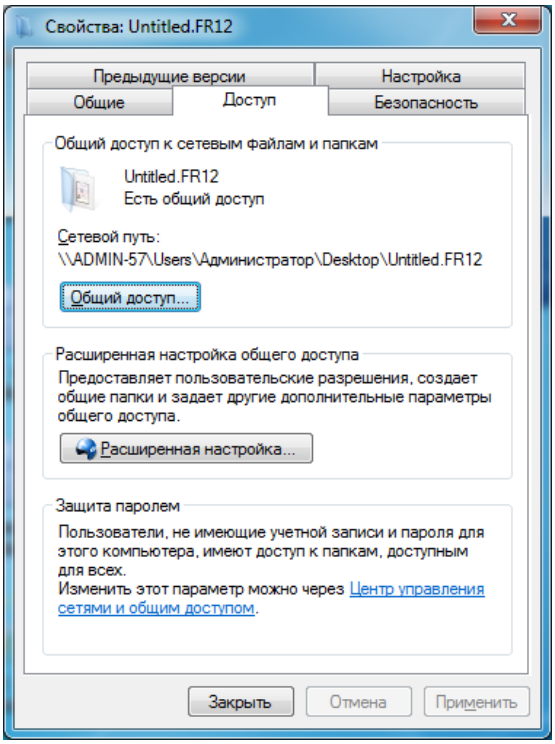
На практике принято сочетать разные методы разграничений доступа. Например, первые три метода усиливаются парольной защитой. Использование разграничения прав доступа является обязательным условием защищенной информационной системы.

Практическая часть – можно ничего не менять в своих настройках. Просто прогуляйтесь по указанным путям и сделайте соответствующие скрин-шоты.

1. *Освоить средства разграничения доступа пользователей к папкам*:

- выполнить команду «Общий доступ и безопасность» контекстного меню папки (если эта команда недоступна, то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки) или команду «Свойства»;
- открыть вкладку «Безопасность» и включить в отчет сведения о субъектах, которым разрешен доступ к папке и о разрешенных для них видах доступа;
- с помощью кнопки «Дополнительно» открыть окно дополнительных параметров безопасности папки (вкладка «Разрешения»);
- включить в отчет сведения о полном наборе прав доступа к папке для каждого из имеющихся в списке субъектов;
- открыть вкладку «Владелец», включить в отчет сведения о владельце папки и о возможности его изменения обычным пользователем;

- открыть папку «Аудит», включить в отчет сведения о назначении параметров аудита, устанавливаемых на этой вкладке, и о возможности их установки обычным пользователем;



- закрыть окно дополнительных параметров безопасности.

2. *Освоить средства разграничения доступа пользователей к файлам*:

- выполнить команду «Свойства» контекстного меню файла;
- повторить все задания п. 1, но применительно не к папке, а к файлу.

3. *Освоить средства разграничения доступа к принтерам*:

- выполнить команду «Принтеры и факсы» меню «Пуск»;
- выполнить команду «Свойства» контекстного меню установленного в системе принтера;
- повторить все задания п. 1, но применительно не к папке, а к принтеру.

4. *Освоить средства разграничения доступа к разделам реестра операционной системы*:

- с помощью команды «Выполнить» меню «Пуск» запустить программу редактирования системного реестра regedit (regedt32);
- с помощью команды «Разрешения» меню «Правка» редактора реестра определить сведения о правах доступа пользователей к корневым разделам реестра, их владельцах и параметрах политики аудита;
- включить в отчет сведения о правах доступа пользователей к данной папке и о ее владельце.

Отчет должен содержать:

1. Тему и цель работы
2. Экранные копии выполнения работы
3. Составьте матрицу доступа по своей (курсовой) ИС.
4. Ответы на контрольные вопросы.

Контрольные вопросы:

1. В чем достоинства дискреционной политики безопасности?
2. В чем недостатки мандатной политики безопасности?
3. Кто определяет права доступа к папкам, файлам, принтерам при использовании дискреционной политики безопасности?
4. В чем отличие определения прав на доступ к файлам по сравнению с определением прав на доступ к папкам?
5. В чем отличие определения прав на доступ к принтерам по сравнению с определением прав на доступ к папкам и файлам?
6. В чем отличие определения прав на доступ к разделам реестра по сравнению с определением прав на доступ к папкам и файлам?

Практическая работа
«Создание резервных копий базы данных»

Задание 1. Просмотр структуры базы данных

1. Используя SQL Server Management Studio, подключитесь к SQL Server **SHAMOO**.
2. Выберите БД **DB_собственное_имя**, созданную на предыдущих занятиях. Просмотрите имеющиеся таблицы, представления и хранимые процедуры.
3. Запустите хранимую процедуру [Ten Most Expensive Products], просмотрите результаты выполнения данной процедуры.
4. Создайте запрос ViewSalesByCategory.sql и внесите следующие данные:

```
USE SEMDB_ваше_имя;

SELECT CategoryName,ProductName,ProductSales FROM [Sales by Category];

GO
```

5. Просмотрите результаты выполнения запроса.
6. Просмотрите структуру таблицы **Categories**, как поля включает данная таблица, какие значения могут быть заданы.

Задание 2. Создание резервных копий базы данных

1. Используя системную хранимую процедуру sp_helpdevice, просмотрите список устройств резервного копирования локального сервера.
2. С помощью хранимой процедуры sp_addumpdevice, создайте новое дисковое устройство резервного копирования **BACKUPDevice_ваше_имя**, связав с файлом BackUp_Ваше_имя.bak в созданной папке **C:\BackUPDB**.
3. Сформируйте запрос T-SQL, создающий полную резервную копию Вашей базы данных **DB_собственное_имя,** задав имя копии **DBackFull1** и использовав созданное устройство резервного копирования **BACKUPDevice_ваше_имя**.
4. Внесите изменения в таблицу Categories, используя запрос на добавление строки

USE **DB_собственное_имя**

INSERT INTO dbo.Categories (CategoryName,Description)

VALUES ('Vines','Vines and liqueur');

GO

5. Сформируйте запрос T-SQL, создающий резервную копию журнала транзакций БД **DB_собственное_имя** в файл **C:\BackUPDB\DB_Ваше_имя.TRN**.
6. Внесите изменения в таблицу Products, используя запрос на обновление
use SEMDB_Admin;

UPDATE Products SET UnitPrice=UnitPrice*1.15 WHERE (UnitsInStock<15);

GO

7. Сформируйте запрос T-SQL, создающий дифференциальную резервную копию БД **DB_собственное_имя**, задав имя копии **DBackDiff1** и используя созданное устройство резервного копирования **BACKUPDevice_ваше_имя.**
8. Сформируйте запрос T-SQL, создающий резервную копию журнала транзакций БД **DB_ваше_имя** в файл **C:\BackUPDB\DB_Ваше_имя_2.TRN**.
9. Просмотрите размеры созданных резервных копий.
10. Покажите результат преподавателю.

Задание 3. Восстановление базы данных из резервных копий

1. Используя SQL Server Management Studio, подключитесь к SQL Server **SHAMOO**.

2. Найдите БД **DB_собственное_имя.** Используя оператор DROP DATABASE, удалите Вашу базу данных с сервера баз данных.
3. Выполните проверку резервных копий, созданных в предыдущем задании, используя операторы T-SQL: **RESTORE VERIFYONLY** устройство резервного копирования.
4. Выполните полное восстановление БД **DB_собственное_имя** из резервной копии **DBackFull1** устройства **BACKUPDevice_ваше_имя.** Установите параметр **NORECOVERY**.
5. Используя операторы T-SQL, выполните восстановление резервной копии журнала транзакций (п.5 предыдущего задания – файл **DB_Ваше_имя.TRN**).
6. Используя операторы T-SQL, выполните восстановление дифференциальной резервной копии (п.7 предыдущего задания).
7. Используя операторы T-SQL, выполните восстановление резервной копии журнала транзакций (п.9 предыдущего задания), установите параметр **WITH RECOVER**
8. Просмотрите результат выполнения. Просмотрите структуру созданной БД. Какие файлы данных и файловые группы были восстановлены.
9. Покажите результат преподавателю.

