

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кузбасский государственный технический университет
имени Т. Ф. Горбачева»

Институт профессионального образования
Кафедра информатики и информационных систем

Елена Александровна Игнатьева

СЕРТИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Методические материалы к лабораторным
и самостоятельным работам

Рекомендовано цикловой методической комиссией
специальности СПО 09.02.07 «Информационные системы и
программирование» в качестве электронного издания
для использования в образовательном процессе

Кемерово 2024

Рецензенты: Чичерин И.В. – канд. тех. наук, доцент, заведующий кафедрой информационных и автоматизированных производственных систем ФГБОУ ВО «Кузбасский государственный технический университет имени Т.Ф. Горбачева»

Игнатьева, Е.А. Сертификация информационных систем: методические материалы к лабораторным и самостоятельным работам для обучающихся специальности СПО 09.02.07 «Информационные системы и программирование» / сост. Е. А. Игнатьева, Кузбасский государственный технический университет имени Т. Ф. Горбачева. – Кемерово, 2024. – Текст: электронный.

Приведенные методические указания к лабораторным и самостоятельным работам по курсу «Сертификация информационных систем» позволяют углубить знания, полученные в ходе аудиторных занятий; способствуют закреплению теоретических положений; развивают навыки по их практическому применению.

© Кузбасский государственный
технический университет
имени Т. Ф. Горбачева, 2024
© Игнатьева Е. А.,
составление, 2024

СОДЕРЖАНИЕ

Содержание	2
Лабораторные занятия	4
Лабораторная работа №1 Настройка политики безопасности	4
Теоретическая часть	4
Порядок выполнения работы	23
Контрольные вопросы.....	24
Лабораторная работа №2 Создание резервных копий и восстановление баз данных	25
Теоретические положения	25
Порядок выполнения работы	30
Контрольные вопросы.....	34
Лабораторная работа №3 Восстановление носителей информации. Восстановление удаленных файлов.....	36
Теоретические положения	36
Порядок выполнения работы	51
Контрольные вопросы.....	51
Лабораторная работа №4 Мониторинг активности и блокирование портов.....	52
Теоретические положения	52
Порядок выполнения работы	67
Контрольные вопросы.....	67

Лабораторная работа №5 Проверка наличия и сроков действия сертификатов	68
Теоретические положения	68
Порядок выполнения работы	73
Контрольные вопросы.....	73
Лабораторная работа №6 Разработка политики безопасности корпоративной сети	74
Теоретические положения	74
Порядок выполнения работы	80
Контрольные вопросы.....	81
Лабораторная работа №7 Получение сертификата.....	82
Теоретические положения	82
Порядок выполнения работы	101
Контрольные вопросы.....	101
Самостоятельная работа	102
Список литературы.....	104
Основная литература.....	104
Дополнительная литература	104

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ

ЛАБОРАТОРНОЕ РАБОТА №1 НАСТРОЙКА ПОЛИТИКИ БЕЗОПАСНОСТИ

Цель работы – изучить структуру и возможности групповых и локальных политик безопасности, научиться настраивать политику безопасности.

Теоретическая часть

Служба каталогов *Active Directory* является средством для именования, хранения и выборки информации в некоторой распределенной среде, доступное для приложений, пользователей и различных клиентов этой среды. Служба сетевых каталогов хранит информацию об общедоступных приложениях, файлах, принтерах и сведения о пользователях.

Служба каталогов *Active Directory* обеспечивает эффективную работу сложной корпоративной среды, предоставляя следующие возможности.

Пользователи могут регистрироваться в сети с одним именем и паролем и получать при этом доступ ко всем сетевым ресурсам (серверам, принтерам, приложениям, файлам и т. д.) независимо от их расположения в сети.

Средства аутентификации и управления доступом к ресурсам, встроенные в службу *Active Directory*, обеспечивают централизованную защиту сети. Права доступа можно определять не только для каждого объекта каталога, но и каждого свойства (атрибута) объекта.

Администраторы могут централизованно управлять всеми корпоративными ресурсами.

При загрузке компьютера или регистрации пользователя в системе выполняются требования групповых политик; их настройки хранятся в объектах групповых политик (GPO) и «привязываются» к сайтам, доменам или организационным единицам. Групповые политики определяют, например, права досту-

па к различным объектам каталога или ресурсам, а также множество других правил работы в системе.

Служба Active Directory тесно связана с DNS. Этим достигается единство в именовании ресурсов локальной сети и сети Интернет, в результате чего упрощается подключение пользовательской сети к Интернету.

Служба Active Directory может охватывать как один домен, так и множество доменов, один контроллер домена или множество контроллеров домена, т. е. она отвечает требованиям сетей любого масштаба. Несколько доменов можно объединить в дерево доменов, а несколько деревьев доменов можно связать в лес.

Для разработчиков приложений служба каталогов предоставляет доступ ко всем возможностям (средствам) каталога и поддерживает принятые стандарты и интерфейсы программирования (API). Служба каталогов тесно связана с операционной системой, что позволяет избежать дублирования в прикладных программах функциональных возможностей системы, например, средств безопасности.

Каталог состоит из элементов (entries), представляющих собой информацию, или атрибуты, связанные с некоторым реальным объектом, например компьютером, человеком или организацией.

Каждый объект принадлежит хотя бы к одному объектному классу, представляющему собой некоторое семейство объектов с определенными общими характеристиками. Класс объектов определяет тип информации, содержащейся в Active Directory для экземпляров (объектов) данного класса. Атрибуты могут быть как обязательными (mandatory) для данного класса (например, имя), так и дополнительными (optional) (пароль).

Контейнер (container) – это специфический объект службы каталогов, который, в отличие от обычных объектов, не имеет какого-либо физического представления, а служит только структурной организации других объектов каталога. Типичным примером контейнеров могут служить организационные единицы, или подразделения, используемые для упрощения администрирования отдельных групп ресурсов или пользователей в домене.

Элементы каталога организованы в виде иерархического дерева, называемого Directory Information Tree (DIT, Информационное дерево каталога или просто Дерево каталога). Элементы, находящиеся ближе к корню дерева, обычно представляют крупные объекты, например, организации или компании; элементы, располагающиеся на ветвях этого дерева (листья), представляют более простые объекты – пользователей, устройства, компьютеры.

Схема каталога (Directory Schema) – это набор правил, описывающих структуру дерева каталога, объявления и синтаксис объектных классов и типы атрибутов, входящих в каталог.

Схема каталога гарантирует, что все добавления или изменения каталога соответствуют данным правилам, и препятствует появлению некорректных элементов, ошибочных типов атрибутов или классов.

В Active Directory схема реализована как набор экземпляров объектных классов, хранящийся в самом каталоге. Этим Active Directory отличается от многих каталогов, в которых схема хранится в текстовом файле, считываемом при запуске каталога. Когда схема хранится в каталоге, пользовательские приложения могут обращаться к ней и узнавать об имеющихся объектах и свойствах. Схему Active Directory можно динамически обновлять: модифицировать и расширять.

Основные компоненты любой службы каталога – база данных, содержащая нужную информацию, и один или несколько протоколов, обеспечивающих доставку данных пользователям.

Active Directory обеспечивает хранение любой общедоступной информации. Как и другие службы каталогов, Active Directory обеспечивает некоторый механизм хранения информации и протоколы для доступа к ней.

Домены – это известное решение для администрирования групп, предоставляющее каждому пользователю учетную запись в конкретном домене. В среде Windows Server каждый домен должен иметь имя, отвечающее соглашениям именования доменов Domain Name System (DNS). В каждом домене один или несколько компьютеров должны выполнять функции контроллеров домена.

В среде Windows Server каждый контроллер домена содержит полную копию базы данных Active Directory этого домена. В Active Directory используются так называемое ядро Extended Storage Engine (ESE) и два различных протокола, обеспечивающих связь между клиентами и базой данных. Для поиска контроллера домена клиент обращается к протоколу, описанному в DNS. Для доступа к данным в Active Directory клиент использует протокол Lightweight Directory Access Protocol (LDAP).

В большинстве современных сетей TCP/IP используется служба DNS, главное назначение которой преобразовывать символичные имена в IP-адреса. Для этого каждый компьютер-сервер DNS имеет набор записей с информацией о ресурсах. Каждая запись имеет некоторый тип, определяющий характер и назначение хранящейся информации. Интеграцию служб Active Directory и DNS можно рассматривать в трех аспектах:

- домены Active Directory и домены DNS имеют одинаковую иерархическую структуру и схожее пространство имен;
- зоны (zone) DNS могут храниться в Active Directory. Если используется сервер DNS, входящий в состав Windows Server, то первичные зоны (primary zone), занесенные в каталог, реплицируются на все контроллеры домена, что обеспечивает лучшую защищенность службы DNS.

Каждый элемент Active Directory и каждый атрибут любого элемента имеют список управления доступом (ACL), который определяет права и возможности пользователей в отношении доступа к конкретным элементам и атрибутам. Эффективное управление доступом невозможно без достоверной аутентификации клиентов, Active Directory использует для этой цели протокол Kerberos.

Управление подразделениями, компьютерами, группами и учетными записями пользователей.

Для управления учетными записями пользователей и компьютерами следует вначале войти в раздел администрирования (Administrative Tools) и выбрать Active Directory Users and Computers .

Для создания подразделения, или организационной единицы (Organizational Unit, OU) следует:

1. Выделить объект типа «домен» и нажать правую кнопку мыши. В появившемся меню выбрать команду Создать | Подразделение (New | Organizational Unit). Можно воспользоваться панелью инструментов и кнопкой Создание нового подразделения в текущем контейнере (Create a new organizational unit in a current container) на панели инструментов.

2. В открывшемся окне указать имя создаваемого подразделения и нажмите кнопку ОК.

В результате в выбранном вами домене будет создано подразделение с заданным именем. В дальнейшем внутри него можно создать вложенные подразделения.

В процессе установки домена Windows в нем создается несколько встроенных групп, обладающих определенным набором прав. Их можно использовать для присвоения администраторам или пользователям определенных ролей или прав доступа в домене. Эти группы служат для назначения разрешений доступа пользователям, на которых возложено выполнение в данном домене каких-либо административных функций.

Локальные группы в домене:

- администраторы (Administrators);
- гости (Guests);
- операторы архива (Backup Operators);
- операторы печати (Print Operators);
- операторы сервера (Server Operators);
- операторы учета (Account Operators);
- пользователи (Users);
- репликатор (Replicator);
- совместимый с пред-Windows доступ (Pre-Windows CompatibleAccess).

Глобальные группы:

- администраторы домена (Domain Admins);
- владельцы-создатели групповой политики (Group Policy Creator Owners);
- гости домена (Domain Guests);
- издатели сертификатов (Cert Publishers);

- компьютеры домена (Domain Computers);
- контроллеры домена (Domain Controllers);
- пользователи домена (Domain Users);

Универсальные группы:

- администраторы предприятия (Enterprise Admins);
- администраторы схемы (Schema Admins).

Универсальные группы создаются только на контроллерах корневого (первого в лесу) домена. В зависимости от установленных на сервере служб могут быть и дополнительные встроенные группы, локальные в домене или глобальные. По умолчанию все встроенные локальные группы домена находятся в папке BuiltIn объекта домена. Все встроенные глобальные группы находятся в папке Users. Встроенные группы можно переносить в другие контейнеры или подразделения в пределах домена.

По умолчанию каждая созданная в домене учетная запись автоматически становится членом группы Пользователи домена. Кроме того, группа Пользователи домена является членом локальной в домене группы Пользователи.

Любой объект типа Компьютер (Computer) при создании по умолчанию автоматически включается в группу Компьютеры домена.

Группа Администраторы домена объединяет всех пользователей, имеющих полный административный доступ в домене. По умолчанию Администраторы домена являются членами локальной в домене группы Администраторы.

Группа Гости домена объединяет все учетные записи, с помощью которых можно зарегистрироваться в домене без пароля и получить минимальные права доступа. По умолчанию Гости домена являются членами локальной в домене группы Гости.

Помимо перечисленных выше встроенных групп администратор может создать любое количество групп пользователей и предоставить им необходимый набор прав и разрешений.

Для создания группы необходимо выполнить следующее:

1. Выбрать подразделение, где следует создать группу, и нажмите правую кнопку мыши. Выбрать в появившемся меню команду Создать | Группа (Group), либо нажать кнопку Создание

новой группы в текущем контейнере (Create New Group in a Current Container) на панели инструментов.

2. В открывшемся окне диалога Новый объект – Группа (New Object – Group) в поле Имя группы (Group name) ввести имя создаваемой группы.

3. Установить переключатель Тип группы (Group type) в одно из положений, соответствующее типу создаваемой группы: Группа безопасности (Security) или Группа распространения (Distribution). Первый тип группы служит для предоставления пользователям определенного набора прав доступа к таким ресурсам сети, как файлы и принтеры. Вторым типом группы служит только для распространения информации в сети, например в качестве списков рассылки электронной почты. Следует отметить, что группы безопасности могут использоваться в качестве групп распространения.

4. Установив в одно из положений переключатель Область действия группы (Group scope), выбрать подходящую область действия создаваемой группы. Область действия группы определяет, где может быть видна данная группа (уровень доступности) и какие типы объектов могут быть ее членами, и может быть выбрана как:

- локальная в домене (Domain Local): пользователи, а также глобальные и универсальные группы из всего леса, другие локальные группы из этого же домена;
- глобальная (Global): пользователи, а также глобальные и универсальные группы;
- универсальная (Universal): пользователи и глобальные группы (только в основном режиме домена).

Для создания в домене учетной записи пользователя, предположим с идентификатором `rorov_as`, необходимо выполнить следующее:

1. Указать подразделение, в котором следует создать учетную запись, и нажмите правую кнопку мыши. В появившемся меню выбрать команду Создать | Пользователь.

2. В окне диалога Новый объект – Пользователь (New Object – User) в поле Имя входа пользователя (User logon name) ввести уникальный идентификатор, в поле Имя (First name) – имя поль-

зователя, в поле Фамилия (Last name) – фамилию пользователя, в поле Полное имя (Full name) автоматически появятся имя и фамилия пользователя. После ввода всей необходимой информации нажать кнопку Далее (Next).

3. В следующем окне в полях ввода Пароль (Password) и Подтверждение (Confirm password) ввести с клавиатуры пароль учетной записи пользователя.

4. Если необходима принудительная смена пароля при первой регистрации в сети, установить флажок Потребовать смену пароля при следующем входе в систему (User must change password at next logon). С целью защиты от атак по подбору пароля, следует установить срок действия пароля пользователя, сбросив флажок Срок действия пароля не ограничен (Password never expires).

6. Установленный флажок Запретить смену пароля пользователем (User cannot change password) запрещает пользователю самостоятельно изменять свой пароль.

7. Если только что созданная учетная запись по каким-либо причинам должна быть заблокирована, установить флажок Отключить учетную запись (Account disabled).

8. По завершении настройки создаваемой учетной записи нажать кнопку Далее.

9. В окне диалога, запрашивающего подтверждение правильности выполняемого действия, нажать кнопку Готово (Finish).

Для ввода дополнительной информации или изменения некоторых данных пользователя:

1. Указать учетную запись пользователя, информацию которой следует изменить, и нажать правую кнопку мыши. В появившемся меню выбрать команду Свойства.

2. Внести необходимые изменения и нажать кнопку ОК.

Учетную запись пользователя можно перемещать из одного подразделения в другое в пределах одного домена или между доменами. Для соответствующего перемещения учетной записи этого пользователя следует воспользоваться технологией Drag and Drop (перетаскивание), применяемой практически ко всем визуальным объектам операционной системы семейства Windows.

Для добавления пользователя в группу необходимо выполнить следующие действия:

1. Указать группу, в которую необходимо добавить пользователя, и нажмите правую кнопку мыши. В появившемся меню выбрать команду Свойства. Появится окно свойств группы.

2. Перейти на вкладку Члены группы (Members) окна свойств и нажать кнопку Добавить.

3. Появится окно Выбор: Пользователи, Контакты или Компьютеры (Select Users, Contacts, or Computers). Здесь можно задать область выполнения запроса: весь каталог, определенный домен или определенная часть дерева подразделения внутри домена. Обратите внимание, что каталог может состоять из множества доменов.

4. Выбрать имя добавляемого пользователя и нажать кнопку Добавить. Обратите внимание, что, нажав клавишу и одновременно выполняя щелчки на нужных объектах, в этом диалоговом окне можно одновременно выбрать несколько пользователей или групп.

В результате все выбранные объекты станут членами соответствующей группы.

После создания объекта «компьютер» можно управлять им удаленно, диагностируя службы, работающие на этом компьютере, просматривая события и т. д.

Для того чтобы управлять компьютером удаленно:

1. В окне оснастки Active Directory – Пользователи и компьютеры укажите имя компьютера и нажмите правую кнопку мыши. В появившемся меню выбрать команду Управление (Manage).

2. Для выбранного компьютера будет запущена оснастка Управление компьютером (Computer Management).

Как правило, сети больших предприятий на платформе Windows обладают чрезвычайно разветвленным деревом каталога. Большое количество ветвей, а также наличие достаточно автономных площадок организации, включенных в общее дерево каталога, усложняют управление. Администрирование сети, каталог которой состоит из десятков тысяч объектов, не может без-

опасно осуществляться одним или несколькими администраторами, имеющими права доступа ко всем объектам.

В подобных случаях следует применять делегирование прав администрирования. Это чрезвычайно мощный инструмент, который в больших организациях позволяет более эффективно сконфигурировать систему безопасного администрирования. С его помощью управление отдельными областями сети смогут осуществлять специально назначенные ответственные лица – администраторы. При делегировании прав администрирования очень важно наделять ответственных лиц полномочиями, позволяющими выполнять функции администратора только в пределах их зоны ответственности, они не должны иметь возможность администрировать объекты каталога, находящиеся в других частях сети организации.

Права на создание новых пользователей или групп предоставляются на уровне подразделения или контейнера, в котором будут создаваться учетные записи. Администраторы групп одного подразделения могут не иметь прав на создание и управление учетными записями другого подразделения в том же домене. Если права доступа и настройки политик получены на более высоком уровне дерева каталога, они могут распространяться вниз по дереву благодаря механизму наследования прав доступа.

