Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Оренбургский государственный университет»

Кафедра вычислительной техники

А.Ю. Кручинин Е.И. Ряполова

ВСТРОЕННЫЕ СРЕДСТВА ЗАЩИТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS 7

Рекомендовано к изданию Редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Оренбургский государственный университет» в качестве методических указаний для студентов, обучающихся по программам высшего профессионального образования по направлению подготовки 090900.62 Информационная безопасность

Оренбург
2013

УДК 004(07)
ББК 32.81я7
К 84

Рецензент – кандидат технических наук А.С. Цыганков

Кручинин, А.Ю.

К 84 Встроенные средства защиты операционной системы Windows 7: методические указания к лабораторным работам / А.Ю. Кручинин, Е.И. Ряполова. – Оренбургский гос. ун-т. – Оренбург: ОГУ, 2013. – 56 с.

Методические указания содержат 3 лабораторные работы и методические указания к ним. Каждая работа включает теоретическое изложение материала, постановку задачи, порядок выполнения и контрольные вопросы для самоподготовки.

Методические указания предназначены для студентов направления 090900.62 - «Информационная безопасность».

УДК 004(07)
ББК 32.81я7

Содержание

Введение

Методические указания содержат 3 лабораторные работы и методические указания к ним. Каждая работа включает теоретическое изложение материала, постановку задачи, порядок выполнения и контрольные вопросы для самоподготовки. Методические указания предназначены для студентов направления 090900.62– «Информационная безопасность».

Лабораторные работы направлены на изучения основ организации безопасности на ОС Windows 7. Рассмотрены вопросы структуры системы безопасности, организации аутентификации пользователей локально и по сети. Выделены элементы безопасности компьютерной системы и понятие маркера доступа, который влияет на разрешение или запрещение доступа к ресурсам.

Важную роль в обеспечении безопасности играю встроенные средства управления, в том числе и консоль ММС. В методических указаниях рассмотрены примеры работы с консолью, а задания направлены на ознакомление с основными функциями консоли.

Задача обеспечения конфиденциальности данных является одной из самых актуальной, поэтому в методических указаниях отдельное внимание уделено рассмотрению средств обеспечения доступа к файлам и папкам, в том числе с использованием шифрованной файловой системой.

1 Структура системы безопасности Windows 7 и процедура аутентификации

Цель работы: ознакомиться со структурой системы безопасности и процедурой аутентификации Windows 7**.**

1.1 Основные понятия

В структуру операционной системы (ОС) входят следующие ключевые элементы с точки зрения безопасности:

- возможность защищённого входа в систему с идентификацией пользователей;
- контроль доступа по категориям пользователей;
- аудит, т.е. независимая проверка с целью выражения мнения о достоверности.

Это далеко не полный список элементов, однако они наиболее важные с точки зрения безопасности – аутентификация, авторизация и аудит. Они были встроены в ОС Windows NT с самого начала. Во всех системах этого семейства, включая и современные, эти возможности реализованы с помощью подсистемы безопасности (рисунок 1.1).

Главным элементом системы безопасности является менеджер безопасности режима ядра (SRM), исполняющий сложный механизм безопасности Windows, удовлетворяющий требованиям класса С2 Оранжевой книги Министерства обороны США. Помимо этого в режиме пользователя работают следующие важные компоненты.

Winlogon – компонент операционной системы Microsoft Windows, отвечающий за вход в систему и т.д. Winlogon обрабатывает нажатие Ctrl-Alt-Del и Ctrl-Shift-Esc. В ходе запуска ОС Winlogon запускает LSASS и Services.exe.

Lsass – подсистема полномочий локальной безопасности, т.е. часть ОС отвечающей за авторизацию локальных пользователей отдельного компью-

тера. При получении полного доступа к данному сервису злоумышленник может получить полные права для доступа к компьютеру. Поэтому способ шифрования и способ передачи данных для авторизации между компонентами не документируется.