Практическая работа
«Восстановление базы данных»

1. Цель работы

Получение практических навыков администрирования и сопровождения логической и физической структур базы данных.

2. Методические указания

Лабораторная работа направлена на ознакомление с основами администрирования СУБД Oracle: работа с табличными пространствами, файлами данных, резервное копирование и восстановление базы данных.

Требования к выполнению лабораторного практикума:

- Выполнять все действия строго в том порядке, указанном в задании;

- Составить отчет о проделанной работе;
- В отчете должны содержаться снимки экрана, показывающие процесс выполнения заданий;
- Отчет должен содержать выводы по результатам каждого выполненного задания;
- Работа должна быть выполнена согласно требованиям к выполнению лабораторной работы;
- Особое внимание следует уделить правильности задания переменной окружения ORACLE_SID; перед выполнением лабораторной работы рекомендуется сделать резервную копию файлов, расположенных в каталоге /opt/oracle/OraHome1/oradata/testN, N=1..10.

Перед выполнением упражнений вам предстоит выполнить следующие действия:
Проверьте переменную окружения ORACLE_SID:

echo $ORACLE_SID;

Задайте

ORACLE_SID=testN, N=1..10, выполнив команду

#export ORACLE_SID=testN;

3. Подсоединитесь к БД с помощью программы svrmgrl

#svrmgrl

SVRMGRL> connect internal

При составлении и оформлении отчета следует придерживаться «Требований к оформлению дипломных, курсовых, лабораторных работ», расположенных на странице **http://unesco.kemsu.ru/student/rule/rule.html**.

3. Теоретический материал

Введение

Для небольшой базы данных достаточно создать одно табличное пространство SYSTEM; однако, Oracle рекомендует создавать дополнительные табличные пространства для хранения данных и индексов пользователя, сегментов отмены, временных сегментов отдельно от словаря данных. Это обеспечивает вам большую гибкость в выполнении различных задач администрирования и уменьшает конкуренцию при обращении к объектам словаря и схемы.

Администратор может создавать новые табличные пространства, изменять размер файлов данных, добавлять файлы к табличным пространствам, устанавливать и изменять параметры хранения по умолчанию сегментов в табличном пространстве, переводить табличное пространство в состояние «только чтение» или «чтение-запись», делать табличное пространство временным или постоянным или удалить его.

Табличное пространоство system и другие

1. Табличное пространство system:
   - создается во время создания базы данных
   - содержит словарь данных
   - содержит сегмент отмены system
2. Другие табличные пространства:
   - отделяют сегменты
   - обеспечивают большую гибкость решения задач администрирования пространства
   - дают возможность контролировать выделение пространства пользователю

Создание табличных пространств

Табличное пространство может быть создано при помощи следующей команды:

CREATE TABLESPACE табличное_пространство
[DATAFILE фраза_файла_данных]
[MINIMUM EXTENT целое[K|M]]
[BLOCKSIZE целое [K]]
[LOGGING|NOLOGGING]
[DEFAULT фраза_хранения]
[ONLINE I OFFLINE]
[PERMANENT I EMPORARY]
[extent_management_clause]
[autoextend_clause]

Файлы параметров инициализации:

табл_пространство – имя табличного пространства, которое требуется создать.

DATAFILE –задает файл или файлы данных, составляющие это табличное пространство. Для временных табличных пространств можно использовать

TEMPFILE.

MINIMUM EXTENT – обеспечивает то, что размер каждого экстента этого табличного пространства кратен целому (используйте K и M для указания размера в килобайтах и мегабайтах).

BLOCKSIZE – указывает размер блока данных, с которым будет создано табличное пространство. Необходимо указать параметр инициализации DB_nK_CACHE_SIZE (n- 2,4,8,16 или 32, размер блока) для этого размера блока. Он устанавливает размер кэша буферов для обслуживания табличных пространств с указанным размером блока. Можно указать до 4 параметров. По умолчанию используется стандартный размер блока и кэш буферов по умолчанию, заданный параметром инициализации DB_CACHE_SIZE.

LOGGING – указывает, что по умолчанию все изменения таблиц, индексов и секций табличного пространства записываются в журнал (режим LOGGIN установлен в команде по умолчанию).

NOLOGGING – указывает, что по умолчанию все изменения таблиц, индексов и секций табличного пространства не записываются в журнал (режим NOLOGGIN затрагивает только некоторые команды DML и DDL, например, использующие прямую загрузку).

DEFAULT – задает параметры хранения по умолчанию для всех объектов, которые будут созданы в данном табличном пространстве.

ONLINE – делает табличное пространство доступным сразу после создания.

OFFLINE – сразу после создания табличное пространство будет недоступно.

PERMANENT – указывает на то, что это табличное пространство может быть использовано для хранения постоянных объектов.

TEMPORARY – указывает на то, что данное табличное пространство может хранить только временные объекты, например, сегменты, используемые фразой ORDER BY для неявной сортировки. Используется стандартный размер блока.

SIZE – задаёт размер файла (используйте K и M для задания размера файла).

REUSE – разрешает серверу Oracle повторно использовать существующий файл.

autoextend_clause OFF/ON – разрешает или запрещает автоматическое расширение файла данных: NEXT- какими кусками будет расширяться файл, MAXSIZE/UNLIMITED- до какого максимального размера.

Пример создания нового табличного пространства:

```
CREATE TABLESPACE userdata
DATAFILE '/u01/oradata/userdata01.dbf
```

SIZE 100M
AUTOEXTEND ON NEXT 5M
MAXSIZE 200M;

Табличные пространства «только для чтения»

Команда alter tablespace...read only.

Перевод табличного пространство в режим только для чтения запрещает последующие операции записи в файлы данных. Табличные пространства «только для чтения» используются для предотвращения каких-либо изменений и для отмены необходимости выполнять резервирование и восстановление больших, статичных областей базы данных. Сервер Oracle никогда не обновляет файлы табличного пространства, используемого только для чтения, и, поэтому эти файлы могут располагаться на носителях, запись на которые невозможна, таких как CD-ROM.

Табличное пространство может быть переведено в режим только для чтения или «чтение-запись» при помощи команды ALTER TABLESPACE:

ALTER TABLESPACE табличное_пространство READ [ONLY | WRITE]

Перевод табличного пространства в режим «только чтение»

Команда ALTER TABLESPACE...READ ONLY переводит табличное пространство в режим «только чтение», не дожидаясь завершения всех активных транзакций. В этом режиме не разрешаются никакие последующие операции записи в табличное пространство, за исключением отката текущих транзакций, которые до этого модифицировали блоки табличного пространства. После того, как выполнится **фиксация или откат всех текущих транзакций, команда alter tablespace ... read** only завершается и табличное пространство переводится в режим «только чтение».

Вы можете удалять из табличного пространства «только чтение» такие объекты, как таблицы и индексы, так как эти команды вносят изменения только в словарь данных, но не в файлы данных табличного пространства.

Перед переводом табличного пространства «только чтение» в режим «чтение-запись», все файлы данных табличного пространства должны быть в оперативном режиме.

- Перевод табличного пространства в режим «только чтение»
- Активизирует контрольную точку для файлов данных табличного

пространства.

Автономный режим

Табличное пространство, находящееся в автономном режиме, не разрешает доступа к данным.

Некоторые табличные пространства должны находиться всегда в оперативном режиме:

- SYSTEM;
- табличные пространства, содержащие активные сегменты отмены;
- временное табличное пространство по умолчанию;

Перевод в автономный режим: ALTER TABLESPACE userdata OFFLINE;
Перевод в оперативный режим: ALTER TABLESPACE userdata ONLINE;

Перевод табличных пространств в автономный режим (offline)

Пользователи могут получить доступ к табличному пространству, только если оно находится в оперативном режиме. Табличное пространство может быть переведено администратором базы данных в автономный режим для того, чтобы:

- сделать недоступной часть базы данных, тогда как оставшаяся ее часть будет работать в нормальном режиме;
- выполнить резервирование табличного пространства в автономном режиме (хотя можно производить резервирование табличного пространства, которое находится в оперативном режиме и используется);
- восстановить табличное пространство или файл данных, когда база данных открыта;
- изменить местоположение файлов данных, когда база данных открыта.