С помощью инструментов управления Active Directory администратор может делегировать другим пользователям и группам право управления частью каталога. Это в полной мере относится и к объектам групповой политики, в отношении которых могут быть, в частности, делегированы следующие права:

- управление связями GPO с сайтом, доменом или подразделением (организационной единицей). Для этого с помощью инструмента управления Active Directory следует указать объект (сайт, домен или организационную единицу) и щелкнуть правой кнопкой мыши. В появившемся контекстном меню выбрать команду Делегирование управления (Delegate Control). Запустится Мастер делегирования управления (Delegation of Control Wizard). С его помощью можно выбрать объект групповой политики, группу или пользователя, которому должны быть делегированы

права, а также и само право (в данном случае Управление ссылками групповой политики (Manage Group Policy links));

– создание и удаление всех дочерних объектов групповой политики. По умолчанию правом создания объектов в GPO обладают администраторы домена (Domain Admins) и администраторы предприятия (Enterprise Admins), а также операционная система. Для делегирования пользователю права управления объектами групповой политики домена необходимо включить его в группу «Создатели-владельцы групповой политики» (Group Policy Creator Owners);

– редактирование свойств объектов групповой политики. По умолчанию правом редактирования GPO обладают администраторы домена, администраторы предприятия и операционная система. Для делегирования пользователю права редактирования объекта групповой политики необходимо включить его в одну из указанных групп безопасности.

Чтобы позволить группе или пользователю управлять некоторым подразделением (контейнером):

1. Запустите Active Directory – Пользователи и компьютеры.
2. Укажите подразделение, управление которым необходимо передать, и нажмите правую кнопку мыши. В появившемся меню выберите команду Делегировать управление (Delegate control). Запустится Мастер делегирования управления (Delegation of Control Wizard). Нажмите кнопку Далее.
3. В следующем окне мастера нажмите кнопку Добавить и выберите пользователя или группу, которой вы хотите разрешить управление подразделением, нажмите кнопку ОК и затем кнопку Далее.
4. В открывшемся окне диалога мастера делегирования управления в окне со списком Делегировать следующие обычные задачи (Delegate the following common tasks) выберите одну или несколько операций, право выполнения которых делегируется указанному пользователю или группе. Если нужно делегировать право выполнения более специализированной задачи, установите переключатель Создать особую задачу для делегирования (Create a custom task to delegate). Нажмите кнопку Далее.

5. Если указана особая задача для делегирования в следующем окне, можно выбрать область применения для этой задачи: положение переключателя. Этой папкой и существующими в ней объектами, созданием новых объектов в этой папке (This folder, existing objects in this folder, and creation of new objects in this folder), в этом случае вы передадите группе право на администрирование всего контейнера, или положение Только следующими объектами в этой папке (Only the following objects in the folder) и установить флажки возле нужных объектов, в этом случае группа сможет управлять только выбранными объектами. Затем нажмите кнопку Далее.

6. В открывшемся окне определяются делегируемые разрешения. Можно отображать и устанавливать общие разрешения или разрешения для отдельных свойств или дочерних объектов. В пределах контейнера можно делегировать не все, а только некоторые права администрирования: например, можно делегировать только права на модификацию (чтение-запись) выбранного контейнера без дочерних объектов. Задайте нужные разрешения и нажмите кнопку Далее.

7. В следующем окне сводки выводится информация о выбранных действиях. Можно вернуться назад и скорректировать параметры. Если все правильно, нажмите кнопку Готово.

Эффективное функционирование многопользовательской операционной системы невозможно без четкого разграничения доступа к ресурсам. Одним из средств, позволяющих настраивать параметры безопасной работы пользователей в сети в операционных системах семейства Windows (NT, 2000, XP и выше), являются политики безопасности.

Реализация политик безопасности в Windows предоставляет достаточно широкие возможности, в том числе настройку политики безопасности для всего дерева доменов. Установив политику безопасности в одном месте, администраторы могут контролировать безопасность всех рабочих станций домена. Политики безопасности в Windows реализуются с помощью средств групповых политик (group policy).

Групповая политика имеет следующие преимущества:

- основываясь на службе Active Directory системы Windows , позволяет как централизованно, так и децентрализованно управлять параметрами политики;
- обладает гибкостью и масштабируемостью. Может быть применена в широком наборе конфигураций системы, предназначенных как для малого бизнеса, так и для больших корпораций;
- обладает высокой степенью надежности и безопасности;
- групповые политики расширяют и используют преимущества Active Directory. Их настройки находятся в объектах групповых политик (Group Policy Object, GPO), которые в свою очередь ассоциируются с такими контейнерами Active Directory, как сайты, домены и подразделения (организационные единицы).

Для запуска объекта Групповая политика следует выполнить следующие действия:

- 1) выбрать объект Active Directory, для которого необходимо установить групповую политику безопасности и правой кнопкой мыши вызвать контекстное меню;
- 2) выбрать элемент Свойства (Properties);
- 3) в диалоговом окне свойств выбрать вкладку Групповая политика (Group Policy);
- 4) для модификации глобальной политики следует выбрать кнопку Edit, если политика еще не была создана – New и ввести имя, либо воспользоваться тем, которое предлагает система.

Создать групповую политику для контейнера Active Directory можно только при наличии определенного набора условий. Необходимо иметь работающий контроллер домена Windows . Пользователь, который создает групповую политику, должен обладать правами на чтение и запись в системный том контроллеров домена (папка Sysvol). Кроме того, он должен иметь право модификации выбранного контейнера Active Directory.

После выбранных действий загружается корневой узел, представляющий собой GPO, присоединенный к определенному контейнеру.

Имя этого GPO и имя контейнера, к которому он присоединен, отображаются в окне структуры в следующем формате: Имя_политики [Имя_домена] Policy.

Затем пространство имен подразделяется на два узла более низкого уровня: «Конфигурация компьютера» (Computer Configuration) и «Конфигурация пользователя» (User Configuration). Используя их, можно создавать и настраивать групповые политики для компьютера и пользователей.

Узел «Конфигурация компьютера» содержит параметры всех политик, определяющих работу компьютера. Они регулируют функционирование операционной системы, вид рабочего стола, задают параметры выполняемых приложений, определяют работу средств обеспечения безопасности и т. д. Групповая политика применяется к рабочей станции домена на этапе загрузки системы и в дальнейшем при выполнении циклов обновления.

Узел «Конфигурация пользователя» содержит параметры всех политик, определяющих работу пользователя на компьютере. Они регулируют вид рабочего стола, как и в предыдущем случае, задают параметры выполняющихся приложений, определяют работу средств обеспечения безопасности и пользовательских сценариев входа и выхода. Групповая политика применяется к пользователю при его регистрации и в дальнейшем при выполнении циклов обновления.

Опишем некоторые расширения объекта «Групповая политика»:

- административные шаблоны. (Administrative Templates). Здесь находится групповая политика, определяющая параметры реестра, задающие работу и внешний вид рабочего стола, компонент операционной системы и приложений;
- параметры безопасности (Security Settings). Служит для настройки параметров системы безопасности компьютеров, на которые воздействует данный объект групповой политики. С помощью групповых политик можно настроить безопасность индивидуального компьютера, домена и целой сети;
- установка программ (Software Installation). Служит для централизованного управления программным обеспечением ор-

ганизации. С его помощью можно задавать различные режимы установки новых программ на компьютеры пользователей;

- сценарии (Scripts). Сценарии используются для автоматического выполнения набора команд при загрузке операционной системы и в процессе завершения ее работы, а также при регистрации и отключении пользователя от сети. Для выполнения сценариев, написанных на Microsoft JScript и Microsoft Visual Basic Scripting Edition, можно применять сервер сценариев (Windows Scripting Host);

- перенаправление папок (Folder Redirection). Позволяет перенаправлять обращение к специальным папкам в сеть.

С помощью расширения «Параметры безопасности» в GPO можно определить параметры политики безопасности, определяющие различные аспекты работы системы безопасности Windows. Созданная в объекте групповой политики конфигурация воздействует на все компьютеры, находящиеся в контейнере, к которому присоединен данный GPO.

Расширение «Параметры безопасности» позволяет настраивать следующие аспекты системы безопасности компьютера:

- –политики учетных записей (Account Policies). Можно настраивать политики безопасности как учетных записей в масштабах домена, так и локальных учетных записей. Здесь определяются политика паролей, политика блокировки паролей и политика Kerberos, распространяющаяся на весь домен;

- локальные политики (Local Policies). Можно настраивать политику аудита, назначать права пользователей и различные параметры безопасности, доступные для настройки в системе Windows;

- журнал событий (Event Log). Можно настраивать политики безопасности, определяющие работу журналов событий приложений, системы и безопасности;

- группы с ограниченным доступом (Restricted Groups). Можно регулировать членство пользователей в специфических группах. Сюда обычно включают встроенные группы, такие как Администраторы, Операторы архива и другие, имеющие по умолчанию права администратора. В эту категорию могут быть включены и другие группы, безопасность которых требует особо-

го внимания и членство в которых должно регулироваться на уровне политики;

- системные службы (System Services). Можно настраивать безопасность и параметры загрузки для работающих на компьютере служб. В этом разделе могут быть использованы расширения, с помощью которых можно осуществлять настройку безопасности, специфическую для данной службы;

- реестр (Registry). Можно настраивать безопасность различных разделов реестра;

- файловая система (File System). Можно настраивать безопасность определенных файлов;

- политики открытого ключа (Public Key Policies). Можно настраивать политики безопасности в отношении шифрования информации с помощью EFS, авторизации корневого сертификата в масштабах домена, авторизации доверенного сертификата и т. д.;

- политики безопасности IP (IPSEC). Позволяет настраивать политику безопасности IP для компьютеров.

Политики безопасности, определяемые расширением «Параметры безопасности», действуют на компьютеры и частично на пользователей. Поскольку политика безопасности Windows NT, при переходе к Windows низкоуровневые политики безопасности не переносятся. Если при переходе создается новое дерево доменов, одновременно создается и новая политика безопасности, назначаемая по умолчанию. Если при переходе домен присоединяется к уже существующему дереву, политика безопасности берется от родительского домена.

Для модификации настроек безопасности щелкните на папке «Параметры безопасности», затем щелчками на соответствующих узлах откройте весь путь, ведущий к интересующим настройкам. В правом подокне окна «Групповая политика» двойным щелчком выберите настраиваемую политику и в открывшемся окне настройте ее.

Рассмотрим работу указанных расширений на конкретных примерах.

1. Настройка политики паролей.

Предположим, нам необходимо установить следующие правила политики паролей и блокировки:

- минимальная длина пароля – 8 символов;
- максимальный срок действия пароля – 30 дней;
- блокировать консоль после трех неудачных попыток входа.

Для реализации указанных правил выполним следующие действия:

1) откроем глобальную политику безопасности домена (см. выше) и расширение «Политики безопасности» (Security Settings);

2) выберем пункт «Политика учетных записей» (Account Policies), а затем политику паролей (Password Policy);

3) в правой части окна появится полный список правил, поддерживаемых политикой безопасности Windows ;

4) найдем требуемые правила:

а) минимальная длина пароля (Minimum password length);

б) максимальный срок действия пароля (Maximum password age);

установим требуемые значения, вызвав соответствующие диалоговые окна двойным щелчком мыши на названии правила;

5) для установки параметра блокировки перейдем в раздел политики блокировки учетных записей (Account Lockout Policy), выберем необходимое правило в правой части окна – Account lockout threshold – и установим требуемое значение – три.

2. Политика учетных записей.

Предположим, нам необходимо разрешить всем пользователям домена использовать привилегию изменения системного времени. Для этого следует выполнить:

1) откроем глобальную политику безопасности домена (см. выше) и расширение «Политики безопасности» (Security Settings);

2) выберем пункт «Локальные политики» (Local Policies), а затем политику назначения прав пользователей (User Rights Assignment);

3) в правой части окна выберем требуемое правило – Change the system time и добавим пользователя Все (Evryone).

Применение групповых политик происходит в последовательности, соответствующей иерархии GPO: сначала объект групповой политики сайта, затем домена, затем GPO, связанные с подразделениями в соответствии с их вложенностью. Порядок выполнения групповых политик можно изменить с помощью настроек, блокирующих определенные групповые политики или заставляющих их выполняться принудительно. Кроме того, на порядок выполнения групповых политик влияет применение групп безопасности.

По умолчанию настройки групповой политики, применяемые к контейнеру определенного уровня, наследуются всеми контейнерами более низких уровней и находящимися внутри них пользователями и компьютерами. Если с дочерней организационной единицей (контейнером) связан свой GPO, он может устанавливать для нее индивидуальные настройки групповых политик, отменяющие применение к ней наследуемых настроек. Если некоторые настройки групповых политик родительского контейнера не заданы (not defined), то они не наследуются и дочерними контейнерами. Если родительский контейнер обладает сконфигурированными настройками групповых политик, которые не заданы в GPO дочернего контейнера, то такие настройки наследуются.

Наследование настроек групповых политик родительского контейнера дочерним контейнером, с которым связан собственный объект групповой политики, может иметь место только в случае совместимости этих групповых политик. Например, если политика родительского контейнера задает определенную конфигурацию рабочего стола компьютера пользователя, а политика дочернего контейнера дополняет ее, пользователь увидит на своем рабочем столе все элементы, заданные обеими политиками. Если же групповая политика родительского контейнера противоречит групповой политике дочернего контейнера, выполняются только настройки GPO, связанного с дочерним контейнером.

Подобное положение вещей может быть изменено. Установка флажка Блокировать наследование политики (Block Policy

inheritance), находящегося на вкладке Групповая политика окна свойств некоторого контейнера, запрещает наследование каких-либо групповых политик, установленных для родительского контейнера.

Существует средство, позволяющее установить принудительное применение групповой политики, настроенной для некоторого контейнера, всеми контейнерами более низкого уровня. Для этого на вкладке Групповая политика окна свойств контейнера следует нажать кнопку Параметры (Options). В появившемся окне диалога Параметры необходимо установить флажок Не перекрывать (No override). В этом случае дочерние контейнеры будут наследовать (т. е. не смогут переопределить) все настройки родительского контейнера, даже в том случае, если для дочерних контейнеров установлен флажок Блокировать наследование политики.

По умолчанию групповая политика применяется синхронно, т. е. политики компьютера применяются до появления окна «Вход в Windows» (Log on to Windows), а политики пользователя – до передачи операционной системой управления оболочке, интерактивно взаимодействующей с пользователем. Подобный порядок можно изменить, однако делать это не рекомендуется, поскольку асинхронное применение групповых политик может привести к непредсказуемым и нежелательным результатам.

Применение групповых политик не ограничивается только, например, моментом загрузки операционной системы компьютера или регистрацией пользователя в системе. При работе компьютера в сети групповые политики могут измениться, поэтому они применяются периодически (по умолчанию – каждые 90 минут). Длительность периода применения политик можно изменять. Если задать его равным нулю, групповые политики применяются через каждые 7 секунд. Следует учитывать, что при уменьшении периода применения групповых политик значительно увеличивается нагрузка на систему. На контроллерах доменов период применения политик равен 5 минутам.

Настройки расширений Установка программ и Переназначение папки применяются только при загрузке операционной системы или регистрации пользователя в системе, поскольку пери-

одическое применение этих групповых политик может вызвать нежелательные результаты.

Порядок выполнение работы

Данная лабораторная работа предполагает выполнение следующих этапов:

1. Создать новую организационную единицу (имя выбрать произвольно, например, my_unit).
2. Создать новую группу.
3. Создать в организационной единице трех новых пользователей: для всех потребовать смену пароля при входе и ограничить срок действия пароля. Одного из пользователей включить в новую группу.
4. Делегировать права на созданную организационную единицу пользователю из новой группы.
5. Установить максимальный срок действия пароля – 30 дней.
6. При вводе нового пароля требовать его неповторяемость. Хранить в системе 2 предыдущих пароля.
7. Установить минимальную длину пароля – 10 символов.
8. Установить аудит успеха для событий входа в систему.
9. Назначить возможность выключения системы только для администраторов.
10. Разрешить вход в систему только для членов группы «Администраторы» и определенного пользователя.
11. Разрешить доступ к компьютеру из сети только для определенного пользователя.
12. Блокировать консоль пользователя после ввода двух неверных паролей на 5 минут.
13. Отображать последнее имя пользователя при диалоге входа в систему.
14. Разрешить определенному пользователю изменять политику аудита системы.

Контрольные вопросы

1. Назначение Active Directory и основные возможности.
2. Какова структура Active Directory?
3. Для чего используются организационные единицы, когда и с какой целью их следует создавать?
4. Какие группы пользователей операционная система создает по умолчанию?
5. Может ли один и тот же пользователь входить в разные группы?
6. В каких случаях следует использовать делегирование прав?
7. Какие права могут быть делегированы?
8. Пользователям, каких групп можно делегировать права?
9. Какие виды политик безопасности поддерживаются, сферы их применения?
10. Какие параметры безопасности можно настроить в глобальной политике безопасности?
11. Как взаимодействуют между собой глобальная и локальная политики безопасности?
12. Какие правила наследования политик безопасности поддерживаются?

ЛАБОРАТОРНАЯ РАБОТА №2

СОЗДАНИЕ РЕЗЕРВНЫХ КОПИЙ И ВОССТАНОВЛЕНИЕ БАЗ 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.

Теоретические положения

Предотвращение потерь данных – одна из самых важных проблем, с которой можно столкнуться при управлении системами баз данных. Потери данных могут иметь место в результате множества самых различных проблем:

- неисправности аппаратного обеспечения;
- вирусы;
- некорректное использование инструкций UPDATE и DELETE;
- ошибки программного обеспечения;
- аварийные ситуации, например, пожар или затопление.

Чтобы избежать потери данных, можно реализовать для базы данных стратегию восстановления. Стратегию восстановления необходимо спланировать, реализовать и протестировать с учетом возможных неисправностей, с которыми можно встретиться в процессе работы системы, и необходимого уровня защиты данных. В витринах данных, то есть в случаях, когда данные можно восстановить из других систем, вероятно, нет необходимости создавать резервные копии каждой отдельной транзакции. Возможно, будет достаточно выполнять полное резервное копирование данных с регулярными временными интервалами. И, наоборот, для базы данных, в которой хранятся транзакции интернет-магазина, возможно, будет необходимо сохранять резервные копии каждой отдельной транзакции. СУБД SQL Server предоставляет полный комплекс функций для реализации именно того вида резервного копирования, который вам необходим. В данной лекции рассматриваются наиболее широко используемые в Microsoft SQL Server стратегии для защиты данных.