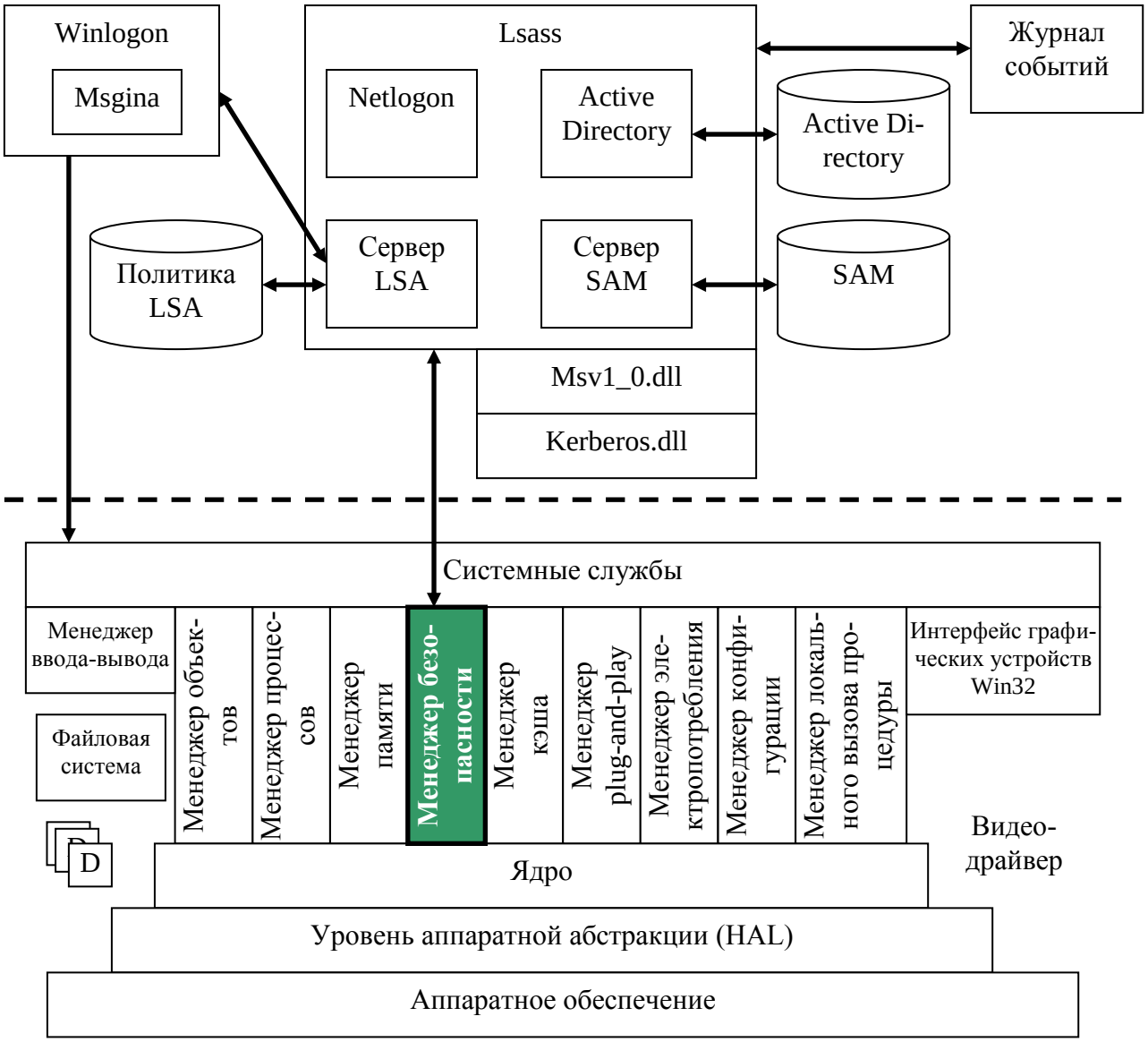

Рисунок 1.1 – Подсистема безопасности Windows

Сервер LSA отвечает за вход в систему. Служба Net Logon автоматически запускается, только когда к домену подключается рядовой компьютер или контроллер домена.

SAM – RPC-сервер Windows, оперирующий базой данных учетных записей.

Active Directory – LDAP-совместимая реализация интеллектуальной службы каталогов корпорации Microsoft для операционных систем семейства Windows NT. Active Directory позволяет администраторам использовать групповые политики (GPO) для обеспечения единообразия.

Суть рисунка 1.1 сводится к тому, что в Windows реализован диспетчер системы безопасности, который выполняется в высоко-привилегированном режиме ядра и проверяет все запросы ресурсов из кода, исполняющегося в пользовательском режиме при работе приложений.

Диспетчер SRM выступает в роли хранителя ресурсов Windows. Но в каких случаях он разрешает или запрещает доступ к ресурсу? Почти весь контроль доступа к ресурсам Windows осуществляется по отношению к элементам системы безопасности. Элементами системы безопасности Windows являются:

- пользователи;
- группы;
- компьютеры.

Важными понятиями являются аутентификация и авторизация. Аутентификация – это установление подлинности лица, а авторизация – предоставление этому лицу некоторых прав. ОС оперирует с элементами безопасности и должна решать, к каким ресурсам имеет доступ тот или иной элемент безопасности.

ОС должна определить, что она работает с действительным элементом системы безопасности. Это делается посредством аутентификации. Простейший пример – вход пользователя в систему Windows с консоли. Пользователь нажимает клавиши <CTRL+ALT+DEL>, после чего вводит свои имя пользователя и пароль. Программа защиты входа в систему обрабатывает введенные данные с помощью компонентов, работающих в пользовательском режиме, как показано на рисунке 1.1 (программы Winlogon и LSASS). Если аутентификация проходит успешно, программа Winlogon создаст маркер доступа (набор атрибутов пользователя или процесса), который присваивается

сеансу работы пользователя и используется при любой последующей попытке доступа к ресурсам.