Автономный режим таблиичного пространства

- Сервер Oracle не позволяет никаким командам SQL выполнять операции над объектами, содержащимися в автономном табличном пространстве. Если пользователи пытаются получить доступ к объектам автономного табличного пространства либо непосредственно, либо при проверке ссылочной целостности, они получают сообщение об ошибке.
- Информация о переходе табличного пространства в автономный режим или о возвращении в оперативный сохраняется в словаре данных и в управляющих файлах. Если табличное пространство находится в

автономном режиме во время остановки базы данных, то оно останется таковым и не будет проверяться при последующем монтировании и открытии базы данных.

- Экземпляр Oracle автоматически переключает табличное пространство из оперативного режима в автономный, когда возникают ошибки определенного вида (например, когда процесс Database Writer в ходе нескольких попыток не может произвести запись в файл данных табличного пространства).

Изменение размера табличного пространства

1. **Добавление** файлов данных
2. **Изменение** размеров файла данных:

- **автоматически**
- **вручную**

Установка автоматического расширения файлов данных

Указание параметра autoextent для нового файла данных

В следующих командах с помощью фразы AUTOEXTEND включается или отключается автоматическое расширение файла данных:

- CREATE DATABASE
- CREATE TABLESPACE ... DATAFILE
- ALTER TABLESPACE ... ADD DATAFILE

Используйте команду ALTER DATABASE, чтобы изменить файл данных и предоставить возможностью его автоматического расширения:

ALTER DATABASE DATAFILE спецификация_файла [фраза_авторасширения].

Если в табличном пространстве существует несколько файлов, расширяться будет тот, в котором, сервер захочет выделить экстент. Если в файле нет места, и он не может расширяться, будет взят другой файл. Если ни в одном файле нет места, и они не могут расширяться дальше, пользователь, чья команда требует, расширения сегмента получит ошибку.

фраза_авторасширения :== [AUTOEXTEND { OFF | ON [NEXT целое [K |M]] [MAXSIZE UNLIMITED | целое[K|M]] }],

где:

AUTOEXTEND OFF выключает автоматическое расширение файла данных.

AUTOEXTEND ON включает автоматическое расширение файла данных. NEXT устанавливает размер выделяемого дискового пространства, когда требуются дополнительные экстенты.

MAX SIZE определяет максимальный размер дискового пространства, который может быть выделен файлу данных.

UNLIMITED снимает ограничение на максимальный размер дискового пространства для файла данных.

Пример установки автоматического расширения файла данных**:**

ALTER DATABASE DATAFILE

'/u01/oradata/app_data_04.dbf‘

SIZE 200M AUTOEXTEND ON NEXT 10M MAXSIZE 500M;

Изменение установки autoextend для существующего файла данных

Для включения или отключения автоматического расширения уществующего файла данных используется команда ALTER DATABASE:

ALTER DATABASE [database] DATAFILE 'имя_файла'[,'имя_файла']...фраза_авторасширения

Определение параметров AUTOEXTEND:

DBA_DATA_FILES есть столбцы, показывающие параметры Авторасширения. Столбец AUTOEXTENSIBLE показывает включено или нет авторасширение:

SQL> select tablespace_name, file_name, autoextensible from dba_data_files;

Например:

TABLESPACE_NAME FILE_NAME AUTOEXTENSIBLE

SYSTEM /home/dbaOl/ORADATA/uOl/systemOl.dbf YES

DATA01 /home/dba01/ORADATA/u04/data01.dbf NO

USERS /home/dba01/ORADATA/u03/users01.dbf NO

UNDO2 /horae/dba01/ORADATA/u01/UND02.dbf NO

Изменение размера файлов данных вручную

Команда ALTER DATABASE DATAFILE RESIZE

Администратор может изменить размер существующего файла данных вместо того, чтобы увеличивать пространство базы данных при помощи создания новых файлов. Администратор может исправить ошибки, допущенные при планировании базы данных, и освободить неиспользуемое пространство. Для того чтобы

уменьшить или увеличить размер файла данных вручную используется команда ALTER DATABASE следующего вида:

ALTER DATABASE [база_данных]

DATAFILE 'имя_файла'[, 'имя_файла']...

RESIZE целое[K|M]

где: целое- требуемый размер файла данных.

Если объекты базы данных располагаются в файле данных за указанным размером, то файл данных уменьшается только до последнего блока последнего объекта базы данных.

Добавление файлов данных к табличному пространству

Команда ALTER TABLESPACE ADD DATAFILE

При помощи следующей команды ALTER TABLESPACE ADD можно добавить к табличному пространству файл данных, чтобы увеличить общее количество дискового пространства, отведенного для этого табличного пространства :

ALTER TABLESPACE табличное_пространство

ADD [DATAFILE I TEMPFILE]

спецификация_файла [фраза_авторасширения]

[,спецификация_файла [фраза_авторасширения]]...

Файлы добавляют, если в текущем разделе диска нет места или превышено ограничение на максимальный размер файла в операционной системе.

ALTER TABLESPACE: перемещение файлов данных

Методы перемещение файлов данных.

Администратор базы данных может изменять местоположение файлов данных в зависимости от вида табличного пространства одним из следующих двух способов: при помощи команд ALTER TABLESPACE или ALTER DATABASE.

Использование команды ALTER TABLESPACE.

Команда ALTER TABLESPACE следующего вида применяется только для файлов данных, не принадлежащих табличному пространству SYSTEM, которое, к тому же, не содержит активных сегментов отмены или временных сегментов. Более того, она работает только в режиме открытой базы данных.

ALTER TABESPACE табличное_пространство RENAME DATAFILE 'имя_файла'[, 'имя_файла']... TO 'имя_файла'[, 'имя_файла']

Для переименования файла данных выполняется следующая последовательность шагов:

1. Переведите табличное пространство в автономный режим.
2. Переместите или скопируйте файлы при помощи команд операционной системы.
3. Выполните команду ALTER TABLESPACE RENAME DATAFILE.
4. Верните табличное пространство в оперативный режим.
5. Если требуется, удалите файл при помощи команды операционной системы. Имя исходного файла должно совпадать с именем в управляющем файле.

ALTER DATABASE: перемещение файлов данных

Для перемещения любого вида файла данных может быть использована команда ALTER DATABASE (см. занятие "Сопровождение журнальных файлов"). В отличие от предыдущей команды, она работает как в режиме открытой базы данных, так и в режиме смонтированной базы.

ALTER DATABASE [база_данных]RENAME FILE

'имя_файла'[, 'имя_файла']... TO 'имя_файла'[, 'имя_файла']...

Файлы табличного пространства SYSTEM , которые не могут быть переведены в автономный режим, переименовываются следующим образом:

1. Остановите экземпляр.
2. Переместите файлы при помощи команды операционной системы.
3. Смонтируйте базу данных.
4. Выполните команду ALTER DATABASE RENAME FILE.
5. Откройте базу данных.

Удаление табличных пространств

- Нельзя удалять табличное пространство SYSTEM и содержащее активные сегменты отката.
- Информация о табличном пространстве удаляется из словаря данных.
- В команде удаления табличного пространства необходимо указывать режим удаления его содержимого.
- При помощи команды DROP TABLESPACE табличные пространства можно удалить из базы данных, когда отпала надобность в них самих и в их

содержимом:

DROP TABLESPACE табличное_пространство

[INCLUDING CONTENTS [AND DATAFILES] [CASCADE CONSTRAINTS]]

где:

- табличное_пространство - имя табличного пространства, которое требуется удалить
- INCLUDING CONTENTS - удаляет все сегменты табличного пространства
- AND DATAFILES - удаляет соответствующие файлы ОС
- CASCADE CONSTRAINTS - удаляет те ссылочные правила целостности таблиц из других табличных пространств, которые ссылаются на первичные и уникальные ключи таблиц, принадлежащих удаляемому табличному пространству

Табличное пространство, содержащее данные, не может быть удалено без использования параметра INCLUDING CONTENTS. Использование этого параметра может привести к генерации большого объема информации отмены, если в табличном пространстве находится много объектов.