Полное резервное копирование базы данных

Самой распространенной стратегией резервного копирования является резервное копирование всей базы данных через заранее заданные промежутки времени (например, каждую ночь). Благодаря такой стратегии аварийного восстановления можно восстановить базу данных до состояния на момент выполнения последнего резервного копирования. Эта стратегия реализуется посредством выполнения полных резервных копий базы данных, как рассказывается ниже.

Полная резервная копия базы данных содержит все данные и метаданные базы данных, которые необходимы для восстановления базы данных полностью, включая полнотекстовые каталоги. При восстановлении базы данных из полной резервной копии восстанавливаются все файлы базы данных, причем данные извлекаются в непротиворечивом состоянии на тот момент времени, в который выполнялось резервное копирование. Пока выполняется резервное копирование, база данных работает в рабочем режиме, и пользователь может выполнять транзакции, изменяя данные обычным путем. Термин "непротиворечивое состояние" означает, что все транзакции, которые были зафиксированы в процессе выполнения резервного копирования базы данных, применяются, а все транзакции, которые не были завершены, подвергаются откату. Для ситуаций, которые могли бы привести к нарушению непротиворечивости данных вследствие выполнения транзакций, изменяющих данные в процессе выполнения резервного копирования, в SQL Server есть особый процесс, который позволяет гарантировать непротиворечивость данных. Этот процесс выполняет запись на устройство резервного копирования как страниц данных, так и журнала транзакций.

Полнотекстовые каталоги были введены в базы данных, чтобы добавить в SQL Server функции полнотекстового индексирования. Полнотекстовое индексирование позволяет быстрее и с большей точностью осуществлять поиск данных в базе данных. Дополнительную информацию о полнотекстовом индексировании см. в Электронной документации по SQL Server в разделе «Полнотекстовые индексы».

Скорость резервного копирования определяется скоростью используемых устройств ввода/вывода (тех устройств ввода/вывода, которые используются для сбора и хранения информации). Чтобы добиться наилучшей производительности, SQL Server считывает файлы последовательно. Если ваши устройства ввода/вывода способны одновременно обрабатывать данные ввода/вывода резервного копирования и данные ввода/вывода, поступающие в результате обычного использования системы, то создание резервной копии окажет на производительность системы незначительное воздействие. Тем не менее, лучше выполнять полное резервное копирование базы данных при отсутствии пиковых нагрузок.

Простая модель восстановления

Следует заранее уведомить SQL Server о том, какой тип резервного копирования вы намерены использовать, поэтому надо сконфигурировать базу данных так, чтобы настройки соответствовали выбранному вами типу резервного копирования. Такая настройка выполняется посредством выбора значения параметра «модель восстановления базы данных». Модель восстановления базы данных, которая используется по умолчанию, является производным от модели восстановления модели базы данных, определенной при ее создании. Чтобы реализовать стратегию резервного копирования, которая будет включать только полные резервные копии, следует выбрать простую модель восстановления (SIMPLE).

Выбираем модель восстановления SIMPLE

В меню Start (Пуск) выберите All Programs, Microsoft SQL Server 2005, SQL Server Management Studio (Все программы, Microsoft SQL Server 2005, Среда SQL Server Management Studio).

В диалоговом окне Connect To Server (Соединение с сервером) нажмите кнопку Connect (Соединить).

В панели инструментов Standard (Стандартная) нажмите кнопку New Query (Новый запрос), чтобы открыть окно New Query (Новый запрос).

Чтобы задать модель восстановления, можно использовать инструкцию ALTER DATABASE. Введите текст следующей инструкции и нажмите кнопку Execute (Выполнить).

```
USE master;
```

```
GO
```

```
ALTER DATABASE AdventureWorks
```

```
SET RECOVERY SIMPLE;
```

```
GO
```

Проверяем настройки модели аварийного восстановления.

Чтобы просмотреть заданную для базы данных модель восстановления, можно использовать функцию DATABASEPROPERTYEX, которая извлекает параметры текущей базы даты или свойства указанной базы данных. Выполните инструкцию, приведенную ниже, чтобы извлечь информацию о модели восстановления базы данных AdventureWorks.

```
SELECT DATA BASE PROPERTYEX ('AdventureWorks',  
'Recovery')
```

Убедитесь, что в результатах запроса указана модель восстановления SIMPLE.

Закройте окно среды SQL Server Management Studio.

Устройства резервного копирования

До начала выполнения операций резервного копирования необходимо определить, где будут храниться резервные копии. Место хранения резервных копий называется устройством резервного копирования. Каждое устройство резервного копирования может хранить несколько резервных копий разных типов. Существует два разных вида устройств резервного копирования:

Ленточные устройства. Могут использоваться для хранения резервных копий на лентах. Ленточные устройства должны быть установлены локально. Резервная копия может занимать несколько лент, а на одной ленте могут находиться одновременно резервные копии SQL Server и Windows.

Дисковые устройства. Файлы на локальном или удаленном диске или дисковом накопителе. К этим файлам обращаются, указывая путь к файлу, в котором хранится резервная копия. Для

обращения к удаленным хранилищам следует использовать путь в формате UNC.

Резервное копирование файлов SQL Server на ленточные устройства в настоящее время используется не очень часто. Если резервные копии SQL Server сохраняются на лентах, то они обычно создаются при помощи программ сторонних разработчиков, которые предлагают дополнительные функции, например, использование удаленного ленточного хранилища. В качестве альтернативы ленточное устройство может использоваться для дополнительного страхования сохранности данных, резервная копия которых уже сохранена на дисковом устройстве.

Устройства резервного копирования идентифицируются по имени устройства. В качестве имени устройства может использоваться имя логического или физического устройства. Имя физического дискового устройства представляет собой путь к файлу резервной копии, например, «\\BACKUPSERVER \Backups\ adv\ AdventureWorks.bak». Этот путь можно включить непосредственно в инструкцию резервного копирования. Имя логического устройства представляет собой имя, указывающее на имя физического устройства резервного копирования и хранящееся в SQL Server. Когда в инструкции резервного копирования используется имя логического устройства, SQL Server осуществляет поиск соответствующего физического устройства в системном каталоге и выполняет резервное копирование, сохраняя резервную копию в указанной папке.

Чтобы добавить в системный каталог логическое устройство, можно использовать хранимую процедуру `sp_addumpdevice`. В следующем примере определяется логическое устройство с именем `Adv_FullDb_Dev`.

```
EXEC sp_addumpdevice 'disk', 'AdvFullDbDev', 'T:\BACKUPS\AdvFullDbDev.bak';
```

Обязательно измените, путь к файлу, чтобы он соответствовал вашему компьютеру. `T:/`, то измените эту часть пути к файлу в инструкции так, чтобы он соответствовал букве диска на вашем компьютере. Кроме того, убедитесь в том, что все папки, заданные в этом пути, существуют на вашем компьютере.

Имена логических и физических устройств являются взаимозаменяемыми, для резервного копирования и восстановления базы данных могут использоваться оба имени. Конечно, как правило, лучше все время использовать одно из двух соглашений о назначении имен, чтобы не усложнять код. Следует заранее выбрать соглашение, которое вам больше нравится.

Никогда не следует выполнять резервное копирование на дисковое устройство, которое размещается на том же физическом устройстве хранения, что и сама база данных. Даже если дисковое хранилище отличается устойчивостью против сбоев благодаря наличию RAID, всегда существует возможность возникновения неисправности контроллера и повреждения данных на дисках. Кроме того, следует подумать о сохранении файлов резервной копии устройства резервного копирования на лентах и хранении этих лент в удаленном месте.

Порядок выполнения работы

Данная лабораторная работа предполагает выполнение следующих этапов:

1. Необходимо создать резервные копии базы данных «МММ» с использованием полного резервного копирования, разностного резервного копирования и резервного копирования журнала транзакций.

Ход работы:

Запустите SQL Server Management Studio (SSMS), подключитесь к своему экземпляру SQL Server, используя технологию 1.

Создайте папку с именем c:\Student\ВашаПапка\test.

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.

Внесите изменение в таблицу «Модель» базы данных MMM. Добавьте одну запись (придумайте сами).

Откройте окно нового запроса наберите и выполните 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.

Внесите еще одно изменение в таблицу «Модель».

Откройте окно нового запроса наберите и выполните 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.

Внесите еще одно изменение в таблицу «Модель».

Откройте окно нового запроса наберите и выполните 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.

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

Ход работы:

Если необходимо, запустите SSMS, подключитесь к своему экземпляру SQL Server, используя технологию 1.

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. рис. 2.1).

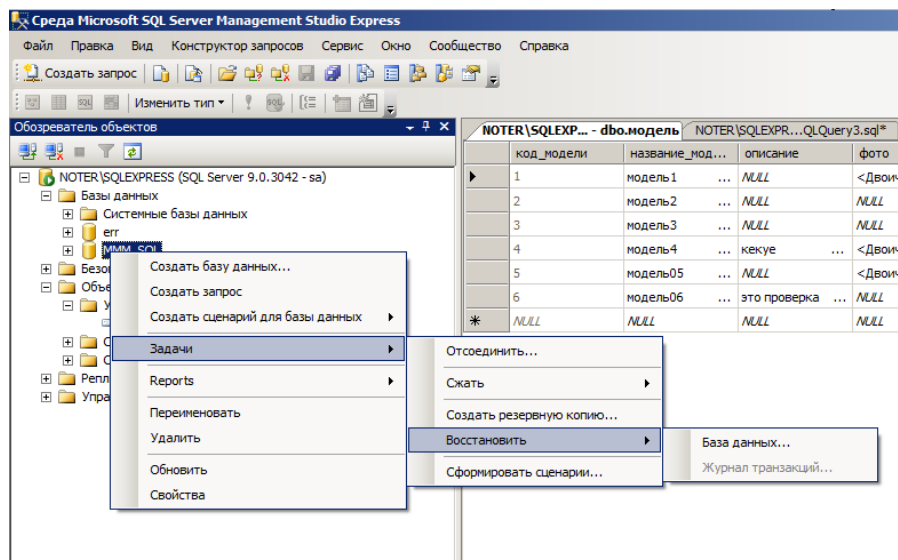


Рисунок 2.1

В открывшемся окне необходимо задать параметры восстановления.

На закладке «Общие» необходимо выбрать:

- базу данных для восстановления (вашу MMM);
- выбрать источник набора данных для восстановления с устройства файл C:\...TEST\AW.BAK.

После определения файла-источника данных необходимо флажком выбрать базу данных для восстановления (см. рис. 2.2).

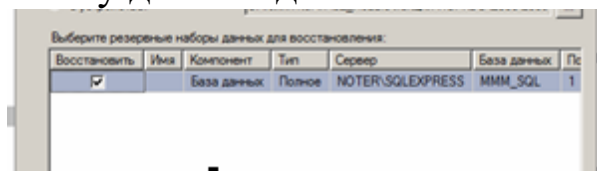


Рисунок 2.2

На закладке «Параметры» необходимо включить опцию «Перезаписать БД» и «оставить БД готовой к использованию», (см. рис. 2.3).

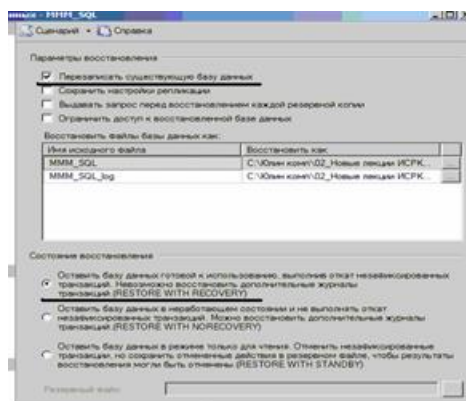


Рисунок 2.3

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).

3. Необходимо организовывать со стороны клиентского приложения, созданного в Visual Studio удаленное администрирование БД (резервное копирование).

Ход работы:

Создайте новый проект Windows Application и сохраните его в своей папке под именем Лабы_MMM_семестр.

В главную форму добавьте меню, изображенное на рисунке 2.4.

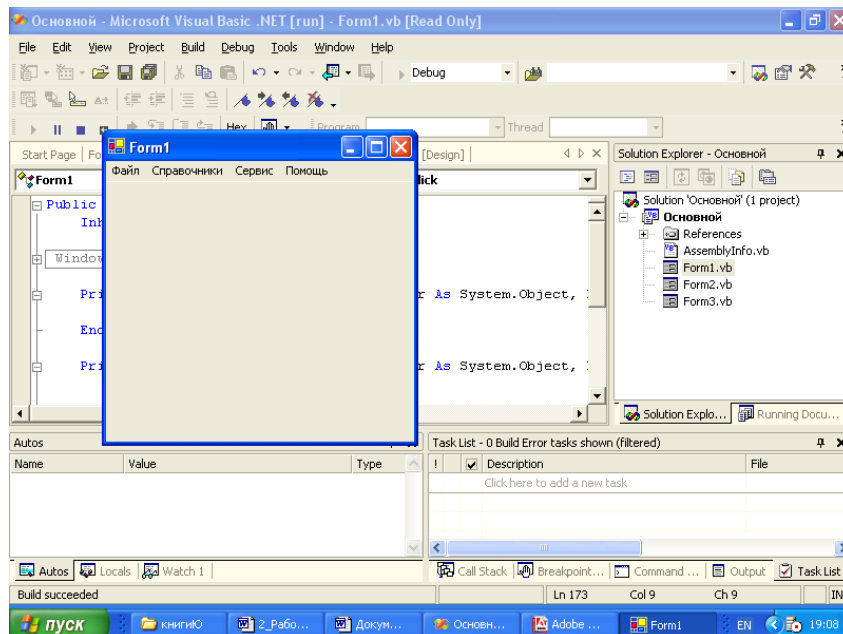


Рисунок 2.4

Добавьте на только что созданную форму компоненты в соответствии с рисунком 2.5.

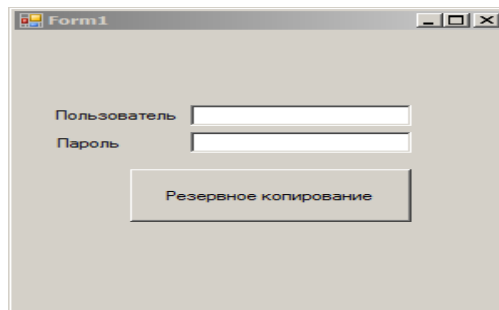


Рисунок 2.5

Обеспечьте функциональную работу формы (напишите обработчик кнопки «Резервное копирование» с использованием объектов SMO).

Добавьте возможность открытия данной формы при выборе в главной форме пункта меню Администрирование БД Резервное копирование.

Запустите проект, проверьте работу формы.

Закройте проект

Убедитесь в появлении файла резервной копии на диске (файл, который указан в тексте программы).

Откройте SSMS. Добавьте в таблицу «Модель» новую строку данных.

Средствами оболочки SSMS, выполните восстановление БД из резервной копии, созданной вашей программой

Убедитесь, что после восстановления добавленных строк в таблице «Модель» нет.

Контрольные вопросы

1. В каких случаях могут иметь место потери данных?
2. В чем заключается полное резервное копирование базы данных?
3. В чем заключается простая модель восстановления?
4. Виды устройств резервного копирования.
5. 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?
 - а) страницы данных, измененные после полуночи;
 - б) экстенды, измененные после полуночи;
 - в) страницы данных, измененные после 08:00;
 - г) экстенды, измененные после 08:00.
6. Вы выполняете полное резервное копирование базы данных AdventureWorks, 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 ми-

нут. Какую информацию будет содержать резервная копия журнала транзакций, созданная в 09:15?

- а) все транзакции, начатые после 09:10;
- б) транзакции, завершённые после 09:10;
- в) страницы, изменённые после 09:10;
- г) экстенды, изменённые после 09:10.

ЛАБОРАТОРНАЯ РАБОТА №3

ВОССТАНОВЛЕНИЕ НОСИТЕЛЕЙ ИНФОРМАЦИИ. ВОССТАНОВЛЕНИЕ УДАЛЕННЫХ ФАЙЛОВ

Цель работы – научиться осуществлять восстановление жесткого диска после сбоев.

Теоретические положения

На сегодняшний день жёсткие диски занимают доминирующее место на рынке накопителей информации. К плюсам жёстких дисков можно отнести низкую стоимость за Гбайт памяти и практичность в использовании. Поэтому возникает необходимость в своевременном обслуживании, тестировании и выявлении критического состояния жесткого диска.

В состав утилит современной операционной системы, входят программы, позволяющие осуществлять дефрагментацию и очистку жесткого диска. Для выполнения программ необходимо выполнить команду Пуск/Стандартные/Служебные и из появившегося списка программ выбрать нужную.

Кроме того, современные накопители имеют систему оперативного наблюдения за своим состоянием – S.M.A.R.T. (Self-Monitoring, Analysis And Reporting Technology) – технология самодиагностики, анализа и отчета. Это набор программ, вшитых в ПЗУ диска.

Данная технология позволяет в любое время оценить такие важные параметры накопителя, как:

- количество отработанных часов, число возникших в процессе чтения/записи ошибок, температуру накопителя
- среднюю производительность, количество циклов запуска/останова шпинделя, время раскрутки шпинделя,
- количество переназначенных секторов, количество ошибок позиционирования головок и т.д.

Технология позволяет предсказать возможный выход из строя накопителя.

Исходя из огромной важности корректной работы жесткого диска, существует большое количество программ, позволяющих восстанавливать удаленные файлы с диска, файловую систему,

критически важные структуры жесткого диска, такие как главная загрузочная запись, таблица разделов и т.д.

Partition Magic

Power Quest @ Partition Magic – это утилита, которая позволяет быстро и легко создавать, удалять, объединять или преобразовывать файловые системы и разделы на жестком диске, не уничтожая существующие данные. Новый инструмент кластерного анализа исследует FAT-дисководы и рекомендует подходящий размер кластера. Кроме того, есть возможность создавать, перемещать и изменять размер разделов типа FAT, FAT 32, файловой системы Windows NT (Windows NT File System, NTFS), HPFS (High-Performance File System – высокопроизводительная файловая система).