Маркер доступа содержит список всех идентификаторов SID, связанных с учетной записью пользователя, включая идентификатор SID самой учетной записи, идентификаторы SID всех групп, в которые добавлена эта учетная запись, и идентификаторы специальных групп, к которым относится данный пользователь (например, Domain Admins или INTERACTIVE). Чтобы узнать, какие идентификаторы SID связаны с сеансом работы, можно воспользоваться программой whoami, которая входит в пакет дополнительных программ Windows.

```
C:\>whoami /user /groups

USER INFORMATION
----------------

User Name         SID
================= ============================================
test\administrator S-1-5-21-351884573-2638605479-2349113266-500


GROUP INFORMATION
-----------------

Group Name                           Type             SID          Attributes
==================================== ================ ============
=============================================================
Everyone                             Well-known group S-1-1-0      Mandatory
group, Enabled by default, Enabled group
BUILTIN\Administrators               Alias            S-1-5-32-544 Mandatory
group, Enabled by default, Enabled group, Group owner
BUILTIN\Users                        Alias            S-1-5-32-545 Mandatory
group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE             Well-known group S-1-5-4      Mandatory
group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users     Well-known group S-1-5-11     Mandatory
group, Enabled by default, Enabled group
NT AUTHORITY\This Organization       Well-known group S-1-5-15     Mandatory
group, Enabled by default, Enabled group
LOCAL                                Well-known group S-1-2-0      Mandatory
group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication     Well-known group S-1-5-64-10  Mandatory
group, Enabled by default, Enabled group
```

Синтаксис использования whoami.

WHOAMI [/UPN | /FQDN | /LOGONID]

WHOAMI { [/USER] [/GROUPS] [/PRIV] } [/FO <Σ«α¼áΓ>] [/NH]

WHOAMI /ALL [/FO <формат>] [/NH]

Параметры:

/UPN Отображение имени пользователя в формате имени участника-пользователя (UPN).

/FQDN Отображение имени пользователя в формате полного доменного имени (FQDN).

/USER Отображение сведений о текущем пользователе вместе с идентификатором безопасности (SID).

/GROUPS Отображение для текущего пользователя членства в группах, типа учетной записи, идентификаторов безопасности (SID) и атрибутов.

/PRIV Отображение привилегий безопасности текущего пользователя.

/LOGONID Отображение идентификатора текущего пользователя.

/ALL Отображение имени пользователя, членства в группах, идентификаторов безопасности (SID) и привилегий для токена доступа текущего пользователя.

/FO <формат> Формат вывода.
Допустимые значения TABLE, LIST, CSV.
Заголовки столбцов в формате CSV не отображаются. Формат по умолчанию: TABLE.

/NH Указывает, что строка заголовков столбцов не отображается при выводе.
Допускается только для форматов TABLE и CSV.

/? Вывод справки по использованию.

Когда пользователь пытается получить доступ к некоторому ресурсу, например к файлу, программа SRM сравнивает его маркер доступа со спи-

ском разграничительного контроля доступа DACL объекта. Список DACL содержит идентификаторы SID, для которых разрешен доступ к объекту, и разрешенный тип доступа (чтение, запись, выполнение и т.п.). Если один из идентификаторов SID учетной записи пользователя совпадает с идентификатором SID из списка DACL, то пользователь получает доступ в соответствии с условиями, указанными в DACL. Эти действия отражены на рисунке 1.2.