Данные табличного пространства перестают существовать в базе данных, как только оно удаляется.

При удалении табличного пространства удаляются только файловые указатели из управляющего файла соответствующей базы данных. Файлы базы данных остаются и должны быть удалены явно на уровне операционной системы, если в команде отсутствует фраза AND DATAFILES .

Табличное пространство в режиме только для чтения тоже может быть удалено вместе со своими сегментами. Это возможно потому, что команда DROP обновляет словарь данных (который должен быть в режиме чтение-запись), а не физические файлы, составляющие базу данных.

Для того чтобы во время удаления табличного пространства не существовало транзакций, пытающихся получить доступ к сегментам этого табличного пространства, рекомендуется перевести его в автономный режим.

Получение информации о табличном пространстве

Информация о табличном пространстве:

- DBA_TABLESPACES
- V$TABLESPACE

Информация о файле данных:

- DBA_DATA_PILES
- V$DATAFILE

Информация о временном файле:

- DBA_TEMP_FILES
- V$TEMPFILE

Резервное копирование и восстановление

Восстановление вручную

1. Выполнить физическое восстановление файла означает заменить его резервной копией.
2. Восстановлению обычно подлежат следующие файлы:
   - файлы данных;
   - управляющие файлы;
   - архивные журнальные файлы;
   - серверный файл параметров.
3. В каждом случае потеря основного файла и восстановление его из резервной копии приводит к следующим последствиям при восстановлении носителя.

Хранение записей для последующего использования в ходе восстановления

Одним из наиболее важных аспектов резервирования и восстановления, управляемого пользователем, является хранение записей обо всех файлах текущей базы данных и резервных копиях этих файлов. Например, у вас должны быть записи о местоположении следующих файлов:

- Файлы данных;
- Управляющие файлы;
- Оперативные журнальные файлы (обратите внимание, что оперативные журналы не резервируются);
- Архивные журнальные файлы;
- Файлы параметров инициализации;
- Файлы паролей;
- Файлы настроек сетевых компонентов;

Запись местоположения файлов данных, управляющих файлов и оперативных

журнальных файлов

Следующий полезный командный файл SQL выводит местоположение всех управляющих файлов, файлов данных и оперативных журнальных файлов базы данных:

```
SELECT NAME FROM V$DATAFILE
UNION ALL
SELECT MEMBER FROM V$LOGFILE
UNION ALL
SELECT NAME FROM V$CONTROFILE;
```

Выходные данные могут выглядеть следующим образом:

```
NAME
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
/oracle/dbs/tbs_01.f
/oracle/dbs/tbs_02.f
/oracle/dbs/tbs_11.f
/oracle/dbs/tbs_12.f
/oracle/dbs/t1_log1.f
/oracle/dbs/t1_log2.f
/oracle/dbs/cf1.f
/oracle/dbs/cf2.f
```

Запись местоположений резервных копий файлов

Недостаточно просто записывать местоположение резервных копий файлов: необходимо устанавливать соответствие между резервными копиями и исходными файлами. По возможности, присваивайте резервным копиям такие же относительные имена, как и у основных файлов. Независимо от используемой системы именования, храните таблицу с соответствующей информацией. Например, можно хранить следующую таблицу с информацией о местоположении файлов базы данных на случай восстановления.

Определение файлов данных, требующих восстановления

Динамическое представление производительности V$RECOVER_FILE позволяет определить, какие файлы нужно

восстановить из резервных копий при подготовке к восстановлению носителя. В этом представлении содержатся все файлы, требующие восстановления, и даются объяснения, почему они Должны быть восстановлены.

Следующий запрос отображает идентификационные номера файлов данных, требуемых для восстановления носителя, а также причину восстановления (если она известна), а также ЗСК и время, с которых нужно начать восстановление:

```
SELECT * FROM V$RECOVER_FILE;
FILE#    ONLINE    ERROR CHANGE#   TIME
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
        14 ONLINE
        15 ONLINE  FILE NOT FIND          0
        21 ONLINE  OFFLINE NORMAL     0
```

Повторное создание файлов данных при отсутсвии резервных копий

Когда файл данных поврежден, а его резервная копия недоступна, этот файл данных все же можно восстановить, если:

- доступны все архивные журнальные файлы, сгенерированные после создания исходного файла данных;
- управляющий файл содержит имя поврежденного файла (это значит, что управляющий файл является текущим или восстановленным из резервной копии, сделанной после того, как поврежденный файл данных был добавлен в базу данных).

Чтобы повторно создать файл данных для восстановления:

1. Создайте новый, пустой файл данных для замены поврежденного файла данных, у которого нет соответствующей резервной копии. Предположим, например, что поврежден файл данных /disk1/users1.f и его резервная копия недоступна. Следующий оператор повторно создает исходный файл данных (того же размера) на диске disk2:

   ALTER DATABASE CREATE DATAFILE ‘/disk1/users1.f’ AS ‘/disk2/users1.f’;

   Данный оператор создает пустой файл того же размера, что и потерянный файл. Oracle ищет информацию о размере файла в управляющем файле и словаре данных. Исходному файлу данных присваивается имя нового файла данных.
2. Выполните восстановление носителя дня пустого файла

данных. Например**,** введите:

RECOVER DATAFILE '/disk2/users1.f'

3. Все архивные журналы, сгенерированные после создания исходного файла данных, должны быть доступны и повторно применены к новой, пустой версии потерянного файла данных во время восстановления.

Восстановление и повторное создание управляющих файлов

Если сбой носителя повредил управляющие файлы базы данных (независимо от того, мультиплексированы они или нет), база данных продолжает работать до тех пор, пока какому-либо процессу сервера Oracle не потребуется получить доступ к управляющим файлам. В этот момент база данных и экземпляр автоматически останавливаются.

Если сбой носителя был временным и база данных до сих пор не остановлена, не допускайте автоматической остановки базы данных – немедленно исправляйте сбой. Однако если остановка базы данных происходит до исправления временного сбоя носителя, ее можно повторно запустить после устранения проблемы и восстановления доступа к управляющим файлам.

Процедура восстановления после сбоя носителя, который делает невозможным доступ к управляющим файлам базы данных, зависит от того, мультиплексированы эти управляющие файлы или нет. Соответствующие процедуры описаны в следующих разделах:

- Потеря одного из элементов мультиплексированного управляющего файла.
- Потеря всех элементов мультиплексированного управляющего файла, когда резервная копия доступна.
- Потеря всех текущих и резервных управляющих файлов.

Потеря одного из элементов мультиплексированного управляющего файла

Следующие процедуры используются для восстановления базы данных после сбоя носителя, который привел к повреждению одного или нескольких управляющих файлов базы данных, но при этом как минимум один управляющий файл *остался неповрежденным.*

Копирование мультиплексированного управляющего файла в местоположение по умолчанию

Если диск и файловая система, содержавшие потерянный управляющий файл, остались невредимы, можно просто скопировать один из неповрежденных управляющих файлов туда, где находился потерянный управляющий файл. В этом случае вам не придется изменять значение параметра инициализации CONTROL_FILES.