Partition Magic помогает надежно устанавливать и использовать несколько операционных систем на одном жестком диске. Partition Magic включает в себя Boot Magic – мощный администратор загрузки, который помогает безопасно устанавливать новые операционные системы и позволяет выбирать через меню систему при загрузке компьютера.

Программа имеет наглядный доброжелательный интерфейс.

В версии Partition Magic 8.0 включена новая утилита – Power Quest Data Keeper. Она поможет защитить ценные данные на диске от системных сбоев, упростить процесс копирования и пересылки в пределах системы, восстановить удаленный файл.

В процессе установки программы можно сделать две загрузочные дискеты – на одной будет DOS от Caldera, а на другой – Partition Magic for DOS. С помощью этих дискет можно подготовить новый диск к работе с нуля, т.к. программа наряду с организацией разделов выполняет и их форматирование, причем эти процедуры выполняются намного быстрее, чем при использовании традиционных программ.

Прежде чем начать работу с программой Partition Magic обязательно нужно выполнить следующие рекомендации:

- Установить самые последние обновления для операционных систем Windows 95/98/Me/NT Workstation/2000/XP Professional. Удостовериться, что самые последние исправления

для операционных систем Windows 95/98/Me/NT Workstation/2000/XP Professional установлены и запущены.

- Сделать копию вашего жесткого диска. Данные на диске – самая ценная часть компьютера. Хотя это и маловероятно, чтобы Partition Magic повредил бы данные, но влияние других ошибок типа системных отказов аппаратных средств, программного обеспечения, или питания, могут привести к повреждению данных в момент выполнения программы Partition Magic. Используя программу Power Quest's Drive Image, можно создать резервную копию раздела, который будет изменяться. Можно также использовать эту программу и для полного восстановления раздела к первоначальному состоянию.

- Создать загрузочный диск Windows. Загрузочный диск позволит загрузить Windows при возникновении проблемы.

- Запустить опцию проверки ошибок на диске. Для раздела, который будет проверяться, нажать Partition – Check for Errors. Небольшие ошибки могут быть исправлены Partition Magic, однако более серьезные ошибки прекратят выполнение программы. Проверить и исправить обычные ошибки на диске. Проверка загрузочного раздела операционной системы Windows невозможно, так как есть всегда открытые файлы. Для этого раздела, можно воспользоваться Partition > MS ScanDisk.

- Закрыть все запущенные приложения. Нельзя запускать Partition Magic вместе с другими приложениями, включая вирусные сканеры. Если осуществляется работа в сети под управлением Windows NT, перед выполнением Partition Magic, необходимо удостовериться что другие пользователи, не подключены к вашему компьютеру.

- Использовать UPS (Источник бесперебойного питания). Partition Magic не способна восстановить данные, если в процессе деления диска происходит сбой питания. Используя источник бесперебойного питания (UPS) можно избежать проблем, вызванных сбоем питания.

Из-за несовместимости аппаратной и системной конфигурации одного компьютера с другим, не рекомендуется переносить с одного на другой компьютер, жесткий диск, разделенный с помощью программы Partition Magic, во избежание потери данных.

Программа Partition Magic проверяет целостность диска сложной системой анализа и проверки достоверности, которая скрыто начинает свою работу, каждый раз, когда запускается программа или завершается операция. Первоначальная проверка на целостность диска, сообщает о любых проблемах связанных с разделами, которые могут препятствовать нормальной работе программы Partition Magic. Проверка целостности действует как ранняя система предупреждения, которая сообщит о том, что структура диска полностью проверена и проанализирована еще до изменения.

Если физический диск проходит первоначальную проверку целостности диска, то появляется таблица разделов, и вы можете начинать работу с программой. В случае появления сообщения об ошибке вместо таблицы разделов, указывается проблема с жестким диском, а не с программой Partition Magic (так как никакие изменения с диском еще не проводились).

Необходимо исправить проблему с жестким диском и перезапустить Partition Magic . Для получения дополнительной информации можно воспользоваться кнопкой помощи на панели инструментов.

В дополнение проверки целостности при запуске программы, Partition Magic выполняет еще две проверки в течение любой операции. До операции разделения диска проверяется файловая система (наподобие CHKDSK или MS ScanDisk) , после проверяется целостность данных. Partition Magic анализирует диск и немедленно сообщает о найденных ошибках.

Интерфейс программы Partition Magic состоит из панели действия, строки меню, инструментальной панели, карты жестких дисков, списка разделов, кнопок мастера и строки легенда. Можете показать или скрыть, а также установить размеры для различных частей интерфейса. Выполнить настройку главного окна программы любым удобным способом для различных частей интерфейса. Если выбранный жесткий диск содержит логические разделы, то они показываются внутри расширенного раздела.

Строка меню и Панель инструментов (Menu Bar and Toolbar). В главном окне программы Partition Magic, строка меню

и панель инструментов находятся наверху окна. Строка меню дает возможность доступа к любой из настроек Partition Magic, в то время как панель инструментов обеспечивает доступ к обычно используемым вариантам. Можно скрыть панель инструментов, что увеличит видимую область главного окна. Опция «Disks» на строке меню будет видна, только если у установлен второй жесткий диск.

Информация о разделах жесткого диска (Partition Information). Информационная область окна, отображает все данные для выбранного жесткого диска. Информация представлена в виде панели задач, карты диска и списка разделов.

Панель задач (Action Panel). Панель задач позволяет выбрать задачу, а также увидеть текущие незаконченные операции разделения диска.

Карта диска (Disk Map). На карте очень наглядно изображены разделы диска, с возможностью масштабировать. (Для масштабирования нажимать View – Scale Disk Map).

Каждый раздел на карте обозначается цветом (согласно легенде), которая приведена внизу окна. Освобожденное место на карте диска обозначается блоком темно – серого цвета.

Если у вас имеется второй жесткий диск то, возможно вы должны передвинуть карту что бы увидеть всю доступную информацию. Вы можете переместить карту дисков вверх или вниз, для более удобного просмотра.

Список разделов (Partition List) выводит информацию о каждом разделе на вашем жестком диске, конкретно это: имя диска, метки, тип файловой системы, размер в мегабайтах, количество используемого и неиспользуемого пространства в мегабайтах, состоянии, и является раздел первичным или логическим.

Разделы диска обозначаются названием тома, буквой с двоеточием. Звездочка заменяет букву в том случае, если раздел является:

- скрытым разделом;
- расширенным разделом;
- разделом с файловой системой, которая не поддерживается активной операционной системой;
- высвобожденным пространством.

Состояние раздела, может быть:

- **Активным (Active):** Раздел диска, с которого загружается компьютер.

- **Скрытым (Hidden):** К разделу, который не имеет букву диска, нельзя обратиться из текущей операционной системы. Разделы диска могут быть скрыты операционной системой (возможно, скрыть все первичные разделы кроме активного) или вы можете использовать Partition Magic чтобы самостоятельно скрыть нужный вам раздел. В среде Windows 2000/XP, скрытые разделы могут иметь имя.

- **Никакой (None):** Разделы, которые ни активны, ни скрыты.

Легенда (Legend) – это цветовые обозначения различных файловых систем, которые должны помочь пользователям понять цвета, которые используются в панели задач, карте диска, списка разделов. Можно скрыть строку легенды, что увеличит видимую область главного окна.

Можно выполнить задачу двумя различными способами.

Первый способ – использовать мастер программы Partition Magic из опускающего меню панели задач.

Второй способ – это сделать вручную.

Чтобы выполнить задачу вручную надо:

1. Выбрать жесткий диск или раздел.
2. Выбрать задачу (operation).
3. Применить выбранные задачи к вашей системе

Выбор жесткого диска и раздела. Можете выделить раздел сразу, не выделяя первый жесткий диск. Для этого необходимо нажать на выбранном разделе на карте диска или выбрать его из списка в главном окне. Есть две задачи, которые всегда могут быть выполнены: удалить все разделы и вывести подробную информацию о жестком диске. Когда выделяется жесткий диск, его разделы отображаются в списке разделов главного окна.

Выбор задачи (Selecting an operation). После того как были выбраны диск и раздел, используя строку меню или панель задач, выбрать операции. Есть несколько вариантов выполнения выбранной операции, для этого надо:

- В строке меню нажать Partition, затем нужную операцию. Справка советует этот метод как предпочтительный.

- На панели инструментов выбрать нужную операцию и нажать <Enter>.

- На карте диска или в списке, выбрать раздел и щелкнуть на нем правой клавишей, затем выбрать нужную операцию.

Если операция недоступна, значить она не может быть применена к данному разделу.

Partition Magic начинает выполнять немедленно операции по сбору информации, проверки на ошибки, MS ScanDisk. Остальные операции помещаются в очередь в диалоговом окне Текущие действия (Operations Pending) и ожидают нажатия кнопки Применить (Apply).

Можно в любой момент отменить последнюю операцию, которые помещаются в очередь в диалоговом окне Текущие действия (Operations Pending).

Есть несколько вариантов выполнения выбранного действия, для этого надо:

- Нажать General > Undo Last Change.
- На панели задач нажать кнопку Undo (отмена) которая находится внизу панели задач.
- Нажмите Click View > Operations Pending – Undo Last.
- На панели инструментов нажать кнопку Undo (отмена).
- Нажмите клавиши (Ctrl+Z).

Чтобы отменить все операции сразу, которые помещены в очередь в диалоговом окне Текущие действия (Operations Pending) надо:

- Нажать General – Discard All Changes.
- Нажать View – Operations Pending – Discard All.
- Нажать клавиши <Ctrl+D>.

Сделанные изменения отображаются на карте диска, в списке разделов. Однако реальные изменения будут произведены только после нажатия кнопки Apply (применить). Если кнопка на панели задач активна, а текущие операции находятся в ожидании, значит, изменения еще не были произведены.

Для применения выбранных операций надо:

- Нажать General – Apply Changes.
- Нажать кнопку Apply на панели задач главного окна программы Partition Magic.
- Нажать кнопку Apply на панели инструментов.
- Нажать клавиши <Ctrl+A>.

Индикатор движения процесса может не двигаться в течение нескольких минут.

Изменение настроек (preferences) Partition Magic:

1. Нажать General – Preferences.
2. Поставить галочку напротив надписи «Allow 64K FAT Clusters for Windows NT/2000/XP». Установка этой опции позволит создать файловую систему FAT с размером кластера равного 64К, а также позволит программе Partition Magic создавать FAT разделы размером до 4Гб. Но операционные системы Dos, Windows 3x/95/98/Me не поддерживают размеры кластеров больше 32К. Поэтому нельзя получить доступ к разделу с размером кластера 64К, используя эти операционные системы.
3. Установка галочки в маленьком окне с надписью «Skip bad sector checks» позволит пропустить проверку жесткого диска на сбойные секторы. Однако если жесткий диск имеет сбойные секторы, то возможна потеря всех данных, поэтому не рекомендуется ее включать (по умолчанию отключена).
4. Установка галочки в маленьком окне с надписью «Set as Read-Only for Partition Magic» не позволит программе произвести какие-либо изменения с жестким диском.

Если установить галочку в как шаге 2, то опция «размер кластера 64К» становится доступной в задачах Изменение/Перемещение раздела (Resize/Move Partition), и в диалоговых окнах Изменения размера кластера (Resize Clusters). Если использовать разные операционные системы, то не рекомендуется использовать кластеры размером 64К. В процессе разделения программа Partition Magic выполняет проверку на сбойные секторы. Дисковые интерфейсы IDE и SCSI устроены так, что часто обрабатывают сбойные секторы внутри, делая излишним дополнительную проверку. Partition Magic позволяет отключать проверку на сбойные секторы. Если проверка отключена, то все операции выполняются гораздо быстрее. Если установлено два диска, то

можно отключить изменение одного из них, как в шаге 4. В шаге 4 есть, исключения даже если выбрана эта опция, то некоторые загрузочные файлы Windows NT все равно могут быть изменены.

PARAGON PARTITION MANAGER

Функции программы во многом совпадают с возможностями предыдущей программы – любые разделы можно создавать, удалять, форматировать, перемещать, конвертировать между файловыми системами, объединять и изменять их атрибуты, уменьшать или увеличивать размер разделов – и все это без потери данных. Кроме того, программа от отечественных производителей. Программа способна работать практически с любыми накопителями – жесткими дисками (PATA/SATA/SCSI) с неограниченным объемом, внешними жесткими дисками (USB/FireWire), Zip, Jazz и Flash устройствами.

ACRONIS DISK DIRECTOR SUITE

Еще одна отечественная разработка. Возможности утилиты по редактированию разделов дублируют функциональность предыдущих. Дополнительно в комплект входит утилита Acronis Disk Editor, благодаря которой можно вручную редактировать огромное количество параметров жесткого диска и содержащихся на нем разделов. В частности, можно править таблицу разделов, загрузочные секторы FAT и NTFS, настройки FAT и даже все данные, хранящиеся на накопителе (в шестнадцатеричном виде).

ACRONIS RECOVERY EXPERT

Нередко проблемы потери данных выходят за рамки гибели пары файлов, порой случается и так, что бесследно исчезают и целые разделы. Список причин, в результате которых может случиться подобная неприятность, довольно обширен – простая невнимательность или неосторожность пользователя, сбой в работе жесткого диска, проказы вируса, ошибка в исполняемой программе, скачок напряжения в сети и многое другое. Помочь может эта программа. Сначала она сканирует неразмеченную об-

ласть диска на предмет нахождения пропавших разделов, затем удостоверяется у пользователя, что конкретно надо восстановить, после чего приступает к окончательной процедуре восстановления. Программа понимает большинство распространенных файловых систем. Утилита распространяется в составе предыдущей программы.

PARTITION TABLE DOCTOR

Одна из самых распространенных неприятностей – это частичное повреждение главной загрузочной записи (Master Boot Record), таблицы разделов (Partition Table) или загрузочных секторов (Boot Sectors), в результате чего система может вообще отказать запускаться. Справиться с этими проблемами, и поможет данная программа. Помимо непосредственного лечения с помощью утилиты можно сделать резервную копию таблицы разделов и загрузочных секторов. Программа может создать загрузочную дискету или CD со своим полнофункциональным модулем.

PARAGON MOUNT EVERYTHING

В последнее время все большую популярность набирают файловые системы NTFS, Ext2, Ext3. Но далеко не у всех установлены ОС, поддерживающие эти системы. Поэтому возникают проблемы совместимости при появлении в системе нового накопителя с другой файловой системой. Данная программа позволяет решить эти проблемы: моментально подключает разделы NTFS, Ext2, Ext3 в любой версии Windows, после чего работа с ними никак не будет отличаться от использования стандартных разделов FAT. Подключенным разделам присваивается буква, на них можно копировать, открывать, редактировать любые файлы и даже запускать приложения. Утилита может управлять разделами – создавать, удалять и форматировать. Можно создать загрузочную DOS дискету с возможностью доступа к NTFS.

DISK DIRECTORSUITE

Эта программа предназначена для профессиональной работы с жестким диском. Это комплексный программный пакет, который включает в себя менеджер разделов, позволяющий

осуществлять копирование, перемещение и изменение любых разделов Windows и Linux без риска потери данных, инструмент для восстановления разделов на жестком диске, а также менеджер загрузки, позволяющий установить несколько ОС на один ПК и управлять их запуском. Уже при загрузке программа производит проверку имеющихся дисков. Есть возможность запустить программу с загрузочного CD или дискеты, что позволяет восстановить разделы даже в ситуациях, когда загрузка компьютера невозможна. Программа оснащена паролем на вход и файлом помощи.

EASY RECOVERY PRO

Эта программа предназначена для восстановления утраченных или недоступных (в результате их повреждения) данных. Утилита позволяет без особого труда восстановить данные на жестком диске при утере их вследствие случайного удаления, атаки вирусов, повреждения из-за отключения или резких колебаний напряжения в электросети, ошибок в программе, проблем при создании разделов, неправильного включения ПК, повреждения структуры файловой системы. При помощи команды Drive Test можно проверить диск на наличие физических проблем.

Восстановление удаленных файлов. Общие сведения о программе Easy Recovery Pro. Easy Recovery Pro на сегодняшний день – это одна из лучших программ своего класса. Облегченный вариант – Easy Recovery Lite – входит в состав пакета комплексного обслуживания системы Fix-It Utilities.

Easy Recovery умеет работать почти со всеми более-менее распространенными файловыми системами: FAT12, FAT16, FAT32, NTFS, Novell, стандартами ZIP и JAZ-приводов, поддерживаются также и SCSI-жесткие диски. Одно из важнейших достоинств программы заключается в том, что у нее не только удобный и понятный Windows-интерфейс, доступный неопытным пользователям, но и есть возможность создать комплект загрузочных дискет с полноценной DOS-версией Easy Recovery. Сделано это для того, чтобы в случае серьезных неполадок, когда нет возможности загрузить Windows (а, соответственно, и "виндовскую" версию Easy Recovery), вас всегда был бы доступ к жест-

кому диску, и вы могли бы восстанавливать файлы непосредственно из MS-DOS. Такой режим наиболее предпочтителен при крупных сбоях – на сбойный диск ничего не записывается, Easy Recovery работает для него в режиме Read only («Только чтение»), поэтому и файлы на нем будут в большей сохранности.

Первое, что бросается в глаза сразу после запуска программы – очень долгий процесс сканирования диска. Однако это не является недостатком, а совсем наоборот – свидетельствует о ее неслабых возможностях. Дело в том, что быстрые, простые программы получают информацию об удаленных файлах и шансах на их восстановление из структуры директорий таблицы размещения файлов. Времени это, конечно, занимает очень мало, но ведь файл может еще быть на диске даже в том случае, если больше никаких его следов не осталось, да и сама таблица размещения файлов и корневая директория могут быть разрушены. Easy Recovery – она просканирует целиком весь жесткий диск, кластер за кластером, пытаясь собрать все кусочки каждого файла воедино. При этом допускается полная потеря обеих копий таблицы FAT, повреждение Root Folder и загрузочного сектора диска. Разумеется, если что-то из этого все-таки сохранилось, то будет в полной мере использовано. Кстати, если вы регулярно дефрагментируете диск, то шансы на успех еще больше увеличиваются – файл, у которого используемые кластеры идут друг за другом, восстановить проще.