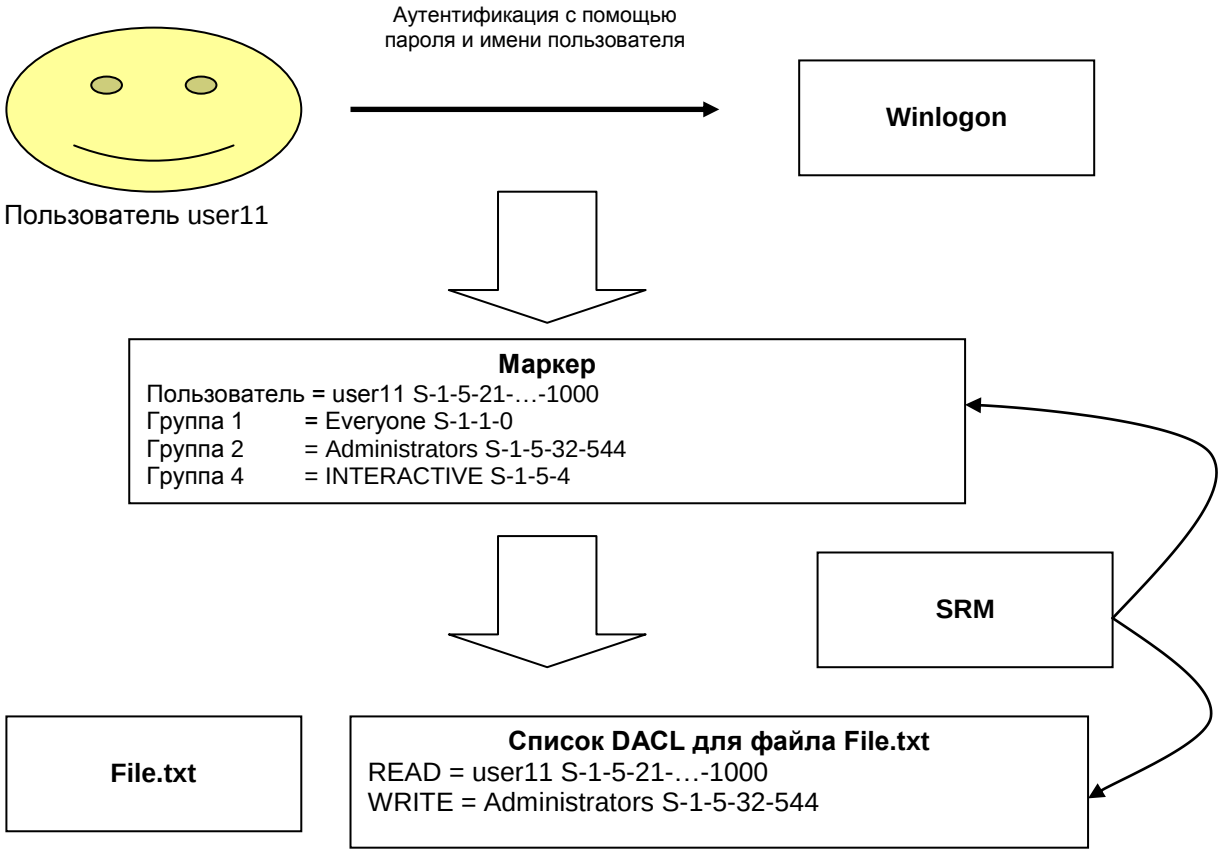

Рисунок 1.2 – Процедура аутентификации при помощи пароля и имени

Чтобы уменьшить затраты на обслуживание сети, в семействе систем Wndows NT реализована возможность заимствования прав учетной записи пользователя при работе с ресурсами на удаленном сервере. При заимствовании прав сервер сообщает службе SRM, что он временно принимает маркер доступа клиента, который обращается к ресурсу. Также активно используется понятие делегирования – позволяет службе заимствовать права учетной записи пользователя или учетной записи компьютера в целях предоставления службе доступа к ресурсам домена.

В современно мире аутентификации непосредственно на одном персональном компьютере недостаточно, поэтому используется аутентификация по сети, что является потенциально более опасным механизмом.

В системах семейства Windows NT в основном используют аутентификацию с запросом и подтверждением, при которой сервер передает клиенту случайное число (запрос), клиент затем обрабатывает полученное число с помощью функции хеширования, используя хешированный пароль пользователя, и возвращает новое хешированное значение (ответ) серверу. После этого сервер берет свою копию хешированного пароля пользователя из локальной базы данных SAM или Active Directory, хеширует отправленный им запрос и сравнивает полученное значение с ответом клиента. Таким образом, при аутентификации в системах семейства Wndows NT пароли не передаются по сети даже в зашифрованном виде (рисунок 1.3).