Чтобы заменить поврежденный управляющий файл путем копирования мультиплексированного управляющего файла:

1. Остановить экземпляр, если он еще работает: SHUTDOWN ABORT.
2. Устраните аппаратную проблему, которая привела к сбою носителя. Если не удается быстро решить эту проблему, переходите к восстановлению базы данных – восстановите поврежденный управляющий файл на другом запоминающем устройстве, как описано в разделе «Копирование мультиплексированного управляющего файла в местоположение, отличное от используемого по умолчанию ».
3. Замените поврежденные управляющие файлы неповрежденной мультиплексированной копией текущего управляющего файла базы данных. Например, чтобы заменить файл bad_cf.f файлом good_cf.f введите: % ср /oracle/good_cf.f /oracle/dbs/bad_cf.bad
4. Запустите новый экземпляр, смонтируйте и откройте базу данных. Например, введите: STARTUP

Потеря всех элементов мультиплексированного запоминающего файла, когда резервная копия доступна

Следующие процедуры для восстановления управляющего файла из резервной копии при сбое носителя, который привел к повреждению всех управляющих файлов базы данных. Если управляющий файл недоступен, можно запустить экземпляр, но не монтировать базу данных. Если попытаться смонтировать базу данных, когда управляющий файл недоступен, появится следующее сообщение об ошибки:

ORA-00205: ошибка определения управляющего файла, дополнительную информацию см. в сигнальном файле ALERT

Нельзя смонтировать и открыть базу данных до тех пор, пока управляющий файл не будет снова доступным. Если управляющий файл восстанавливается из резервной копии, необходимо открыть базу данных с опцией RESETLOGS.

Как видно из Таблицы, процедура восстановления управляющего файла

зависит от того, доступны ли журналы.

ВОССТАНОВЛЕНИЕ УПРАВЛЯЮЩГО ФАЙЛА ИЗ РЕЗЕРВНОЙ КОПИИ В МЕСТОПОЛОЖЕНИИ ПО УМОЛЧАНИЮ

По возможности, восстанавливайте управляющий файл в его исходном местоположении. В этом случае вам не придется указывать новые местоположения управляющего файла в файле параметров инициализации.

Чтобы восстановить управляющий файл в местоположении по умолчанию**:**

1. Остановите экземпляр, если он еще работает: SHUTDOWN ABORT
2. Устраните аппаратную проблему, которая привела к сбою носителя.
3. Восстановите управляющий файл из резервной копии во всех местоположениях, указанных в параметре инициализации CONTROL_FILES. Например, если в файле параметров сервера указаны местоположения управляющего файла /dsk/oracle/dbs/cf1.f и /dsk/cf2.f, используйте утилиту операционной системы для восстановления управляющего файла в этих местоположениях:
   % cp /backup/cf.bak /dsk1 /oracle/dbs/cf1.f
   % cp /backup/cf.bak /dsk2/cf2.f
4. Запустите новый экземпляр и смонтируйте базу данных. Например, введите: STARTUP MOUNT
5. Начните восстановление выполнением оператора RECOVER с предложением USING BACKUP CONTROLFILE. Укажите предложение UNTIL CANCEL, если вы выполняете неполное восстановление. Например, введите:
   RECOVER DATABASE USING BACKUP CONTROLFILE UNTIL CANCEL
6. Примените запрошенные архивные журналы. Если появится сообщение о том, что требуемый архивный журнал отсутствует, значит, необходимая запись, вероятно, находится в оперативном журнале. Эта ситуация может возникнуть, если незаархивированные изменения находились в оперативных журналах, когда произошел сбой экземпляра. Например, предположим, что вы видите следующее сообщение:
   ORA-00279: изменение 55636, созданное 06/08/2000 в 16:59:47, необходимое для потока 1
   ORA-00289: предложение /oracle/work/arc_dest/arcr_1_111.arc
   ORA-00280: изменение 55636 для потока 1 находится в последовательности

#111

Задайте журнал: (<RET>=предлагаемое | имя файла | AUTO | CANCEL)

Можно указать имя оперативного журнала и нажать Enter (возможно, придется сделать это несколько раз до тех пор, пока не будет найден нужный журнал):

/oracle/dbs/t1_log1.f

Журнал применен.

Восстановление носителя завершено.

Если по каким-либо причинам оперативные журналы недоступны, можно прекратить восстановление и не применять оперативные журналы. Обратите внимание, что если все файлы данных являются текущими и требуемые для восстановления записи находятся в оперативных журналах, базу данных нельзя открыть без применения оперативных журналов. Если оперативные журналы недоступны, необходимо повторно создать управляющий файл.

7. Откройте базу данных в режиме RESETLOGS после завершения восстановления:

ALTER DATABASE OPENRESETLOGS;

4. Порядок выполнения работы

1. Сопровождение табличных пространств и файлов данных

1. Создайте постоянные табличные пространства со следующими именами и параметрами хранения:

DATA01, управляемое с помощью словаря данных.

DATA02, с экстентами одинакового размера (размер каждого экстента должен быть кратен 100 Кб.) (включите автоматическое расширение с выделением пространства размером 500 Кб и максимальным размером 2 Мб.

RONLY для таблиц, доступных только на чтение с параметрами хранения по умолчанию.

НЕ СОЗДАВАЙТЕ табличное пространство в режиме «только чтение» в данный момент времени.

2. Выведите информацию из словаря данных.
3. Выделите дополнительно 500Кб для табличного пространства DATA02 . Проверьте результат.
4. Переместите табличное пространство DATA01 в другой каталог (оба

способа).

5. Добавьте файл данных для табличного пространства DATA01.
6. Измените размер фала данных для DATA01 вручную.
7. Создайте таблицу в табличном пространстве RONLY. Переведите RONLY в режим «только чтение».
8. Попытайтесь создать еще одну таблицу. Удалите первую таблицу. Что произошло и почему?
9. Удалите табличное пространство RONLY и соответствующий файл данных. Проверьте результат.

2. Резервное копирование и восстановление

1. Выполните резервное копирование управляющих файлов и файлов данных.
2. Удалите один из файлов данных.
3. Выполните восстановление удаленного файла путем создания нового файла данных.
4. Удалите все управляющие файлы.
5. Восстановите управляющие файлы из резервной копии.
6. Проверьте работоспособность БД.

Практическая работа

Восстановление носителей информации, удаленных файлов

Цель работы: научиться осуществлять восстановление жесткого диска после сбоев.

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).

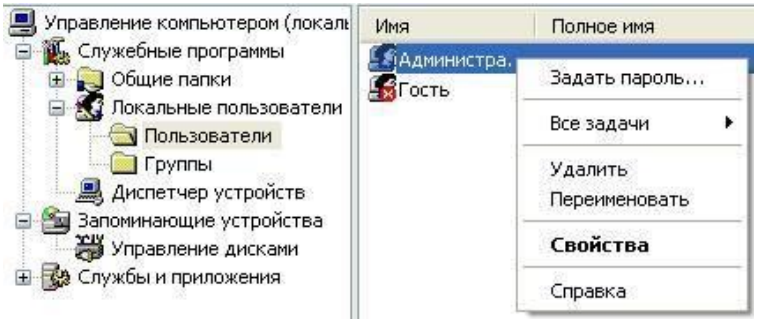


Рис. 1 - Окно Управление компьютером

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).

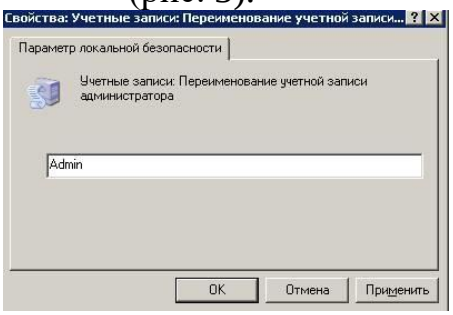


Рис. 3 - Пользователю Администратор присваиваем новое имя

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, использовав окно **Учетные записи пользователей**, что гораздо проще (рис. 5).