Таким образом, Easy Recovery – это одна из немногих программ, которая справляется не только с восстановлением ошибочно удаленных файлов, но и восстанавливает информацию на диске после повреждения его вирусами, форматирования, переразбиения на разделы, порчи при скачках напряжения питания, сбоях аппаратного оборудования или программ.

Целесообразно сделать заранее загрузочные дискеты Easy Recovery – с ними ваши данные будут иметь как бы дополнительный "спасательный круг". Правда, поскольку Easy Recovery с поврежденным диском работает только на чтение, то придется запастись вторым винчестером или другим носителем, прежде чем приступить к восстановлению больших объемов данных.

Причем доступ к диску вы, скорее всего, получите, даже если ваша ОС его не обнаруживает.

Конечно, с DOS-вариантом программы работать сложнее, поэтому желательно предварительно изучить инструкцию, чтобы разобраться во всех многочисленных опциях Easy Recovery.

Восстановление файлов с помощью EasyRecovery Запустите EasyRecovery (Пуск – Тема – Осмотр носителя – 4 Восстановление данных – EasyRecovery Professional).

После загрузки программы на экране появляется окно, в левой части которого размещено меню в виде кнопок, обеспечивающих доступ к четырем категориям функций, а также к двум дополнительным сервисам:

- Диагностика диска – утилиты для проверки физических параметров диска и целостности файловой системы;
- Восстановление данных – утилиты для поиска и восстановления удаленных и поврежденных данных;
- Восстановление файлов – специализированные утилиты для восстановления файлов, созданных приложениями из семейства MS Office (кроме Outlook), а также ZIPархивов;
- Восстановление Email – специализированная утилита для восстановления файлов Outlook;
- Обновление программы – сервисные функции, позволяющие получать информацию и выполнять обновление лицензионной версии Easy Recovery через Интернет;
- Кризисный центр – набор функций, обеспечивающих доступ к сервисным вебслужбам компании Ontrack.

В меню выберите Восстановление данных и далее DeletedRecovery. В левой части выберите диск. Если вы удалили один или несколько файлов, быстрое сканирование должно найти эти файлы. Поиск будет производиться только в файловой системе (это должно продолжаться всего несколько секунд). В случае, когда вы удалили целые каталоги, используйте опцию полного поиска. Для этого выберите опцию Complete Scan.

Нажмите кнопку Далее, чтобы начать сканирование диска. Вы увидите окно прогресса сканирования. Processing block показан сканированный блок диска и число всех блоков до момента сканирования, Elapsed time – время, которое прошло от момента

начала сканирования, Remaining time – предполагаемое время, которое осталось до окончания операции, Directories found – количество найденных на диске каталогов, Files found – количество найденных файлов, Last file – название последнего найденного файла.

После окончания сканирования вы увидите список найденных файлов. Однако надопомнить, что не каждый найденный с помощью Easy Recovery файл возможно восстановить.

Поле Condition в списке файлов показывает в каком состоянии находится найденный файл.

Выберите файлы, которые хотите восстановить и щелкните Далее. Первый символ имени удаленного файла заменен символом подчеркивания. В следующем окне в поле Recovery Statistics находится короткая статистика о восстановленных файлах, включающая количество файлов, которые вы выбрали для восстановления, а также их полный размер. Выберите директорию, в которую их надо записать (Recover to Local Drive). Вы также можете отправить восстановленные файлы непосредственно на сервер FTP (Recover to an FTP Server). Помните, что Easy Recovery не позволит записать файлы в раздел, с которого происходит восстановление данные. Версия Professional предлагает возможность компрессии восстановленных файлов в архив ZIP (Create ZIP). На ваше усмотрение вы можете установить лимит размера файла ZIP (ZIP File Size Limit), а также создать отчет о восстановлении файлов (Generate Recovery Report). Выберите для восстановления диск C:\, нажмите Далее. В следующем окне нажмите Готово. Easy Recovery может записать установки восстановления, чтобы потом вы смогли продолжить операцию восстановления других файлов. Нажмите кнопку No. Вы восстановили данные. Просмотрите восстановленный файл.

FILE RECOVERY

Утилита предназначена для восстановления удаленных или стертых в результате форматирования жесткого диска, данных. Работает с файловыми системами FAT 12/16/32 и NTFS, а также умеет восстанавливать зашифрованные и сжатые файлы. Имеется возможность восстановления информации не только на жестком

диске, но и на съемных носителях – дискетах, картах SmartMedia, CompactFlash, Memory Stick и т.д.

RESTORER2000 Data RECOVERY

Это мощная программа, которая поможет быстро и просто восстановить нужные файлы, утерянные в результате случайного удаления, а также восстановить отформатированные или разрушенные диски. Утилита поддерживает возможность создания образа диска, это очень полезно для таких задач, как восстановление жесткого диска с большим количеством неработоспособных секторов. Можно установить размер сканируемой области, в зависимости от этого будет меняться время выполнения, которое программа автоматически подсчитывает.

HDD Temperature Pro

Это очень маленькая утилита, предназначена для отслеживания состояния жестких дисков. Используя технологию SMART, встроенную во все современные жесткие диски, она анализирует и показывает текущую температуру диска. Здесь возможна установка максимальной температуры накопителя, при превышении которой программа выдаст сообщение. Можно сделать так, чтобы эта утилита самостоятельно загружалась при входе в ОС, так что она будет незаметна, но в нужный момент предупредит о возможной опасности перегрева диска.

TREESIZE

Эта утилита предназначена для мониторинга пространства на жестком диске и его освобождения. Она умет искать старые и неиспользуемые, а также временные файлы и удаляет их. С помощью этой утилиты можно найти папки, которые занимают больше всего места на диске, сравнить их объем в процентном соотношении в виде графика. Примерно такие же возможности имеют программы: FCLEANER, FREESPACE.

Порядок выполнения работы

Данная лабораторная работа предполагает выполнение следующих этапов:

- изучить методические указания;
- ответить на контрольные вопросы.

Контрольные вопросы

1. В чем назначение программы Partition Magic?
2. Какие действия необходимо выполнить перед началом работы с программой Partition Magic?
3. Как осуществляется проверка целостности жесткого диска с помощью программы Partition Magic?
4. Назначение программы Paragon Partition Manager?
5. Перечислите известные вам программы по обслуживанию жестких дисков в процессе их эксплуатации и определите их назначение.
6. Опишите последовательность восстановления удаленной информации, если: файл удален в корзину; файл удален в корзину и затем корзина была очищена.

ЛАБОРАТОРНАЯ РАБОТА №4 МОНИТОРИНГ АКТИВНОСТИ И БЛОКИРОВАНИЕ ПОРТОВ

Цель работы – формирование умений и навыков блокировки и разблокировки портов подключения устройств.

Теоретические 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 разъемы, которые портами называть не принято, например, RJ11.

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 конечного 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, требуют дополнительного источника питания – это могут быть как разъемы 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 разъемы 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 разъемы 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.

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 актуальней 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.

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 видеорекамеры.

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

Activity Monitor мощный инструмент, который 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.

Net Vizer

Net Vizer – программа для мониторинга сети. Net Vizer позволяет наблюдать за всей локальной сетью из одного рабочего места. Программа может следить за рабочими станциями и индивидуальными пользователями, которые используют различные компьютеры, находящиеся 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. Net Vizor также обезвреживает шпионские программы и помогает следить за безопасностью.

Сравнительный анализ программ приведен в таблицах 4.1 – 4.5.

Таблица 4.1 – Мониторинг

Наименование	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	+	+	+	+

Таблица 4.2 – Контроль

Наименование	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	—	+	+	+

Таблица 4.3 – Отчетность

Наименование	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	+	+	+	+

Продолжение таблицы 4.3

Наименование	Spector 360	Security Curator	Activity Monitor	Net Visor
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	+	+	—	-

Таблица 4.4 – Управление

Наименование	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	+	—	-	+

Продолжение таблицы 4.4

Наименование	Spector 360	Security Curator	Activity Monitor	Net Visor
Разделение доступа к функциям администрирования	+	—	-	+
Возможность группировки компьютеров	+	+	+	+
Возможность группировки пользователей	+	—	+	-

Таблица 4.5 – Безопасность

Наименование	Spector 360	Security Curator	Activity Monitor	Net Visor
Контроль компьютеров в сети	+	+	+	+
Удаленная установка	+	+	+	+
Невидимый режим работы	+	+	—	+
Авторизация при запуске административного модуля	+	+	+	+

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, Net Visor 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 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.

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

Пользователя Администратор заменим на Admin.

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

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.

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.

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

Выполним команду Панель управления – Администрирование – Локальные политики безопасности – Локальные политики – Параметры безопасности – Интерактивный вход: не отображать

последнего имени пользователя. Эту запись необходимо включить.

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

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 на 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, ра-

ботающих 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.

Обнаружение открытых на ПК портов утилитой `Netstat`.

Для выполнения лабораторной работы на компьютере необходимо открыть командную строку.

Чтобы вывести все активные подключения TCP и прослушиваемые компьютером порты TCP/ UDP введите команду `netstat`. 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.

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

Опции команды netstat приведены в таблице 4.6.

Таблица 4.6 – 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 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 объемом переданной информации с момента последней перезагрузки системы
-p	Отобразить идентификатор/название процесса создавшего сокет (-p, –programs display PID/Program name for sockets)

NetStat Agent

С помощью программы NetStat Agent 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 DNS-настройки адаптера, просматривать сетевую статистику для адаптеров и TCP/IP протоколов, а также строить графики для команд Ping и TraceRoute.

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) – популярный сканер портов, который обследует сеть и проводит аудит защиты. Сканером пор-

тов Nmap можно определить открытые порты компьютера, а для безопасности сети пользователям рекомендуется закрыть доступ к этим портам с помощью брандмауэра.

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 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.

Порядок выполнения работы

Данная лабораторная работа предполагает выполнение следующих этапов:

- изучить методические указания;
- ответить на контрольные вопросы.

Контрольные вопросы

1. Какие виды мониторинга рабочих операций пользователей существуют?
2. Дайте характеристику современных программных средств мониторинга действий пользователей.
3. Какое программное средство вы порекомендовали? Почему?
4. Какие уязвимости операционной системы Windows были устранены в данной работе и какими путями?
5. Как узнать закрытые порты?
6. Как открыть нужный порт?
7. Для чего используется программа NetStat Agent?
8. Для чего используется программа Nmap?
9. Для чего используется программа TCPView?

ЛАБОРАТОРНАЯ РАБОТА №5 ПРОВЕРКА НАЛИЧИЯ И СРОКОВ ДЕЙСТВИЯ СЕРТИФИКАТОВ

Цель работы – познакомимся с вопросами использования цифровых сертификатов.

Теоретические положения

Начнем с использования сертификатов протоколами SSL и TLS (это два разных протокола, но т.к. TLS разработан на базе SSL 3.0, принцип использования сертификатов один и тот же).

Эти протоколы широко применяются в сети Интернет для защиты данных передаваемых между web-серверами и браузером клиента. Для аутентификации сервера в нем используется сертификат X.509.

Для примера обратимся на сайт «Нордеа Банка», в раздел «Войти в Интернет-банк», предназначенный для ведения банковских операций через Интернет (см.рис. 5.1).

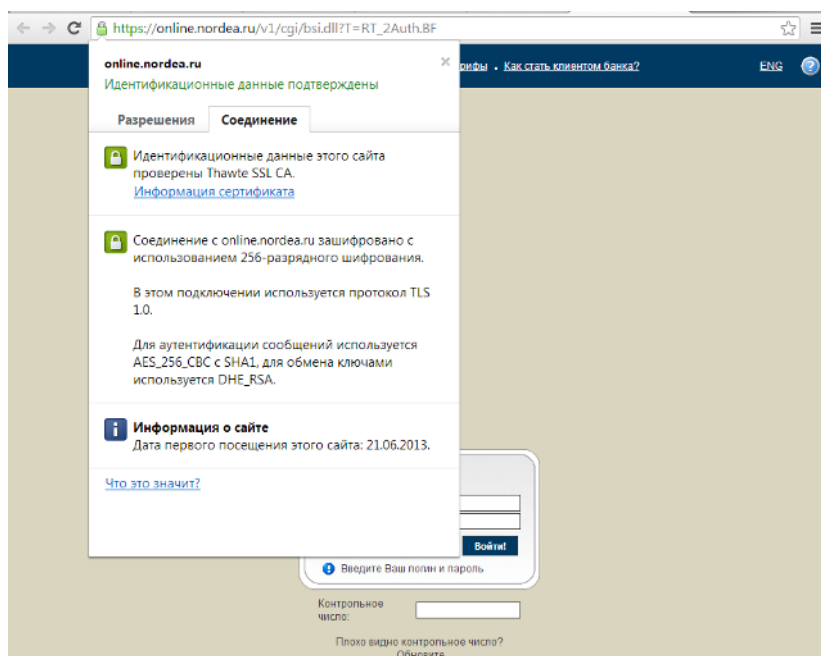


Рисунок 5.1 – Защищенное соединение

Префикс https в строке адреса и изображение закрытого замка справа от строки указывают, что установлено защищенное

соединение. Если щелкнуть мышью по изображению замка, то увидим представленное на рисунке 5.1 сообщение о том, что подлинность узла с помощью сертификата подтверждает центр сертификации Thawte. Значит, мы на самом деле обратились на сайт Нордея Банка (а не подделанный нарушителями сайт) и можем безопасно вводить логин и пароль.

Выбрав «Просмотр сертификата» можно узнать подробности о получателе и издателе, другие параметры сертификата (см. рис. 5.2).

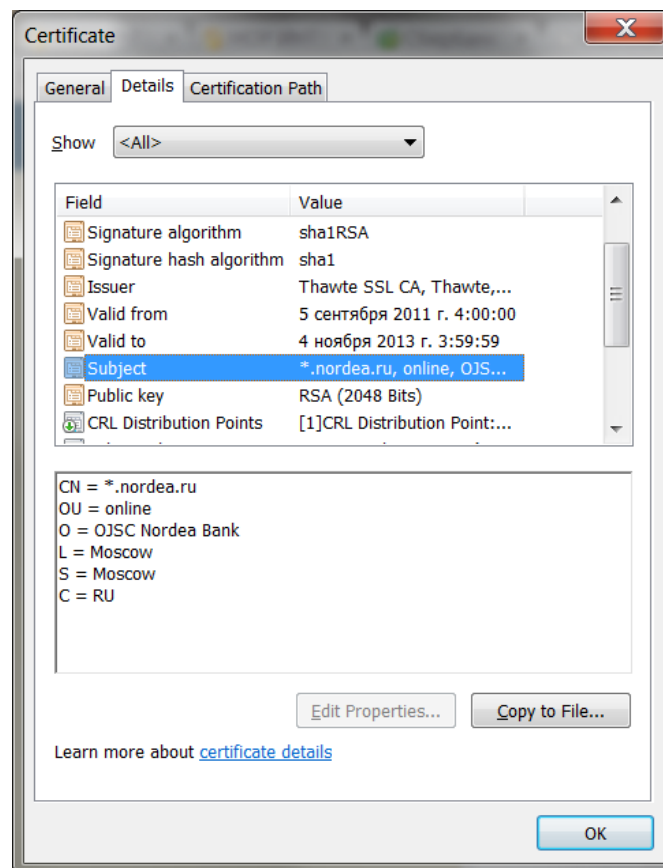


Рисунок 5.2 – Параметры сертификата

Операционная система Windows обеспечивает защищенное хранилище ключей и сертификатов. Работать с хранилищем можно используя настройку консоль управления MMC «Сертификаты».

Из меню Пуск – Выполнить (или «Командная строка») запустите консоль командой mmc.

Таким образом, мы можем просматривать сертификаты текущего пользователя. Если ранее сертификаты не запрашивались, то в разделе «Личное» элементов не будет.

В разделе «Доверенные корневые центры сертификации» представлен достаточно обширный список центров, чьи сертификаты поставляются вместе с операционной системой.

Найдите в нем сертификат thawte Timestamping CA. Благодаря тому, что он уже был установлен, в рассмотренном в начале работы примере с подключением к системам Интернет-банкинга браузер мог подтвердить подлинность узла.

Теперь перейдем к разделу «Сертификаты, к которым нет доверия». Там находятся отозванные сертификаты. Как минимум, там будут находиться два сертификата, которые по ошибке или злему умыслу кто-то получил от имени корпорации Microsoft. Когда это выяснилось, сертификаты отозвали. Сейчас этот список намного больше.

Теперь рассмотрим другой вариант – мы подключаемся по SSL к web-серверу, а браузер не может проверить его подлинность. Подобная ситуация произошла при подключении в раздел Интернет-обслуживания Санкт-Петербургского филиала оператора мобильной связи Tele2 -[https:// www.selfcare.tele2.ru/work.html](https://www.selfcare.tele2.ru/work.html) (см. рис. 5.3).

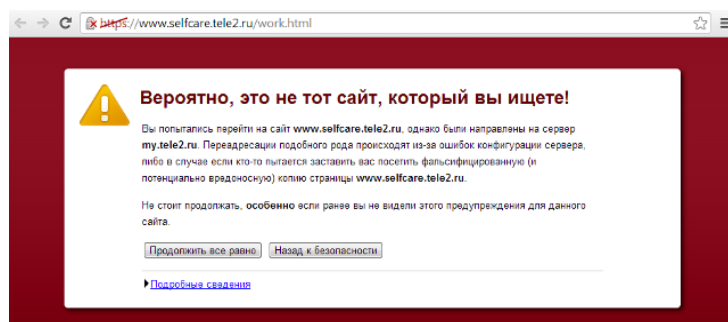


Рисунок 5.3 – Сообщение о проблеме с сертификатом

Если нажать ссылку «Продолжить всё равно» можно будет просмотреть сертификат.

Рассмотрим возможности, которые предоставляет Windows Server по созданию собственно центра сертификации (Certification Authority – CA) на предприятии.

Соответствующие службы присутствовали в серверных операционных системах семейства Windows, начиная с Windows 2000 Server.