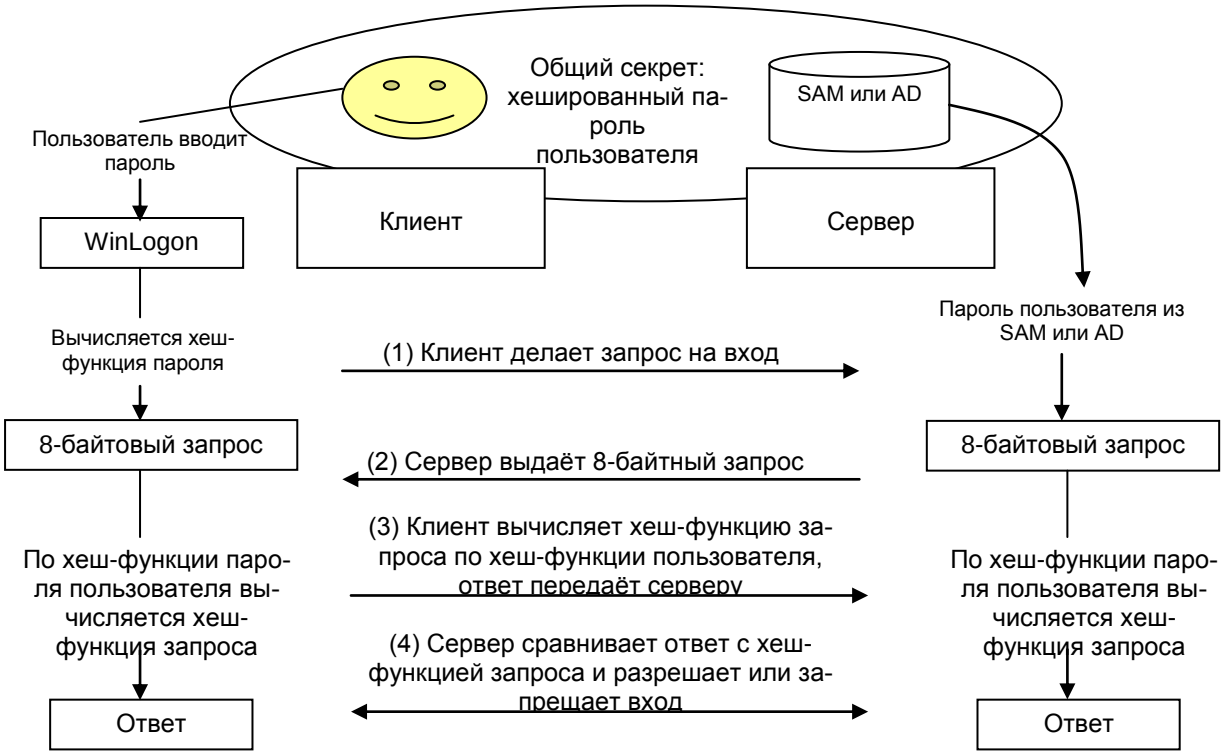

Рисунок 1.3 – Аутентификации по сети

На всех компьютерах под управлением Windows NT информация об именах учетных записей и паролях содержится в базе данных диспетчера системы защиты (служба SAM – Security Access Manager). Пароли хранятся в

зашифрованном виде, их невозможно расшифровать, пользуясь известными методами (хотя зашифрованное значение можно подобрать). Процедура шифрования называется односторонней функцией (ОСФ) или алгоритмом хеширования, значение хеш-функции расшифровать нельзя. Программный интерфейс для доступа клиентов к серверу реализован в виде функций, содержащихся в DLL-библиотеке samlib.dll.

SAM выполняет следующие задачи:

- идентификация субъектов;
- проверка пароля, авторизация (участвует в процессе входа пользователей в систему);
- хранит статистику (время последнего входа, количества входов, количества некорректных вводов пароля);
- хранит настройки политики учетных записей и приводит их в действие (политика паролей и политика блокировки учетной записи);
- хранит логическую структуру группировки учетных записей (по группам, доменам);
- контролирует доступ к базе учетных записей;
- предоставляет программный интерфейс для управления базой учетных записей.

База данных SAM хранится в реестре (в ключе HKEY_LOCAL_MACHINE\SAM\SAM), доступ к которому запрещен по умолчанию даже администраторам.

На контроллерах доменов имя учетной записи и хешированный пароль хранятся службой Active Directory.

Начиная с версии NT4, пакет обновления 3. фирма Microsoft обеспечила возможность использования еще одного уровня шифрования для хешированных паролей SAM, который называется SYSKEY. SYSKEY вычисляет случайный 128-разрядныи ключ и этим ключом еще раз шифрует хешированные пароли (только хеш-функции, а не сам файл SAM).

Рисунок 1.4 – Вызов команды syskey

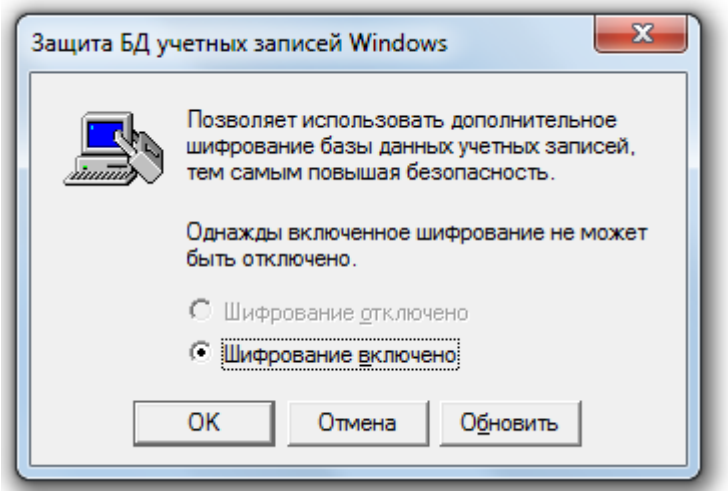

Рисунок 1.5 – Результат вызова команды syskey

Если в окне, показанном на рисунке 1.5 выбрать кнопку «Обновить», то на экране появится следующее окно (рисунок 1.6)

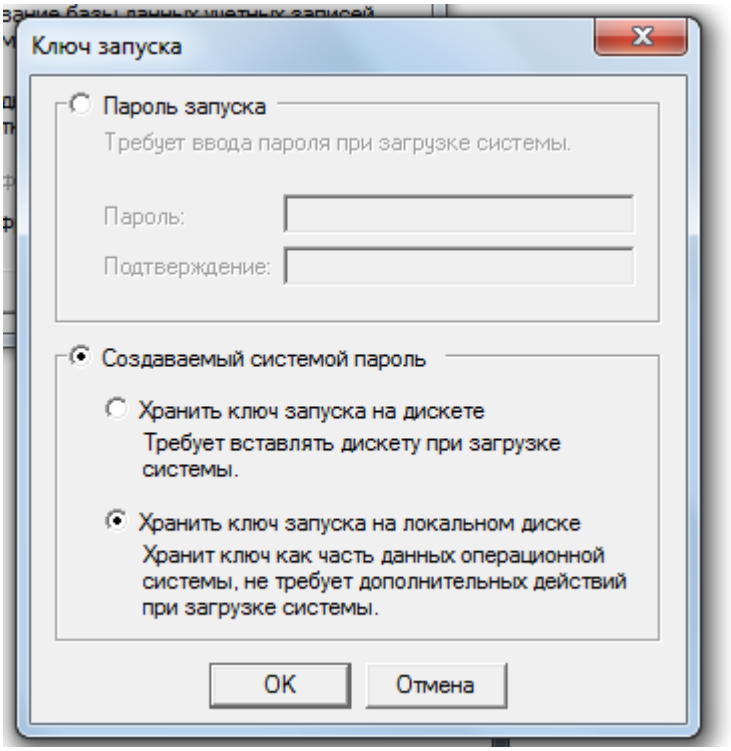

Рисунок 1.6 – Окно настроек syskey

SYSKEY может храниться в одном из трех режимов.