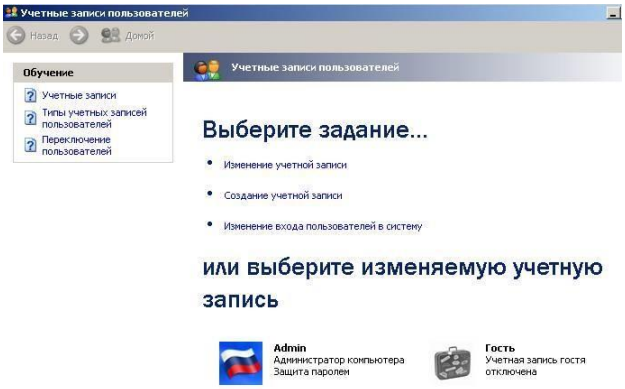


Рис. 5 - Окно Учетные записи пользователей

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 блокирована. Гость не может устанавливать или удалятьпрограммы. 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).

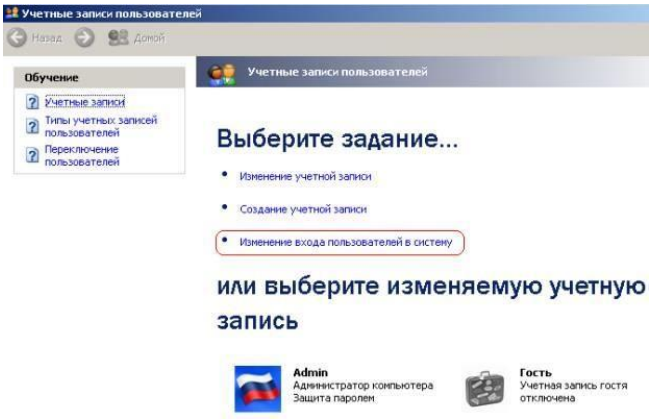


Рис. 6 - Окно Учетные записи пользователей

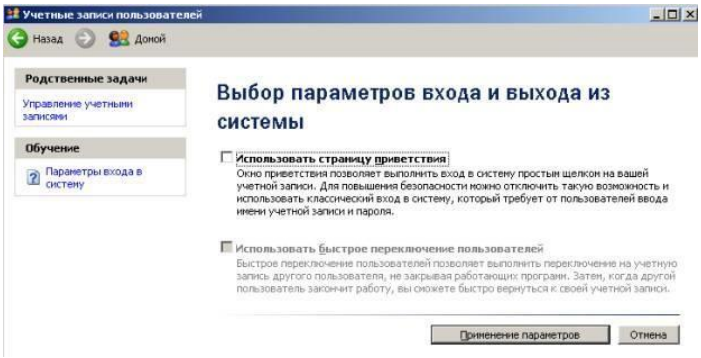


Рис. 7 - Убираем флажок Использовать страницу приветствия

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).

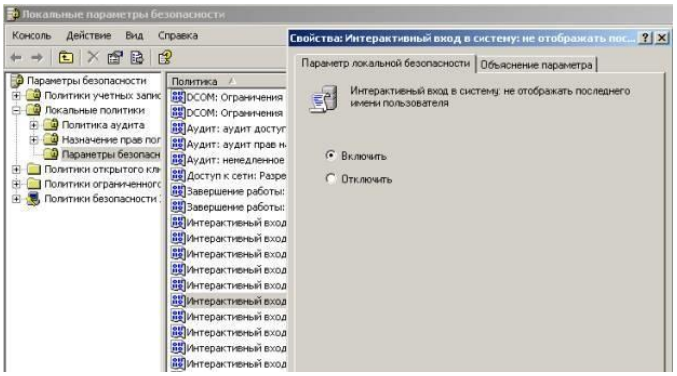


Рис. 9 - Активируем переключатель Включить

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 удаленнымПК 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 компьютер.

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; ожиданиеподтверждения.
- LAST_ACK — Удаленная сторона отключилась, затем сокет закрыт; ожиданиеподтверждения.
- FIN_WAIT_2 — Сокет закрыт; ожидание отключения удаленной стороны.
- TIME_WAIT — Сокет закрыт, но ожидает пакеты, ещё находящиеся в сети дляобработки

Примечание

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

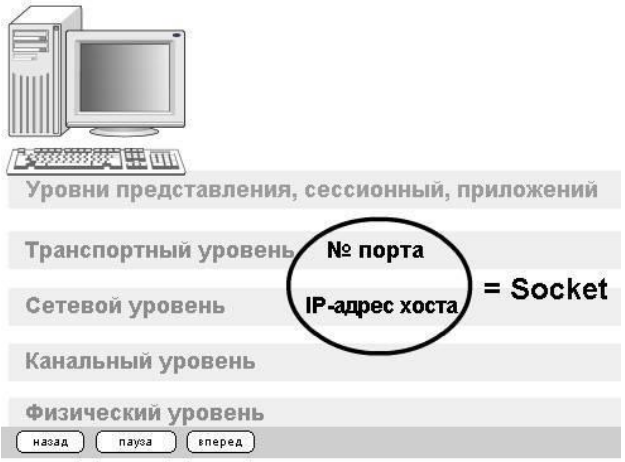


Рис. 11 - Сокет это № порта + IP адрес хоста

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).

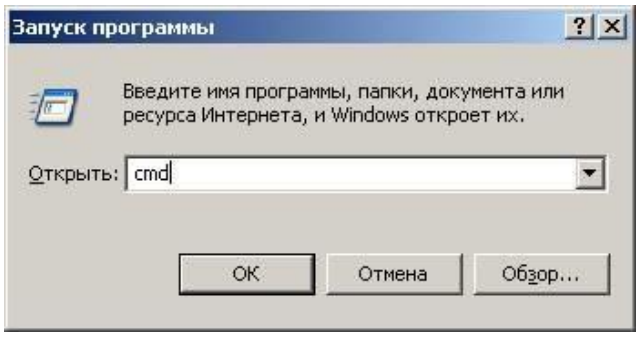


Рис. 12 - Окно Запуск программы

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.

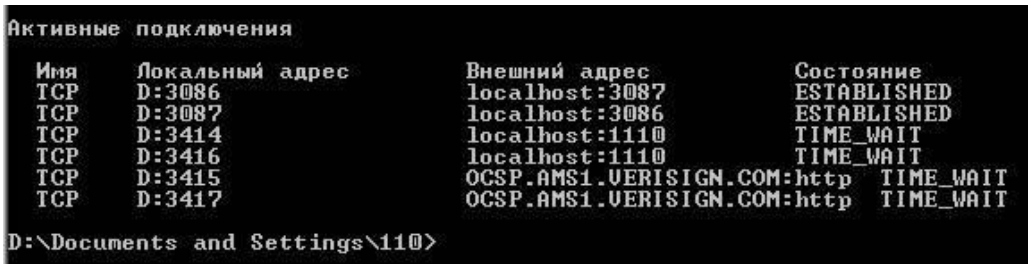


Рис. 13 - Список активных подключений на тестируемом ПК

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

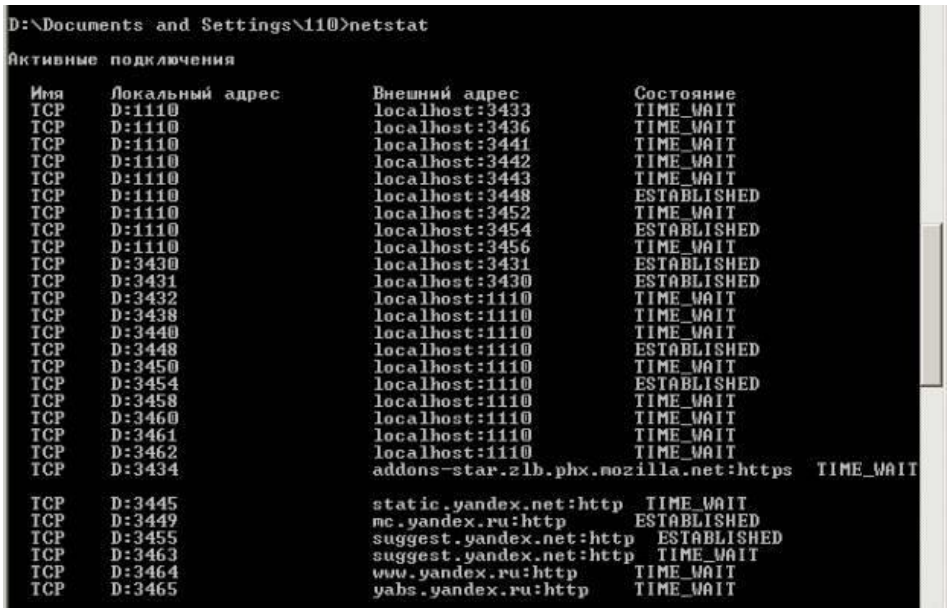


Рис. 14 - Активные подключения при работе ПК в Интернет

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

Опция (ключ)	**Назначение**
-a	Показывать состояние всех сокетов; обычно сокеты, используемые серверными процессами, не показываются.
-A	Показывать адреса любых управляющих блоков протокола, связанных с сокетами; 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 семейство 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 адресов**AF_UNIX**.
-I интерфейс	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** и**TraceRoute** (рис. 15).