В Windows Server 2012 для того, чтобы сервер смог работать как центр сертификации, требуется сначала добавить серверу роль Службы сертификатов Active Directory. Делается это помощью оснастки Диспетчер серверов (см. рис. 5.4), которую можно запустить из меню Пуск.

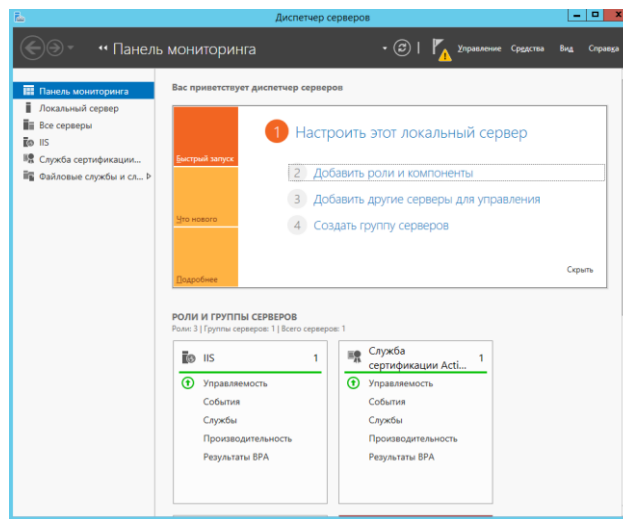


Рисунок 5.4 – Диспетчер серверов

В Server Manager раскроем список ролей и выберем добавление роли (см. рис. 5.5) – Служба сертификатов Active Directory.

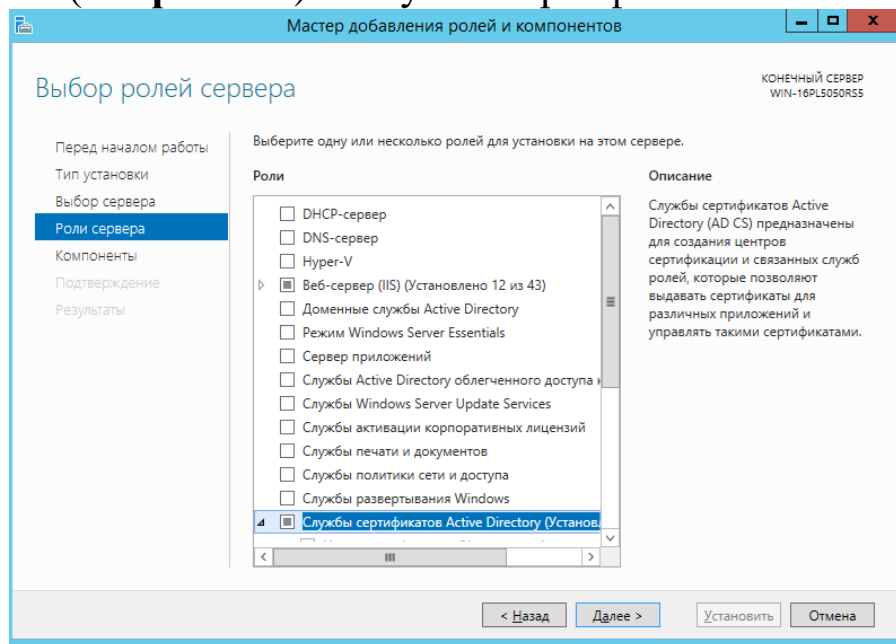


Рисунок 5.5 – Добавление роли

В нашем примере, роль добавляется серверу, который будет также контроллером домена Windows. Так как это первый СА в домене, он в нашей сети будет играть роль корневого (Root).

Контроллер домена в данной работе настраивать не требуется.

Рассмотрим по шагам процедуру установки.

В дополнение к обязательному компоненту «Служба сертификатов Active Directory», могут быть установлены дополнительные средства, предоставляющие web-интерфейс для работы пользователей с СА (см. рис. 5.6). Это может понадобиться, например, для выдачи сертификатов удаленным или внешним, не зарегистрированным в домене, пользователям. Для выполнения данной лабораторной работы это не понадобится.

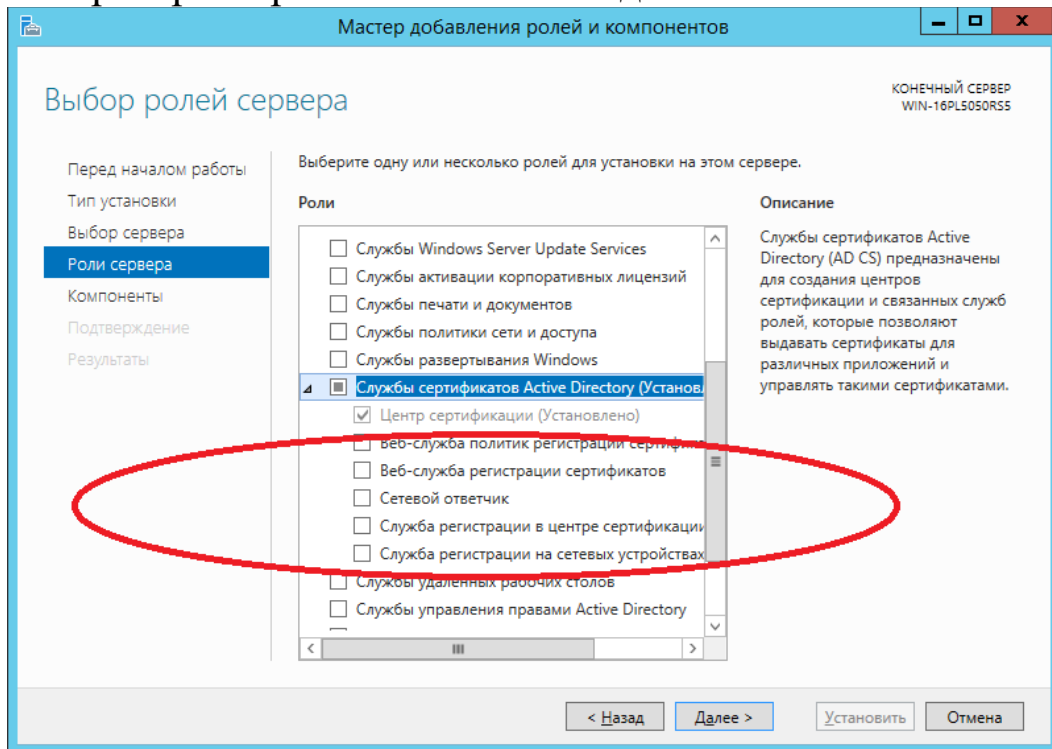


Рисунок. 5.6 – Выбор добавляемой роли

Следующий шаг – определения типа центра сертификации. Он может быть корпоративным (Enterprise) или отдельностоящим (Standalone). Разница заключается в том, что Enterprise СА может быть установлен только на сервер, являющийся членом домена, т.к. для его работы требуется служба каталога Active Directory.

Standalone CA может работать вне домена, например, обрабатывая запросы пользователей, полученные через web-интерфейс.

Порядок выполнения работы

Данная лабораторная работа предполагает выполнение следующих этапов:

- изучить методические указания;
- ответить на контрольные вопросы.

Контрольные вопросы

1. Какие протоколы применяются для за
2. щиты данных?
3. Типы центров сертификации.
4. Алгоритм создания центра сертификации.
5. Как осуществляется работа с хранилищем сертификатов?
6. Как можно узнать подробности о получателе и издателе, другие параметры сертификата?

ЛАБОРАТОРНАЯ РАБОТА №6 РАЗРАБОТКА ПОЛИТИКИ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ

Цель работы – получить навыки использования системы защиты информации в корпоративной сети.

Теоретические положения

Информация о пользователе информационной системы должна содержать следующее:

- имя пользователя;
- сведения о парольной защите;
- тип учетной записи.

Кроме того, в этом окне возможна настройка подсказки о пароле и мастера забытых паролей, позволяющих выполнять сброс и изменение забытого пароля, а также пароль доступа к сетевым ресурсам (для администратора).

Чтобы удалить зарегистрированного пользователя, необходимо выполнить следующее:

- выбрать имя нужного пользователя в списке;
- выбрать пункт «Удаление учетной записи».

Для того чтобы зарегистрировать нового пользователя в системе, необходимо произвести следующие действия:

- находясь в меню «Учетные записи пользователей» выбрать пункт «Создание учетной записи»;
- ввести с клавиатуры имя нового пользователя, например «Начальник»;
- выбрать тип учетной записи;
- если необходимо, установить и подтвердить пароль.

Чтобы изменить информацию о пользователе, нужно выполнить следующие действия:

- выбрать имя нужного пользователя в списке;
- изменить нужные параметры.

Управление учетными записями может выполняться в двух режимах: классического запроса пароля и приглашения, когда вход в систему выполняется простым кликом мышью на иконке

пользователя. Изменение параметров входа доступно в меню «Учетные записи пользователей».

Настройка элементов политики безопасности.

В операционной системе имеется возможность настройки элементов политики безопасности, регулирующей доступ к файлам и папкам.

Единственным условием является наличие версии Professional и файловой системы NTFS. Настройка производится пользовательским интерфейсом, доступ к которому открыт администратору системы.

Для того, чтобы использовать его, следует открыть «Пуск/Панель управления/Администрирование/Локальная политика безопасности/Параметры безопасности/Политика учетных записей/Политика паролей/».

Рассмотрим основные параметры, необходимые для выполнения лабораторной работы.

Максимальный срок действия пароля.

Этот параметр безопасности определяет период времени (в днях), в течение которого можно использовать пароль, прежде чем система потребует от пользователя заменить его. Срок действия пароля может быть установлен в пределах от 1 до 999 дней. При установке значения 0 срок действия пароля не ограничен. Если максимальный срок действия пароля составляет 1 – 999 дней, значение параметра «Минимальный срок действия пароля» должно быть меньше этого значения. При установке значения 0 для максимального срока действия пароля для минимального срока действия может быть установлено любое значение в пределах от 0 до 998 дней.

Минимальная длина пароля.

Этот параметр безопасности определяет наименьшее число символов, которое может содержать пароль учетной записи пользователя. Можно задать значение в диапазоне от 1 до 14 символов или отменить использование пароля, установив число символов равным 0.

Минимальный срок действия пароля.

Этот параметр безопасности определяет период времени (в днях), в течение которого необходимо использовать пароль, прежде чем пользователь сможет заменить его. Можно задать значение в диапазоне от 1 до 998 дней или разрешить немедленное изменение, установив число дней равным 0.

Пароль должен отвечать требованиям сложности.

Этот параметр безопасности определяет требования сложности для паролей.

Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям:

- 1) пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
- 2) пароль должен состоять не менее чем из шести символов;
- 3) в пароле должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- десятичные цифры (от 0 до 9);
- неалфавитные символы (например: !, \$, #, %).

Проверка соблюдения этих требований выполняется при изменении или создании паролей.

Требование неповторяемости паролей.

Этот параметр безопасности определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Это значение должно принадлежать диапазону от 0 до 24.

Данная политика позволяет администраторам повышать уровень безопасности, запрещая все время использовать одни и те же старые пароли.

Хранение паролей с использованием обратимого шифрования.

Этот параметр безопасности определяет, использует ли операционная система обратимое шифрование для хранения паролей. Такая политика обеспечивает поддержку приложений, ис-

пользующих протоколы, которым для проверки подлинности нужно знать пароль пользователя. Хранить пароли, зашифрованные обратимыми методами, – это все равно, что хранить их открытым текстом. Поэтому данную политику следует использовать лишь в исключительных случаях, если потребности приложения оказываются важнее, чем защита пароля.

Блокировка учетных записей.

В системе существует возможность блокировки учетных записей. Задать условия блокировки можно, открыв интерфейс настройки: «Параметры безопасности/Политика учетных записей/Политика блокировки учетных записей/».

Рассмотрим параметры настройки.

Блокировка учетных записей. Этот параметр безопасности определяет число минут, в течение которых учетная запись остается заблокированной, прежде чем будет автоматически разблокирована. Этот параметр может принимать значения от 0 до 99 999 мин. Если установлено значение 0 для длительности блокировки учетной записи, она останется заблокированной до тех пор, пока не будет явно разблокирована администратором.

Если пороговое значение блокировки определено, данный интервал блокировки должен быть больше или равен интервалу сброса.

Пороговое значение блокировки.

Этот параметр определяет число неудачных попыток входа в систему, после которых учетная запись пользователя блокируется. Блокированную учетную запись нельзя использовать до тех пор, пока она не будет инициализирована администратором или пока не истечет интервал ее блокировки. Число неудачных попыток входа в систему можно задать в интервале от 0 до 999. При установке значения 0 учетная запись пользователя никогда не будет блокироваться.

Сброс счетчика блокировки.

Параметр определяет, сколько минут должно пройти после неудачной попытки входа в систему, прежде чем счетчик неудач-

ных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99 999 мин.

Аудит (регистрация и учет событий).

Важным компонентом системы защиты является система регистрации и учета, реализующая фиксирование событий доступа, в том числе несанкционированного.

Получить доступ к этим настройкам можно следующим образом: «Параметры безопасности/Локальные политики/Политика аудита/».

Рассмотрим их более подробно.

Аудит входа в систему. Позволяет контролировать корректность доступа пользователя в систему, в частности, количество неудачных попыток входа.

Аудит доступа к объектам. Этот параметр безопасности определяет, подлежит ли аудиту событие доступа пользователя к объекту – например, к файлу, папке, разделу реестра, принтеру и т. п., – для которого задана собственная системная таблица управления доступом (SACL).

Аудит доступа к службе каталогов. Определяет, подлежит ли аудиту событие доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом (SACL).

Аудит изменения политики. Этот параметр определяет, подлежит ли аудиту каждый факт изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

Аудит использования привилегий. Определяет, подлежит ли аудиту каждая попытка пользователя воспользоваться предоставленным ему правом.

Аудит отслеживания процессов. Определяет, подлежат ли аудиту такие события, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту.

Аудит системных событий. Определяет, подлежат ли аудиту события перезагрузки или отключения компьютера, а также со-

бытия, влияющие на системную безопасность или на журнал безопасности.

Аудит событий входа в систему. Определяет возможность отслеживания доступа пользователей.

Аудит управления учетными записями. Этот параметр безопасности определяет, подлежат ли аудиту все события, связанные с управлением учетными записями на компьютере.

Кроме того, возможна и настройка прав доступа пользователя с помощью отдельного инструмента политики безопасности, но настройка этих элементов в рамках работы не выполняется.

Контроль запуска программ.

Операционная система Windows XP SP2 позволяет управлять доступом к файлам, запускающим приложения. Получить доступ к этим настройкам можно следующим путем: «Параметры безопасности/Локальные политики/Политика ограниченного использования программ/». По умолчанию таких политик не существует, поэтому необходимо создать собственную в меню «Действие». Рассмотрим параметры ее настройки. Уровни безопасности. Позволяет контролировать программы исходя из запрета или полного доступа к отдельной области.

Дополнительные правила.

Этот параметр безопасности определяет, заданы ли пользователем дополнительные параметры безопасности. Для выполнения лабораторной работы необходимо создать правило для пути в меню «Действие».

Контроль доступа к файлам и папкам.

Позволяет контролировать доступ к файлам и папкам каждому пользователю, зарегистрированному в системе. Для доступности такой функции необходима система версии Professional и файловая система NTFS. При соблюдении этого условия также проконтролируйте снятие флажка «Простой общий доступ к файлам и папкам», доступ к которому можно получить следующим образом: «Панель управления/Свойства папки/Вид».

Для настройки прав доступа пользователя к файлу или папке при выполненных условиях необходимо выполнить следующие действия:

- открыть вкладку «Безопасность» в свойствах файла или папки;
- перейти по кнопке «Дополнительно» в меню настройки;
- добавить или изменить запреты и разрешения с помощью кнопки «Изменить»;
- добавить или изменить правила аудита с помощью вкладки «Аудит».

Если пользователь отсутствует в списке, необходимо добавить его, используя следующую последовательность действий «Безопасность/Добавить/Дополнительно/Поиск» и выбрать из списка внизу нужного пользователя.

Можно заблокировать изменение настроек, включив флажок «Использовать простой общий доступ к файлам и папкам».

Система контроля доступа может применяться для задач блокирования, но она не предполагает установки парольной защиты на файлах и папках. Для этих целей используются дополнительные средства защиты информации.

Порядок выполнения работы

Создайте политику безопасности операционной системы для трех пользователей с заданными правами использования файлов и папок при данных условиях:

Администратор компьютера имеет доступ ко всем папкам пользователей на чтение, но не имеет право удалять или изменять файлы. Папка администратора C:\Admin. Бухгалтер – пользователь, имеет право записи и чтения в своей папке C:\bukh, не имеет доступа к папкам администратора, имеет доступ на запись к папке пользователя Начальник. Начальник – пользователь, имеет право записи и чтения в своей папке C:\chief, не имеет доступа к папкам администратора, имеет доступ на чтение к папке пользователя

Бухгалтер. Все нарушения системы защиты записываются в журнал безопасности системы.

Установите следующие настройки: количество циклов затирания (3), ограничения по паролю пользователей (минимальная длина – 6 символов, требования к сложности, требования к неповторяемости, время действия – 45 дней), максимальное число попыток входа – 5, аудит событий НСД (контролируется в журнале «Безопасность», находящемся «Панель управления /Администрирование/ Просмотр событий»), невозможность запуска программ из папки пользователя.

В каждой папке должны быть два файла, содержащие текстовую информацию, и один файл программы (с расширением .exe).

Контрольные вопросы

1. В чем заключается сущность принципов функционирования механизма контроля доступа?
2. Как реализовано управление пользователями?
3. Как выполняется блокировка и разблокировка пользователя?
4. В чем заключаются функции персонального идентификатора?
5. В чем заключается сущность принципов функционирования системы аудита безопасности?
6. Какие существуют правила настройки и условия работы системы контроля доступа к файлам и папкам?

ЛАБОРАТОРНАЯ РАБОТА №7 ПОЛУЧЕНИЕ СЕРТИФИКАТА

Цель работы – изучить цели, задачи и методологические проблемы обеспечения качества информационных технологий (ИТ), программных средств (ПС) и баз данных (БД) при сертификационных испытаниях.