Режим 1. Хранится в реестре и предоставляется автоматически во время загрузки (настройка по умолчанию).

Режим 2. Хранится в реестре, но заблокировано паролем, который необходимо ввести во время загрузки.

Режим 3. Хранится на гибком диске и должно быть предоставлено во время загрузки. Выбор этих режимов показан на следующем рисунке.

1.2 Задание к лабораторной работе № 1

1 Ознакомиться с основными элементами системы безопасности ОС Windows.

2 Используя утилиту whoami, узнайте следующую информацию: а) имя пользователя; б) имя пользователя в формате полного доменного имени; в) SID пользователя; г) в каких группах состоит пользователь; д) привилегии безопасности пользователя.

3 Ознакомиться с процедурами аутентификации пользователей на локальном компьютере и по сети.

4 С использованием syskey, смените режим хранения базы данных на заблокированный паролем.

5 Сделать выводы о проделанной работе.

1.3 Ход выполнения работы №1

1 Ознакомится с пунктом 1.1 и усвоить основные элементы безопасности ОС Windows 7.

2 Запустить командную строку (cmd) через «Пуск» → «Выполнить».

3 Получить информацию о свойствах выполнения утилиты whoami с помощью ключа /?.

4 Воспользовавшись параметрами утилиты, узнайте информацию перечисленную в пункте 2 задания.

5 Ознакомьтесь с механизмом аутентификации пользователей.

6 Запустить утилиту syskey через «Пуск» → «Выполнить».

7 Измените режим хранения SYSKEY на зашифрованный.

8 Перезапустите операционную систему и посмотрите изменения.

9 Возвратите прежний режим хранения SYSKEY.

1.4 Контрольные вопросы

1 Каково назначение SRM?

2 Назовите существующие элементы безопасности Windows 7.

3 Что такое маркер доступа?

4 Как пользователь получает доступ к некоторому ресурсу?

5 Объясните суть аутентификации по сети.

2 Изучение средств управления Windows 7

Цель работы: ознакомиться с функциями консоли MMC**.**

2.1 Основные понятия

В Windows 7 реализована общая консоль управления, которая разработана для запуска всех программных модулей администрирования, конфигурирования или мониторинга локальных компьютеров и сети в целом. Такие законченные модули называются оснастками. Оснастки представляют собой управляющие компоненты, которые объединены в среде MMC.

Консоль MMC включает в себя интерфейсы прикладного программирования (API), оболочку пользовательского интерфейса (консоли) и набор инструкций. Консоль управления имеет преимущества, которые заключаются в упрощении интерфейса, предоставлении больших возможностей по настройке разработанных решений для определенных административных проблем и в обеспечении различных уровней функциональности.

Преимущества MMC:

– **возможность индивидуальной настойки и передача полномочий.** MMC предоставляет возможность полностью индивидуальной настройки, так что администраторы могут создавать такие консоли управления, которые будут включать только необходимые им инструменты. Такая настройка позволяет ориентировать администрирование на выполнение конкретных задач, причем администратор может выделить только необходимые объекты и элементы. Настройка консоли также позволяет администраторам передавать определенную часть полномочий менее опытным сотрудникам. С помощью MMC можно создать консоль, которая будет содержать объекты, необходимые для выполнения только определенных функций;

– **интеграция и унификация.** MMC обеспечивает общую среду, в которой могут запускаться оснастки, и администраторы могут управлять раз-

личными сетевыми продуктами, используя единый интерфейс, что упрощает изучение работы с различными инструментами.

– **гибкость в выборе инструментов и продуктов.** В среде MMC можно использовать различные инструменты и оснастки. Для использования в среде MMC оснастка должна поддерживать объектную модель компонентов (Component Object Model, COM) или распределенную COM (Distributed Component Object Model, DCOM). Это позволяет выбирать наиболее оптимальный продукт среди оснасток, причем гарантируется его полная совместимость со средой MMC.

Консоль управления MMC имеет пользовательский интерфейс, позволяющий открывать множество документов (Multiple Document Interface, MDI). Интерфейс консоли MMC на рисунке 2.1.