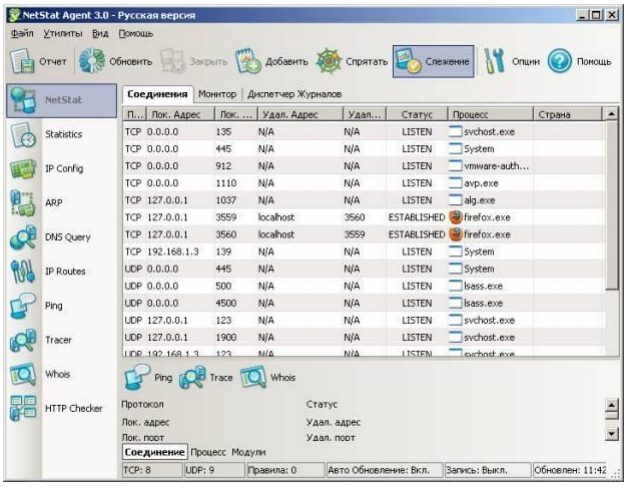


Рис. 15 - Главное окно программы NetStat Agent

В состав программы NetStat Agent вошли следующие утилиты:

· **NetStat** — отслеживает TCP и UDP соединения ПК (при этом отображаетсягеографическое 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 конечнымхостом, 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: Перезагрузка» 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).

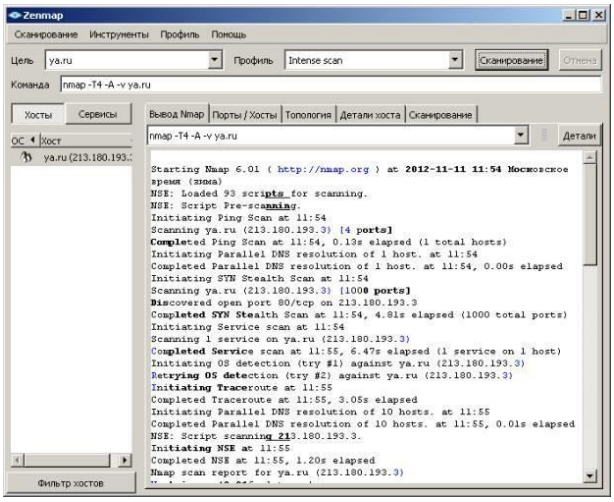


Рис. 16 - Интерфейс программы Nmap

Обычно для того, чтобы просканировать все порты какого-либо компьютера в сети вводится команда **nmap –p1-65535 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.

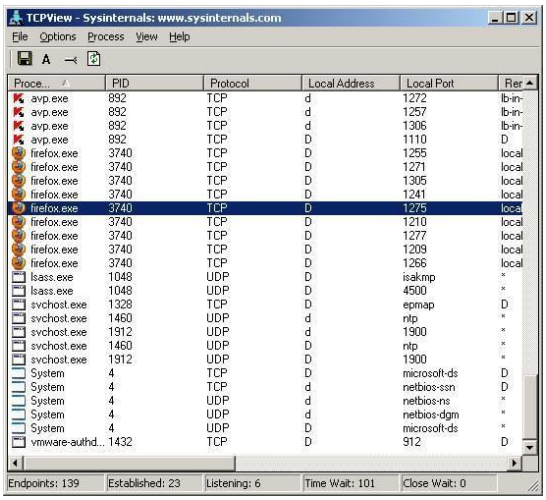


Рис. 17 - Главное окно программы TCPView

Просмотрите активные сетевые подключения локального ПК с помощью монитора портов tpiview. Определите потенциально возможные угрозы (какие порты открыты, и какие приложения их используют). При необходимости можно закрыть установленное приложением 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?

Для чего используется программа `NetStat Agent? Nmap? TCPView`

Комплект заданий для контрольной работы

1. Соотнести понятия и их определения

1. Программы
2. Программное средство
3. Программный продукт
4. ЖЦ ПП

1) это данные, предназначенные для управления конкретными компонентами системы обработки информации в целях реализации определенного алгоритма
2) объект, состоящий из программ, процедур, правил и документов, относящихся к функционированию системы обработки информации
3) это программное средство, предназначенное для поставки, передачи, продажи пользователю
4) это совокупность процессов, работ и задач, включающая в себя разработку, эксплуатацию и сопровождение ПС или системы, охватывающая жизнь ПС или системы от 6 установления требований к ним до прекращения их использования.

2. Выберете недостающее слово:

«Существует ряд национальных, государственных и международных__, посвященных вопросам стандартизации, оценки качества и сертификации программных средств и систем качества предприятия.»

- *Стандартов* +
- Государственных услуг
- Программных средств
- Этапов ЖЦ

3. Впишите недостающее слово:

_____– это совокупность свойств программного средства, обуславливающая его пригодность удовлетворять заданные или подразумеваемые потребности в соответствии с его назначением.

Правильный ответ: качество программного средства

4. Соотнесите понятия и их определения:

1. Атрибут
2. Критерий оценки
3. Характеристика качества ПС
4. Подхарактеристика качества ПС

1) измеримое физическое или абстрактное свойство ПС. Атрибуты могут быть внутренними и внешними
2) это совокупность принятых в установленном порядке правил и

условий, с помощью которых устанавливается приемлемость в целом качества программного средства

3) набор свойств программного средства, посредством которых описывается и оценивается его качество

4) это характеристика качества программного средства, входящая в состав другой характеристики качества

5. Метрика подхарактеристики качества

5) определенные метод и шкала измерения

6. Уровень пригодности ПС

6) это степень удовлетворения потребности, представленная посредством конкретного набора значений характеристик качества программного средства

7. Мера

7) это число или категория, присвоенная атрибуту объекта путем измерения

8. Измерение

8) это использование метрики для присвоения атрибуту значения процесса

(числа или категории) из шкалы

9. Шкала

9) набор значений с определенными свойствами

5. Качество ПС отражается тремя группами показателей, характеризующими:

- *внутреннее, внешнее, качество при использовании* +
- требуемое, обусловленное, реальное
- номинальное, идеальное, реальное
- определенное, достигнутое, недостигнутое

6. На чем основано определение ошибки?

- *на эталонном состоянии объекта* +
- на случайном обнаружении ошибки
- на поисковой деятельности
- на явлении «back door»

7. Какие факторы влияют на степень качества программного средства?

- *качество технологий проектирования* +
- *качество разработки ПС* +
- *качество сопровождения* +
- *качество документирования* +

8. Определите к какому виду относятся следующие угрозы качеству программных средств:

1. Внутренние 1) Ошибки проектирования, ошибки алгоритмизации, ошибки программирования, недостаточное качество защиты
2. Внешние 2) Ошибки эксплуатации, искажение информации в сетях, сбои и отказы аппаратуры компьютера, изменения конфигурации системы

9. Вставьте пропущенное слово

___-средства поддерживают коллективную разработку сложных проектов, используются на этапе системного анализа, разработки технического задания и спецификаций, проектирования концептуальной и логической структур ПС и баз данных (БД), поддерживают автоматическую кодогенерацию и позволяют значительно снижать уровень системных, алгоритмических и программных ошибок при разработке ПО.