Теоретические положения

Основные понятия и цели сертификации информационных технологий, программных средств и баз данных

Эффективность использования информационных технологий (ИТ) во многом определяется их качеством и доверием к ним пользователей. Возрастание роли важнейших компонент ИТ программных средств (ПС) и баз данных (БД) в народном хозяйстве, широты их применения и ответственности решаемых задач вызвало резкое повышение требований к их качеству.

По мере расширения применения ИТ выделились области, в которых ошибки или недостаточное качество программ может нанести ущерб, значительно превышающий положительный эффект от их использования. В таких критических случаях недопустимы аномалии функционирования программ при любых искажениях исходных данных, сбоях, частичных отказах аппаратуры и других нештатных ситуациях. Для этого испытания ИТ должны специально организовываться и документироваться, что объединяется понятием и процессом сертификации.

Архитектурная, техническая и программно-информационная совместимость современных сложных информационных систем (ИС) может быть обеспечена только путем стандартизации программно-технических средств в соответствии с требованиями международных стандартов. Для этого также необходима сертификация используемых средств, процессов и услуг, а также проведение единой технической политики при создании совместимых аппаратных средств и ПС, организации взаимодействия и комплексирования ИС различных уровней.

Сертификация соответствия ИТ, ПС и БД заключается в их формализованных испытаниях особо выделенным третейским коллективом специалистов, имеющим право на официальный государственный или ведомственный контроль функций и качества ИТ и гарантирующим их соответствие стандартам и другим нормативным документам, а также безопасность применения. Эти специалисты имеют право на расширение условий испытаний и создание различных критических и стрессовых ситуаций в пределах нормативной документации, при которых должны обеспечиваться заданное качество и безопасность результатов решения предписанных задач.

Если все испытания проходят успешно, то на соответствующую версию ИТ, ПС и БД оформляется и выдается специальный документ сертификат соответствия. Этот документ официально подтверждает соответствие стандартам, нормативным и эксплуатационным документам функций и характеристик испытанных средств, а также допустимость их применения в определенной области. Сертификат соответствия документально утверждает право на использование знаков соответствия требованиям сертификации, гарантирует безопасность применения, а также юридически допускает ИТ к эксплуатации и использованию по прямому назначению.

В зависимости от области применения ИТ, назначения и класса ПС и БД их сертификация может быть обязательной или добровольной. Эти виды сертификации близки концептуально и технологически, однако значительно различаются характеристиками объектов, правовым и экономическим взаимодействием между поставщиками, испытателями и пользователями.

Обязательная сертификация

Обязательная (жесткая) сертификация ИТ необходима для ИС, выполняющих особо ответственные функции, в которых недостаточное качество, ошибки или отказы могут нанести большой ущерб или опасны для жизни и здоровья людей. Этот ущерб может определяться степенью безопасности применения ИТ в авиации, для управления в космосе и атомной энергетике или большими экономическими потерями вследствие недопустимого

искажения служебной информации в системах управления органов власти, банковских системах, системах управления войсками и др. В подобных системах сертификация ИТ способствует значительному снижению риска от их применения и повышению безопасности функционирования до необходимого уровня. В этих случаях разработчики и поставщики ИТ обязаны подвергать свои изделия независимой экспертизе на соответствие стандартам и конкретным требованиям качества для получения разрешения сертификационных центров на их реальную эксплуатацию по прямому назначению.

Добровольная сертификация

Добровольная (мягкая) сертификация применяется для удостоверения качества ИТ в целях повышения их конкурентоспособности, расширения сферы использования и получения дополнительных экономических преимуществ на рынке. Таким сертификационным испытаниям подвергаются компоненты операционных систем и пакеты прикладных программ широкого применения, повышение гарантий качества которых выгодно как для поставщиков, так и для пользователей ИТ. Затраты на сертификацию ИТ оправдываются повышением их цены, сокращением претензий пользователей, ростом тиража продаж и др. В этих случаях разработчики и поставщики добровольно предоставляют ИТ для сертификации с учетом экономических оценок выгоды ее проведения для их изделий.

При анализе процессов сертификационных испытаний ИТ, ПС и БД следует выделить **ряд базовых компонент методологии** сертификации, подлежащих последующему рассмотрению:

- цели сертификации формальные, технологические, правовые, экономические;
- проблемы, которые необходимо решать для обеспечения высокой эффективности и достоверности результатов сертификационных испытаний ИТ, ПС и БД;
- исходные данные и документы, необходимые для проведения сертификации стандарты и нормативные документы, их структура и содержание;

- характеристики и классификация программ и БД как объектов испытаний и сертификации, их показатели качества, позволяющие выделять однородные группы ПС и БД при проведении сертификации;

- ресурсы обеспечения испытаний финансовые, кадры специалистов, аппаратурная оснащенность, нормативно-технические и программно-инструментальные средства.

Проблемы сертификации ИТ, ПС и БД в принципе близки к тем, которые приходится решать для других видов изделий. Однако вследствие их новизны, высокой сложности объектов сертификации и многообразия их показателей качества выявился ряд особенностей этих проблем.

При анализе сертификации ИТ, ПС и БД целесообразно выделить следующие проблемы:

- научно-методические, состоящие в создании эффективных по затратам ресурсов методов сертификационных испытаний ИТ, ПС и БД, которые гарантируют достоверное определение заданных показателей их качества и соответствие документации;

- технологические, заключающиеся в обеспечении реализации методов испытаний ИТ средствами автоматизации, тестирования и организации регламентированных проверок качества объектов и документации на разных этапах их создания и при непосредственных сертификационных испытаниях;

- проблемы стандартизации и нормативной документации, которые сводятся к созданию, последующему выбору и адаптации исходных документов, применяемых при сертификационных испытаниях определенных видов ИТ, ПС и БД;

- организационные, состоящие в создании международных, государственных и ведомственных органов, ответственных за сертификацию ИТ и их компонент, определении их прав и обязанностей, оснащении их необходимыми нормативно-методическими и инструментально-технологическими средствами;

- экономические, которые сводятся к выявлению, оценке и применению экономически эффективных методов использования ресурсов испытаний ИТ, ПС и БД, обеспечивающих задан-

ную достоверность определения их качества, разработке экономических механизмов взаимодействия организаций и специалистов по сертификации с разработчиками, заказчиками и пользователями этих средств;

— правовые, сосредоточивающие в себе прежде всего создание юридических механизмов процессов сертификации и использования их результатов, создание нормативов, правил взаимодействия и распределения экономической и юридической ответственности между разработчиками, производителями, сертифицирующими организациями и поставщиками ИТ, ПС и БД за несоответствие реальных показателей качества гарантированным характеристикам сертифицированных изделий.

Ниже рассматриваются проблемы, которые наиболее близки к процессам непосредственных испытаний и определению качества ИТ, ПС и БД. Это методические, технологические, организационные проблемы, а также проблемы стандартизации и нормативной документации. Им сопутствуют задачи распределения экономической и юридической ответственности между испытателями, разработчиками, поставщиками и заказчиками за качество сертифицированной продукции и возможный ущерб при ее несоответствии документированному и объявленному качеству. Экономическими целями сертификации могут быть большие тиражи изделий при производстве, большая длительность жизненного цикла с множеством версий, снижение налогов за высокое качество и высокая прибыль разработчиков и поставщиков ИТ, ПС и БД. Результаты сертификации должны оправдывать затраты на ее проведение вследствие получения пользователями продукции более высокого и гарантированного качества при возможном повышении ее стоимости. Юридические проблемы сертификации и распределения ответственности за соответствие продукции, купленной пользователем, гарантиям, закрепленным сертификатом соответствия, должны решаться правоведами. При их решении необходимо отработать юридические механизмы распределения прибыли и затрат за обеспечение качества ИТ и нарушение их гарантированных значений.

Методически процесс сертификации представляет особую совокупность испытаний ИТ и их компонент, для которых необ-

ходимы специальные стандарты, методики, средства автоматизации и подготовленные специалисты. Далее отдельно рассматриваются особенности сертификации основных компонент ИТ ПС и БД. При этом в большинстве случаев, если это не может вызвать сомнений, подразумеваются и ИТ, которые они обеспечивают.

Работы по сертификации ПС объединяются в технологический процесс, на каждом этапе которого регистрируются документы, отражающие состояние и качество результатов контроля программ. В результате процесс сертификации отличается от обычных испытаний ПС более высоким уровнем формализации и документального оформления всех условий и результатов испытаний, проводимых специальным испытательным органом.

Необходимость сертификации программ широкого класса привела к появлению **ряда следующих научных и методических задач**, тесно связанных с процессами разработки ПС высокого качества:

- для каждого вида ПС необходимо определять представительный набор характеристик качества и их значений, его категорию критичности, требуемую достоверность измерения показателей качества и организационный уровень удостоверения сертификата;
- в соответствии с требованиями к достоверности показателей качества должны определяться и минимизироваться содержание и объемы сертификационных испытаний версий ПС;
- для обеспечения качества и ответственности за результаты испытаний должны быть разработаны эффективные методы и методические нормативные документы, регламентирующие процессы сертификации различных видов ПС;
- технологические процессы сертификационных испытаний и измерений качества ПС и их компонент должны быть поддержаны достаточно эффективными средствами автоматизации и определения достоверности измеренных характеристик;
- исследование и обобщение опыта сертификации ПС должны способствовать минимизации затрат на такие испытания, а также улучшению технологических процессов разработки программ, гарантирующих достижение требуемых показателей качества для различных видов программ.

Кроме сертификации объектов разработки в некоторых случаях целесообразна сертификация технологии и средств автоматизации создания комплексов программ. Процесс сертификации технологии разработки ПС в принципе подобен испытаниям программ. Его важная особенность состоит в необходимости регулярного контроля за соблюдением всех характеристик качества технологического процесса всеми его участниками.

Исходные данные для сертификации ПС опираются на совокупность документов, выбираемых и адаптируемых с учетом конкретных объектов сертификации. Наиболее общие исходные данные сосредоточены в стандартах, посвященных непосредственно сертификации, аттестации, тестированию, испытаниям и обеспечению качества различных изделий и, в частности, компонент ИТ. Конкретные нормативные документы должны создаваться в соответствии с базовыми стандартами и содержать методики организации и проведения испытаний, а также контролируемые характеристики сертифицируемых объектов. Эти документы должны отражать все сведения, необходимые для корректного применения ПС по прямому назначению с показателями качества, гарантированными сертификатом соответствия.

Методология принятия решений о допустимости выдачи сертификата на ПС основывается на оценке степени его соответствия действующим и специально разработанным документам:

- международным и национальным стандартам на тестирование, испытания, аттестацию программ, требования которых не ниже требований, регламентируемых отечественными документами;
- международным и государственным стандартам на технологию создания ПС, взаимосвязь открытых систем, языки программирования и др.;
- стандартам на сопровождающую программную документацию с учетом необходимости и достаточности номенклатуры документов, семантической полноты и однозначности понимания содержания документов;
- нормативным документам на испытанное ПС техническим условиям, техническим описаниям, спецификациям требо-

ваний и другим регламентирующим документам по выбору заказчика, разработчика и испытателя.

В исходных нормативных документах должны быть сосредоточены все функциональные и эксплуатационные характеристики проверяемого ПС, обеспечивающие заказчику и пользователям возможность корректного применения сертифицированного объекта во всем многообразии его функций и показателей качества. Номенклатура характеристик сертифицируемых ПС строится на применении многоуровневых систем показателей качества, организованных по принципам квалиметрии и таксономических методов анализа. Выбор и ранжирование показателей должны производиться с учетом классов ПС, их функционального назначения, режимов эксплуатации, степени ответственности и жесткости требований к результатам функционирования и проявлениям возможных ошибок в программах.

Для сертификации необходимо подготовить следующие исходные данные:

- критерии и четко определенные значения показателей качества, которые должны быть достигнуты для выдачи в последующем сертификата соответствия;
- значения исходных и результирующих данных, в пределах которых должны удовлетворяться заданные показатели качества;
- стандарты, нормативные документы и методики точных и воспроизводимых измерений показателей качества программ, а также состав и значения исходных и результирующих данных, обязательных для использования сертификации.

Имеется необходимость вносить в модифицированные версии отдельные небольшие изменения без полных повторных сертификационных испытаний ПС. При любых изменениях необходимы подтверждение сертификата и проведение некоторого минимума испытаний, удостоверяющих их корректность. Для этого используется система официальных уведомлений о проведенных изменениях и подтверждении сертификата. Для инициализации изменений также необходимы официальные уведомления пользователей о выявленных недостатках ПС или о предложениях по его совершенствованию. Таким образом, обычный процесс со-

проведения ПС для сертифицируемых программ дополняется соответствующей системой последовательных официальных уведомлений и контрольных испытаний. При характеристиках и классификации программ как объектов сертификации основная цель классификации состоит в выделении однородных групп программ, имеющих такие показатели или признаки объекта, которые позволяют эффективно применять одинаковые или весьма близкие наборы показателей качества, технологии, методы и средства автоматизации испытаний и сертификации программ. Разнообразие объектов разработки не позволяет обеспечить достаточный уровень качества и технико-экономических показателей при единственной универсальной технологии и комплексе автоматизации испытаний программ. С другой стороны, нерентабельно для каждого нового типа программ создавать собственную технологию и средства автоматизации испытаний.

Классификация программ как база для рационального выбора методов и технологий сертификации, обеспечивающих необходимое качество программ и достаточно высокие технико-экономические показатели испытаний программ.

— Классификация программ и соответствующих технологий их испытаний прежде всего базируется на анализе риска от их недостаточного качества и возможного ущерба от проявления невыявленных ошибок при их функционировании у пользователей. С этой позиции по степени ответственности выполняемых функций можно выделить три группы программ:

— критические программы, от которых требуется особенно высокое качество функционирования, так как ошибки могут привести к катастрофическим последствиям порче ценного оборудования или даже угрозе здоровью и жизни людей;

— важные программы, которые должны обладать особенно высоким качеством, так как экономический ущерб от ошибок в них может быть велик, но невозможны особо катастрофические последствия;

— ординарные программы, недостатки которых не угрожают пользователям большим ущербом, являющиеся наиболее массовыми и широко распространенными, их качество и области применения изменяются в широких пределах и к ним принадле-

жат многие программы, отнесенные ниже к первой и второй категориям.

При оценке целесообразности сертификации необходимо учитывать возможный ущерб не только от кратковременного однократного неудачного применения ПС, но и возможный суммарный потенциальный ущерб от искажений и сбоев при длительной эксплуатации большого тиража версий ПС. Таким образом, в категорию важных ПС, подлежащих сертификации, могут попадать широко тиражируемые, длительно и активно применяемые программы, каковыми являются стандартизированные операционные системы, компиляторы, некоторые компоненты CASE-систем и др. В этих случаях испытания должны проводить также специализированные третейские организации, которые своим авторитетом и; соответствующим документом утверждают высокое качество программ для многочисленных пользователей. Примером может служить аттестация компиляторов с языка Ада, проводимая специализированной организацией АПРО.

У некоторых специалистов сложилось отрицательное отношение к планированию обеспечения качества и детальным формализованным испытаниям программ. Это характерно для создания программ инженерных и научных расчетов, при некоторых вычислительных экспериментах, разработке программ обучения или бытового применения, которые не подвергают сертификационным испытаниям. В категорию ординарных программ входят программы, разрабатываемые и применяемые в отраслях народного хозяйства, как продукция производственно-технического назначения. Основная особенность этой категории программ состоит в промышленном характере их разработки, испытаний, производства и применении в виде ПС. Программы данной категории в большинстве своем принадлежат к группам важных или критических. Это обуславливает определенные регламентированные организационные формы их жизненного цикла, особенно высокие требования к качеству и документации, необходимость применения типовых проблемно-ориентированных технологий и средств автоматизации при разработке, испытаниях и производстве.

Методы достижения высокого качества ПС

При ограниченных ресурсах на разработку ПС для достижения заданных требований необходимо управление обеспечением качества в течение всего цикла создания программ. Адекватный набор показателей качества программ зависит от функционального назначения и свойств каждого ПС. В соответствии с принципиальными особенностями ПС выбираются номенклатура и значения показателей качества, которые отражаются в техническом задании и спецификации требований на конечный продукт. Каждый критерий может использоваться, если определена его метрика, может быть указан способ ее измерения и сопоставления с требуемым значением. Основным методом измерения качества программ на любых этапах разработки является тестирование. Результаты тестирования и измерения показателей сравниваются с требованиями технического задания или спецификаций для определения степени соответствия предъявлявшимся требованиям, полученным разработчиком от заказчика. Такие достаточно полные эталоны, как совокупность требований технического задания и поэтапная их декомпозиция в спецификациях, являются необходимой базой тестирования при промежуточных и завершающих испытаниях.

За ограниченный, относительно короткий, период сертификационных испытаний трудно провести достаточно обширное тестирование, достоверно демонстрирующее достигнутые показатели качества, и гарантировать выполнение всех технических требований к сложному ПС. Поэтому для обеспечения высокого качества программ целесообразно проводить испытания не только завершеного разработкой ПС, но на ряде промежуточных этапов разработки проверять состояние и характеристики компонент проекта. Критические ПС невозможно создавать без проведения 68 этапов промежуточных испытаний и применения целой системы поэтапного контроля качества. Для этого до начала разработки в процессе формирования технического задания формулируются план и основные положения методики обеспечения качества, поэтапных испытаний компонент и определения характеристик, допустимых для продолжения разработки на следующем этапе. Одновременно происходит поэтапное уточнение техниче-

ского задания и методик сертификационных испытаний программ. В этом случае испытатели и представители заказчика получают возможность более полно ознакомиться с создаваемым ПС, а также контролировать качество его компонент и достаточно полно их учитывать при заключительных сертификационных испытаниях.

Достоверность результатов испытаний ПС

Сравнение результатов функционирования проверяемого комплекса программ и его компонент на соответствие эталонам предполагает использование критериев оценки величин отклонения от эталонов и принятие решений о степени корректности. Величины допусков зависят от типа проверяемой программы, метода и этапа проверки ее корректности.

Степень соответствия проверяемых программ эталонам зависит от достоверности функционирования всех компонент, участвующих в установлении корректности. Отклонение проверяемых результатов от эталонов за допустимые пределы может произойти не только вследствие некорректности программ, но и из-за недостаточной точности средств сравнения или эталонов.