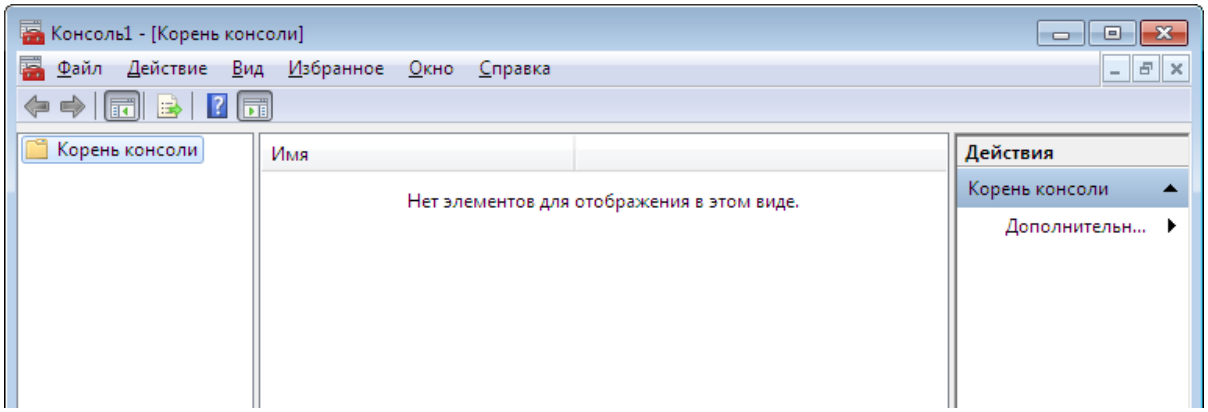

Рисунок 2.1 – Интерфейс консоли MMC

Родительское окно MMC имеет главное меню и панель инструментов. Главное меню обеспечивает функции управления файлами и окнами, а также доступ к справочной системе.

Дочерние окна MMC представляют собой различные средства просмотра автономного документа консоли. Каждое из этих дочерних окон содержит панель управления, панель структуры и панель результатов, или сведений. Панель управления содержит меню и набор инструментов. Панель структуры отображает пространство имен инструментов в виде дерева, кото-

рое содержит все видимые узлы, являющиеся управляемым объектом, задачей или средством просмотра.

Панель результатов в дочернем окне отображает список элементов выбранного узла. Данный список может содержать папки, оснастки, элементы управления, web-страницы, панели задач и другие элементы.

Типы оснасток:

– изолированная оснастка обеспечивает выполнение своих функций даже при отсутствии других оснасток, например, «Управление компьютером»;

– оснастка расширения может работать только после активизации родительской оснастки. Функция оснастки расширения заключается в увеличении числа типов узлов, поддерживаемых родительской оснасткой. Оснастка расширения является подчиненным элементом узлов определенных типов, и при каждом запуске узлов данных типов консоль автоматически запускает все связанные с ней расширения. В качестве примера можно привести оснастку «Диспетчер устройств». Оснастки расширения могут предоставлять различные функциональные возможности. Например, такие оснастки могут расширять пространство имен консоли, увеличивать число пунктов в меню или добавлять определенные мастера.

Управление рабочей средой пользователя

Рабочая среда пользователя состоит из настроек рабочего стола, например, цвета экрана, настроек мыши, размера и расположения окон, из настроек процесса обмена информацией по сети и с устройством печати, переменных среды, параметров реестра и набора доступных приложений.

Для управления средой пользователя предназначены следующие средства Windows 7:

1 Сценарий входа в сеть (сценарий регистрации) представляет собой командный файл, имеющий расширение .bat, или исполняемый файл с расширением .exe, который выполняется при каждой регистрации пользователя в сети. Сценарий может содержать команды операционной системы, предна-

значенные, например, для создания соединения с сетью или для запуска приложения. Кроме того, с помощью сценария можно устанавливать значения переменных среды, указывающих пути поиска, каталоги для временных файлов и другую подобную информацию.

2 Профили пользователей. В профиле пользователя хранятся все настройки рабочей среды компьютера, на котором работает Windows 7, определенные самим пользователем. Это могут быть, например, настройки экрана и соединения с сетью.

3 Сервер сценариев Windows 7. Сервер сценариев независим от языка и предназначен для работы на 32-разрядных платформах Windows 7. Он включает в себя как ядро сценариев Visual Basic Scripting Edition (VBScript), так и JScript. Сервер сценариев Windows предназначен для выполнения сценариев прямо на рабочем столе Windows или на консоли команд. При этом сценарии не надо встраивать в документ HTML.

Профили пользователей

На изолированном компьютере с Windows 7 локальные профили пользователей создаются автоматически. Информация локальных профилей необходима для поддержки настроек рабочего стола локального компьютера, характерных для конкретного пользователя. Профиль создается для каждого пользователя в процессе его первой регистрации в компьютере. Профиль пользователя обладает следующими преимуществами:

При регистрации пользователя в системе рабочий стол получает те же настройки, какие существовали в момент предыдущего выхода пользователя из системы.

Несколько пользователей могут работать на одном и том же компьютере в индивидуальных средах.

Профили пользователей могут быть сохранены на сервере. В этом случае пользователь получает возможность работать со своим профилем при регистрации на любом компьютере сети. Такие профили называются перемещаемыми.

Пользовательские профили можно применять следующим образом:

– создать несколько типов профилей и назначить их определенным группам пользователей. Это позволит получить несколько типов рабочих сред, соответствующих различным задачам, решаемым пользователями.