Правильный ответ: case

10. Вставьте пропущенное слово

_____является основным методом измерения качества, определения корректности, реальной надежности и безопасности функционирования программ на всех этапах ЖЦ ПС.

Правильный ответ: тестирование.

11. Выделите особенности процесса тестирования программ по отношению к тестированию аппаратуры:

- отсутствие эталонной программы, которой должны точно соответствовать все результаты тестирования
- принципиальная невозможность использования полных тестовых наборов для исчерпывающей проверки функционирования сложных ПС

- относительно невысокая степень формализации критериев качества результатов тестирования и достигаемых при этом корректности и надежности функционирования испытуемых ПС
- все ответы верны +

12. Вставьте пропущенное слово:

Целью_____ПС является удостоверение их качества, надежности и безопасности применения

Правильный ответ: сертификации

13. Результатом системного проектирования являются:

- *системный проект* +
- *техническое задание* +
- *договор на продолжение проектирования* +
- выявление системных ошибок

14. Какими бывают первичные ошибки:

- *технологические ошибки* +
- *программные ошибки* +
- *алгоритмические ошибки* +
- *системные ошибки* +

15. Снижение трудоемкости, длительности проектов ПС, повышение качества разрабатываемых ПС, разработке, эксплуатации и сопровождении, обеспечение возможности расширять программное средство по набору прикладных функций и масштабировать в зависимости от размерности решаемых задач и другое являются:

- *целями применения стандартов* +
- методами применения стандартов
- поводами применения стандартов
- заменой применения стандартов

16. Совокупность нескольких базовых стандартов и/или других нормативных документов с четко определенными и гармонизированными подмножествами обязательных и дополнительных возможностей, предназначенная для реализации заданной функции или группы функций – это:

- *профиль стандартов* +
- группа стандартов
- классификация стандартов
- множества стандартов

17. Совокупность организационных структур, методик, технологий и ресурсов, необходимых для осуществления общего руководства качеством – это:

- *система качества* +
- стандартизация
- сертификация
- метрология

18. Закончите построение модели внешнего и внутреннего качества программных средств, разместив характеристики по

соответствующим им подхарактеристикам.

Функциональность	Пригодность	
	Правильность	
	Способность к взаимодействию	Защищенность
Надёжность	Завершенность	
	Отказоустойчивость	
Эффективность	Восстанавливаемость	
	Времяемкость	
Практичность	Используемость ресурсов	
	Понятность	
	Изучаемость	
	Простота использования	
	Привлекательность	
Сопровождаемость	Анализируемость	
	Изменяемость	
	Стабильность	
	Тестируемость	
Мобильность	Адаптируемость	
	Настраиваемость	
	Совместимость	
	Замещаемость	

19. Соотнесите уровни зрелости модели CMM с их описанием

Уровень 1. Начальный	Самоорганизующийся хаос. Процесс осуществляется случайным образом
Уровень 2. Повторяемый	Процесс планируется и отслеживается
Уровень 3. Определенный	Процесс полностью определен и организован на основе единого стандарта компании
Уровень 4. Управляемый	Количественное управление процессом, его качеством
Уровень 5. Оптимизирующий	Планомерное улучшение и повышение качества

Задания для проведения промежуточной аттестации МДК 07.02Сертификация информационных систем.

Вопросы к экзамену:

1. Законодательство Российской Федерации в области защиты информации.
2. Основные группы методов противодействия угрозам безопасности в корпоративных сетях.
3. Программно-аппаратные методы защиты процесса обработки и передачи информации.
4. Политика безопасности, настройка политики безопасности.
5. Виды неисправностей систем хранения данных.
6. Резервное копирование данных: цели.
7. Резервное копирование данных: методы.
8. Резервное копирование данных: концепции.
9. Резервное копирование данных: планирование.
10. Резервное копирование данных: роль журнала транзакций.
11. Виды резервных копий.
12. Утилиты резервного копирования.
13. Автоматизированные средства аудита.
14. Назначение и применение брандмауэров.
15. Восстановление носителей информации.
16. Воссоздание утраченных файлов.
17. Процедура полного восстановления.
18. Процедура неполного восстановления.
19. Уровни качества программной продукции.
20. Восстановление RAID-массива.
21. Требования к конфигурации серверного оборудования и локальных сетей.
22. Объекты информатизации, требующие обязательной сертификации программных средств и обеспечения.
23. Сертификаты безопасности: виды.
24. Сертификаты безопасности: функции.
25. Сертификаты безопасности: срок действия.
26. Системы сертификации.
27. Процедура сертификации.
28. Платформы и центры сертификации.
29. Сертификат разработчика.

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

31. Процесс подписи и проверки кода.

Примерные практические задания для контроля в соответствии с уровнем освоения

1. С помощью ISO/IEC 17000:2004 и ГОСТ Р ИСО/МЭК 17000-2009 установить российские названия для следующих форм и действий оценки соответствия, приведенных в международном стандарте: testing, inspection, sampling, audit, accreditation, declaration, certification, surveillance.
2. Сопоставить ГОСТ Р ИСО/МЭК 17000-2009 и Федеральный закон «О техническом регулировании» и сделать выводы о соответствии определений следующих терминов: декларирование, сертификация, оценка соответствия, подтверждение соответствия, орган по сертификации, схема оценки (подтверждения) соответствия.
3. Работа с ГОСТ Р ИСО/МЭК 17000-2009. Определить знаки соответствия маркировки продукции и процедура присвоения знака.
4. Определить продукцию, подлежащую сертификации, в соответствии с требованиями выбранных технических регламентов Российской Федерации и Таможенного союза.
5. Определить схемы сертификации для выбранной продукции, описать основные особенности схем.
6. Сопоставить схемы сертификации продукции на соответствие требований технических регламентов РФ и технических регламентов ТС, выделить основные различия.
7. Написать кроссплатформенное приложение, обеспечивающее работу с базой данных SQLite «Магазин музыкальных инструментов» (muz.sdb). Для доступа к данным использовать технологию FireDAC. Для поиска используйте стандартное окно ввода, которое выводит функция InputBox.
8. Написать приложение, обеспечивающее работу с базой данных «Рецепты» (recept.mdb). Для доступа к данным использовать технологию ADO. Для поиска используйте
9. стандартное окно ввода, которое выводит функция InputBox.

Критерии оценки образовательных результатов

1. Шкала оценки устных ответов

Критерии	**Качественная оценка образовательных результатов.**	
	балл (отметка)	**вербальный аналог**
Тема раскрыта в полном объеме, высказывания связные и логичные, использована научная лексика, приведены примеры, сделаны выводы. Ответы на вопросы даны в полном объеме или вопросы отсутствуют.	5	отлично
Тема раскрыта не в полном объеме, высказывания в основном связные и логичные, использована научная лексика, приведены примеры, сделаны выводы. Ответы на вопросы сигнализируют о наличии проблемы в понимании темы.	4	хорошо
Тема раскрыта недостаточно, высказывания несвязные и нелогичные. Научная лексика не использована,примеры не приведены, выводыотсутствуют. Ответы на вопросы в значительной степени зависят от помощи со стороны преподавателя.	3	удовлетворительно
Тема не раскрыта. Логика изложения,примеры, выводы и ответы на вопросы отсутствуют.	2	не удовлетворительно

2. Шкала оценки в соответствии с эталоном

Критерии	**Качественная оценка образовательных результатов.**	
	балл (отметка)	**вербальный аналог**
Задача решена в соответствии с эталоном	5	отлично
В задаче допущен один-два недочета и (или) одна ошибка	4	хорошо
В задаче допущено несколько недочётов и две ошибки	3	удовлетворительно
В задаче допущено несколько недочетов и белее двух ошибок	2	не удовлетворительно