Процессы испытаний происходят во времени и их динамические характеристики могут служить частными критериями для оценки достигнутого качества тестирования. Таким критерием может быть интенсивность обнаружения ошибок или количество ошибок, выявляемых в программах в процессе тестирования за единицу времени при постоянных усилиях на его проведение.

Проблемы сертификации БД

БД это набор записей информации, который определен посредством схемы, не зависящей от программ, которые к ней обращаются. Цель сертификации БД защитить требования потребителей к качеству используемой информационной продукции, содержащейся в БД, по полноте, достоверности, актуальности, защищенности и другим показателям. Обобщенным показателем качества информации в БД является степень ее соответствия существующим стандартам и другим нормативно-техническим документам как в содержательной, так и в форматно-структурной

части. Сертификационные испытания БД в некоторых случаях, например при применении их в критических информационных системах, должны проводиться обязательно. Однако чаще сертификация БД имеет факультативный характер, позволяющий пользователям иметь дополнительную гарантию ее качества.

При испытаниях и сертификации возникает проблема определения состава и использования реально существующих международных и отечественных стандартов и других нормативно-технических документов, которым должны соответствовать сертифицированные БД. Стандарты и документы должны охватывать:

- терминологию в области ИТ и систем;
- порядок организации и создания БД;
- концепции структурного построения, взаимодействия компонент и языки описания БД;
- комплектность документов, сопровождающих БД, и требования к ним; показатели качества БД, ИТ и ПС;
- методы и руководства по испытаниям, аттестации и сертификации компонент и БД в целом.

Непосредственно БД посвящены международные стандарты только на языки БД и на некоторые принципы построения БД. Однако имеются развитые системы стандартов по обработке информации и ИТ, в которых не упоминаются конкретно БД, но их положения по терминам и определениям, кодированию и документированию, жизненному циклу и показателям качества могут быть успешно применены при испытаниях и сертификации БД. Кроме того, при испытаниях и сертификации БД по мере необходимости следует учитывать стандарты в областях защиты информации, текстовых и учрежденческих систем, издательского дела, управления торговлей и транспортом и др. В некоторых стандартах имеются разделы, регламентирующие аттестацию ИТ и БД на соответствие данному стандарту. Эти разделы должны использоваться при подготовке методик сертификации БД на соответствие международным стандартам.

Наиболее трудными проблемами при организации и проведении сертификации БД являются:

- классификация БД по характеристикам и сферам их применения;
- определение номенклатуры и требуемых показателей качества БД;
- создание методик тестирования и испытаний БД и их компонент, а также методов и средств достоверного измерения показателей качества БД;
- организация, регламентирование и документирование сертификации БД.

Назначение и особенности современных БД

В ИТ и процессах обработки информации на ЭВМ всегда присутствуют две базовые компоненты: программы, которые реализуют функции обработки, и данные, используемые в процессе обработки. В предшествующих разделах акцент был сосредоточен на анализе и испытаниях ИТ, основные особенности которых заключаются в ПС. При анализе БД на передний план выходит информация, подлежащая накоплению, хранению, обработке и использованию. Соответственно смещается акцент при испытаниях качества БД и при их эксплуатации. Однако при этом сохраняется достаточно важная роль ПС, реализующих все процедуры обработки данных.

Таким образом, при анализе БД как объектов испытаний и сертификации целесообразно рассматривать две компоненты: ПС управления данными и совокупность данных, упорядоченных по некоторым правилам. При этом одна и та же система управления БД может обрабатывать различные по структуре, составу и содержанию данные, а одни и те же данные могут управляться ПС различных СУБД. Хотя эти компоненты тесно взаимодействуют при реализации конкретной прикладной БД, первоначально они создаются независимо и могут рассматриваться как два объекта испытаний. Однако, в конечном счете пользователей интересуют совокупные характеристики качества конкретной используемой БД. Поэтому завершающие испытания и окончательная сертификация БД должны проводиться для проверки функционирования и удостоверения показателей качества во взаимодействии с пред-

полагаемой для использования СУБД, с вполне определенным наполнением БД.

БД графической, речевой, мультимедиа и другой нетрадиционной информации только входят в практику и носят преимущественно экспериментальный характер. Результаты функционирования таких БД отражаются графическими, звуковыми или визуальными образами, качество которых оценивается человеком в значительной степени субъективно. Вследствие этого испытания подобных систем пока слабо формализованы и их сертификация производится редко. Наиболее широко вошли в практику БД для фактографической, документальной, словарной и текстовой информации, для которых накоплен большой опыт использования и испытаний. Поэтому ниже рассматривается сертификация таких БД.

Показатели качества БД

Особенности современных БД и обеспечивающих их СУБД являются следствием возрастающего спектра функций по обработке информации и разнообразия обрабатываемых данных. Отсюда появилось множество наборов показателей качества, определяющих функциональную пригодность каждой БД. Формирование таких наборов представляет собой сложную задачу системного анализа, характеризующуюся оригинальным решением для каждой прикладной проблемно-ориентированной области. Вследствие этого испытания и определения в процессе проектирования достигнутых показателей качества БД отличаются большим разнообразием методов и средств автоматизации.

В рассматривавшихся выше ИТ основное внимание сосредоточено на испытаниях ПС. В системах БД доминирующее значение приобретают сами данные, их хранение и обработка. Поэтому БД при анализе их качества целесообразно разделить на две компоненты:

- ПС СУБД, не зависящие от сферы их применения и смыслового содержания накапливаемых и обрабатываемых данных;
- БД, доступные для обработки и использования в конкретной проблемно-ориентированной сфере применения.

Первой компонентой для испытаний является комплекс программ СУБД. Сертификации должно подвергаться ПС обработки данных на соответствие стандартам и нормативно-техническим документам, адекватным функциям и характеристикам области использования. Методы и технология сертификации, в основном, подобны применяемым при испытаниях других сложных ПС. При этом специфика испытаний так же, как и для других типов ПС, сосредоточивается на выборе адекватных показателей качества из стандартной номенклатуры, особенностях генерации тестов и обработке результатов тестирования. Поставщиками информации для СУБД чаще всего являются специалисты-пользователи и они же должны выступать в роли генераторов тестов. Часть тестов может носить достаточно абстрактный характер и автоматизировано формироваться для заполнения БД и испытания основных операций обработки данных.

Часть функций, связанных с телекоммуникацией, должна испытываться на соответствие стандартам и протоколам телекоммуникации и взаимосвязи открытых систем. Другая значительная часть функций непосредственно обусловлена спецификой применения распределенной СУБД. Некоторые из этих функций регламентируются специальными стандартами, в которых, в частности, представлены рекомендации по их аттестации. Кроме того, для распределенных СУБД значительно возрастает номенклатура сочетаний типов ЭВМ, выполняющих роль клиентов и серверов. Комбинаторика подобных типов ЭВМ и их операционных систем может быть весьма велика, и при испытаниях СУБД трудно охватить и проверить все особенности взаимодействия в таких распределенных СУБД. Поэтому сертификаты распределенных СУБД должны отражать номенклатуру типов ЭВМ и операционных систем, для которых они предназначены.

Второй компонентой для испытаний БД является собственно накапливаемая и обрабатываемая информация в БД. Показатели качества для БД значительно отличаются от применяемых при испытаниях ПС. Однако может сохраняться общий подход к определению и выделению адекватной номенклатуры показателей качества и их упорядочению. Он состоит в том, что выделяемые показатели качества должны иметь практический интерес

для пользователей БД и быть упорядочены в соответствии с приоритетами практического применения. Кроме того, каждый выделяемый для проверки показатель должен быть пригоден для достаточно достоверного измерения и сравнения с требуемым значением при испытаниях и сертификации.

При этом подлежат тестированию, испытаниям и измерению показатели качества информации в БД и определение их соответствия стандартам и технической документации, а также проверяются состав и содержание сопровождающих БД документов. Для сертификации разрабатываются программа и методики испытаний, обеспечивающие достоверную проверку реальных показателей качества БД. Результаты испытаний оформляются протоколами и актом. При положительных результатах заявителю выдается сертификат соответствия.

Так же, как и для ПС, показатели качества БД можно разделить на функциональные и конструктивные. Функциональные показатели качества БД включают:

- полноту накопленных описаний объектов относительно число объектов или документов, имеющих в БД, к общему числу объектов по данной тематике или по отношению к числу объектов в аналогичных БД по той же тематике;
- достоверность степень соответствия данных об объектах в БД реальным объектам вне ЭВМ в данный момент времени, определяющаяся изменениями самих объектов, некорректностями записей о их состоянии или некорректностями расчетов их характеристик;
- идентичность данных относительно число описаний объектов, не содержащих ошибки, к общему числу документов об объектах в БД;
- актуальность данных относительно число морально устаревших данных об объектах в БД к общему числу накопленных и обрабатываемых данных.

К конструктивным показателям качества информации в БД относятся, в основном, объемно-временные характеристики сохраняемых и обрабатываемых данных:

- объем базы данных число записей описаний объектов или документов, доступных для хранения и обработки в БД;

- оперативность степень соответствия динамики изменения данных в процессе сбора и обработки состоянием реальных объектов или величина запаздывания между появлением реального объекта и его отражением в банке данных;
- периодичность промежутков времени между поставками двух последовательных достаточно различающихся версий БД;
- глубина ретроспективы интервал времени от даты выпуска и/или записи в БД самого раннего документа до настоящего времени;
- динамичность относительное число изменяемых описаний объектов к общему числу записей в БД за некоторый интервал времени, определяемый периодичностью издания версий БД.

Кроме того, к конструктивным относятся все показатели защищенности информации. Защищенность реализуется, в основном, ПС СУБД, однако в сочетании с поддерживающими их средствами организации данных. В распределенных БД показатели защищенности тесно связаны с характеристиками целостности данных. Эти показатели отражают степень тождественности данных в памяти удаленных компонент распределенной БД.

К конструктивным относятся также показатели, определяющие форматную, лингвистическую и физическую совместимость БД. Форматная совместимость характеризуется степенью соответствия данных в БД требованиям стандартов на форматы представления данных для документальных, фактографических и словарных БД. Лингвистическая совместимость определяется степенью использования в БД единых лингвистических средств (классификаторов, рубрикаторов, словарей), формализованных соответствующими стандартами. Физическая совместимость заключается в соответствии БД на машиночитаемых носителях информации. Кроме того, каждая БД должна содержать идентификационные признаки (наименование, тематику, область применения, тип), правовые характеристики авторов разработки СУБД и БД и авторское право пользователей на информацию, содержащуюся в БД, в соответствии с конвенцией и законами об охране авторских прав.

Перечисленные характеристики отражают качество совокупности данных без учета динамики их использования пользователями в процессе эксплуатации. При реальном функционировании БД важную роль играют временные характеристики взаимодействия конечных пользователей и администраторов БД в процессе эксплуатации БД по прямому назначению. Эти характеристики зависят от качества СУБД, а также от структуры и показателей качества используемой информации. Они отражаются критерием эффективности использования ресурсов ЭВМ ПС, в данном случае СУБД. Для БД важнейшим ресурсом является память ЭВМ, занимаемая информацией БД. Эти показатели качества влияют на время реакции БД на разные виды запросов пользователей и пропускную способность БД при эксплуатации. Значения ряда других показателей качества ПС, составляющих СУБД, существенно зависят от характеристик и организации информации в БД. Поэтому при испытаниях и сертификации БД номенклатура показатели качества не может ограничиваться характеристиками информации в БД, а должна включать ряд дополнительных показателей, отражающих комплексную эффективность и функциональную полезность применения СУБД и БД пользователями в реальных условиях.

Ресурсы для сертификации ИТ

В зависимости от характеристик объекта сертификации на ее выполнение выделяются ресурсы различных видов. В результате сложность ИТ и доступные ресурсы становятся косвенными критериями или факторами, влияющими на выбор методов испытаний и достигаемое качество компонент ИТ.

Наиболее общим видом ресурсов, используемых при испытаниях ИТ, являются допустимые финансовые затраты или договорная стоимость сертификации компонент ИТ. При анализе эти показатели могут применяться как вид ресурсных ограничений или как оптимизируемый критерий.

Кадры специалистов можно оценивать численностью, а также тематической и технологической квалификацией. В испытаниях сложных ИТ участвуют системные аналитики и руководители различных рангов, программисты и вспомогательный об-

служивающий персонал в некотором рациональном сочетании. Определяющими являются совокупная численность и структура коллектива, а также его подготовленность к коллективной проверке конкретного типа ИТ.

Аппаратурная оснащенность испытателей конкретных ПС или БД определяется прежде всего ресурсами и другими характеристиками реализующей и технологической ЭВМ, доступных для использования коллективу специалистов при сертификации. Тип реализующей ЭВМ, ее ресурсы, архитектура и система команд определяют возможность размещения на ней комплекса автоматизации контроля и регистрации результатов испытаний. Ресурсы технологической ЭВМ важны для сертификации не только по своим абсолютным значениям, но также и относительно численности коллектива специалистов, участвующих в испытаниях.

Порядок выполнения работы

Данная лабораторная работа предполагает выполнение следующих этапов:

- изучить методические указания;
- ответить на контрольные вопросы.

Контрольные вопросы

1. В чем заключается сертификация соответствия программных средств?
2. Что подтверждает сертификат соответствия программного средства?
3. Виды сертификации программных средств.
4. В чем заключается добровольная сертификация?
5. Базовые компоненты методологии сертификации.
6. Проблемы при анализе сертификации.
7. Методы достижения высокого качества программных средств.
8. Достоверность результатов испытаний программных средств.
9. Проблемы сертификации баз данных.
10. Ресурсы для сертификации информационных технологий.

САМОСТОЯТЕЛЬНАЯ РАБОТА

Целью самостоятельной работы обучающихся является получение новых знаний по дисциплине «Сертификация информационных систем».

Самостоятельная работа необходима для формирования у обучающихся способности самостоятельно решать задачи профессиональной деятельности, формирования умения и навыков планирования времени, формирования стремления развиваться и совершенствоваться.

Виды самостоятельной работы обучающихся указаны в таблице 1.

Таблица 1 – Виды самостоятельной работы

№ п/п	Вид самостоятельной работы
1	Изучение литературы на тему «Создание центра сертификации»
2	<p>Выполнение индивидуальных заданий по теме "Защита и сохранность информации баз данных":</p> <p>Задание 1. Исследуйте базу данных на наличие потенциальных уязвимостей. Опишите, какие виды атак могут быть осуществлены на данную базу данных и каким образом их можно предотвратить.</p> <p>Задание 2. Создайте документ с описанием политики безопасности базы данных. Включите в него правила доступа к данным, шифрование информации, резервное копирование и другие меры по обеспечению безопасности.</p> <p>Задание 3. Проведите тестирование на проникновение в базу данных с использованием специальных инструментов. Оцените результаты и предложите меры по устранению обнаруженных уязвимостей.</p> <p>Задание 4. Проверьте настройки аутентификации и авторизации в вашей базе данных. Убедитесь, что доступ к данным предоставляется только авторизованным пользователям с соответствующими правами доступа.</p> <p>Задание 5. Настройте систему мониторинга безопасности базы данных для отслеживания подозрительной ак-</p>

№ п/п	Вид самостоятельной работы
	<p>тивности и несанкционированных попыток доступа.</p> <p>Задание 6. Создайте план реагирования на инциденты безопасности, включая шаги по обнаружению, анализу и реагированию нарушений правил безопасности.</p> <p>Задание 7. Внедрите механизмы шифрования данных в вашу базу данных для защиты конфиденциальной информации. Оцените различные методы шифрования и выберите наиболее подходящие для ваших целей.</p>

СПИСОК ЛИТЕРАТУРЫ

Основная литература

1. Перлова, О. Н. Соадминистрирование баз данных и серверов : учебник для студентов среднего профессионального образования по специальности 09.02.07 "Информационные системы и программирование" / О. Н. Перлова, О. П. Ляпина ; О. Н. Перлова, О. П. Ляпина. – Москва : Академия, 2020. – 304 с. с. – (Профессиональное образование). – URL: <https://academia-moscow.ru/reader/?id=480248> (дата обращения: 17.04.2024). – Текст : электронный.

Дополнительная литература

1. Сергеев, А. Г. Сертификация.: учебник и практикум для СПО / Сергеев А. Г., Терегеря В. В.. – Москва : Юрайт, 2021. – 195 с. – ISBN 978-5-534-04550-5. – URL: <https://urait.ru/book/sertifikaciya-469817> (дата обращения: 14.04.2024). – Текст : электронный.

2. Сергеев, А. Г. Стандартизация и сертификация.: учебник и практикум для СПО / Сергеев А. Г., Терегеря В. В.. – Москва : Юрайт, 2021. – 323 с. – ISBN 978-5-534-04315-0. – URL: <https://urait.ru/book/standartizaciya-i-sertifikaciya-469819> (дата обращения: 14.04.2024). – Текст : электронный.

3. Кошечая, И. П. Метрология, стандартизация, сертификация : Учебник / И. П. Кошечая, А. А. Канке. – Москва : НИЦ ИНФРА-М, 2022. – 415 с. – ISBN 978-5-16-013572-4. – URL: <https://znanium.com/catalog/document?id=428864> (дата обращения: 11.10.2023). – Текст : электронный.

4. Шишмарев, В. Ю. Метрология, стандартизация, сертификация, техническое регулирование и документоведение : Учебник / В. Ю. Шишмарев. – Москва : НИЦ ИНФРА-М, 2024. – 312 с. – ISBN 978-5-906923-15-8. – URL: <https://znanium.com/catalog/document?id=432940> (дата обращения: 11.10.2023). – Текст : электронный.

5. Мартишин, С. А. Проектирование и реализация баз данных в СУБД MySQL с использованием MySQL Workbench : Методы и средства проектирования информационных систем и технологий. Инструментальные средства информационных систем. Учебное пособие / С. А. Мартишин, В. Л. Храпченко М. В. Симонов. – Москва : НИЦ ИНФРА-М, 2023. – 160 с. – ISBN 978-5-8199-0811-2. – URL: <https://znanium.com/catalog/document?id=424789> (дата обращения: 11.10.2023). – Текст : электронный.