– назначать общие групповые настройки всем пользователям.

– назначать обязательные профили, какие-либо настройки которых пользователи изменять не могут.

Итак, профили можно классифицировать:

– по месту использования:

а) локальные;

б) перемещаемые;

– по возможности изменения:

а) изменяемые;

б) обязательные;

– по числу использующих данный профиль пользователей:

а) групповой;

б) индивидуальный;

в) профиль по умолчанию (существует на каждом компьютере и при первой регистрации именно он устанавливается для пользователя, а затем в него вносятся все изменения, сделанные пользователем).

Настройки, хранящиеся в профиле пользователя

Профиль пользователя хранит настройки конфигурации и параметры, индивидуально назначаемые каждому пользователю и полностью определяющие его рабочую среду (таблица 2.1).

Структура профиля пользователя

Профиль пользователя представляет собой совокупность файлов и папок с определенными именами, которые нельзя изменять. Каждая папка содержит определенную группу настроек.

Профиль пользователя создается на основе профиля, назначаемого по умолчанию. Он хранится на каждом компьютере, где работает Windows

7. Файл NTuser.dat, находящийся в папке Default User, содержит настройки конфигурации, хранящиеся в реестре Windows. Кроме того, каждый профиль пользователя использует общие программные группы, находящиеся в папке All Users.

Таблица 2.1 – Настройки профиля пользователя

Объект	Соответствующие ему параметры
Windows NT Explorer	Все настройки, определяемые самим пользователем, касающиеся программы Проводник (Windows NT Explorer)
Панель задач	Все персональные группы программ и их свойства, все программные объекты и их свойства, все настройки панели задач.
Настройки принтера	Сетевые соединения принтера
Панель управления	Все настройки, определенные самим пользователем, касающиеся панели управления.
Стандартные	Настройки всех стандартных приложений, запускаемых для конкретного пользователя
Приложения, работающие в ОС Windows 7	Любое приложение, специально созданное для работы в среде Windows 7, может обладать средствами отслеживания своих настроек относительно каждого пользователя. Если такая информация существует, она хранится в профиле пользователя
Электронная подсказка	Любые закладки, установленные в справочной системе Windows 7
Консоль управления Microsoft	Индивидуальный файл конфигурации и текущего состояния консоли управления

Папки профиля пользователя

Как уже говорилось, при создании профиля пользователя используется профиль, назначаемый по умолчанию, находящийся в папке Default User. Папка Default User, папки профилей индивидуальных пользователей, а также папка All Users, находятся в папке Documents and Settings корневого каталога. В папке Default User находятся файл Ntuser.dat и список ссылок на объекты рабочего стола. В приложении 2 перечислены подпапки, находящиеся внутри папки, профиля пользователя, и описано их содержимое.

Папка All Users

Настройки, находящиеся в папке All Users, не копируются в папки профиля пользователя, но используются для его создания. Платформы Windows 7 поддерживают два типа программных групп:

1 Общие программные группы. Они всегда доступны на компьютере, независимо от того, кто зарегистрирован на нем в данный момент. Только администратор может добавлять объекты к этим группам, удалять или модифицировать их.

2 Персональные программные группы. Они доступны только создавшему их пользователю.

Общие программные группы хранятся в папке All Users, находящейся в папке Documents and Settings. Папка All Users также содержит настройки для рабочего стола и меню Пуск. Группы этого типа на компьютерах, где работает Windows, могут создавать только члены группы Администраторы.

Создание локального профиля пользователя

Локальный профиль пользователя хранится на компьютере в папке, имя которой совпадает с именем данного пользователя, находящейся в папке Documents and Settings. Если для данного пользователя не существует сконфигурированный перемещаемый (находящийся на сервере) профиль, то при первой регистрации пользователя в компьютере для него создается индивидуальный профиль. Содержимое папки Default User копируется в папку нового профиля пользователя. Информация профиля вместе с

содержимым папки All Users используется при конфигурации рабочей среды пользователя. При завершении пользователем работы на компьютере все сделанные изменения настроек рабочей среды, выбираемых по умолчанию, записываются в его профиль. Содержимое папки Default User остается неизменным.

Если пользователь имеет отдельную учетную запись на локальном компьютере и в домене, для каждой из них создается свой профиль пользователя, поскольку регистрация на компьютере происходит с помощью различных учетных записей. При завершении работы все сделанные изменения также записываются в соответствующий данной учетной записи профиль.

Папка профиля пользователя на локальном компьютере содержит файл NTuser.dat и файл журнала транзакций с именем NTuser.dat.LOG. Он нужен для обеспечения отказоустойчивости, позволяя Windows восстанавливать профиль пользователя в случае сбоя при модификации содержимого файла NTuser.dat.

Создание сценариев входа

Для создания сценариев входа может быть использован обыкновенный текстовый редактор. Затем с помощью оснастки Локальные пользователи и группы (Local Users and Groups) сценарии входа назначаются соответствующим пользователям. Кроме того, один сценарий может быть назначен нескольким пользователям. В таблице 2.2 приведены параметры, значения которых можно устанавливать с помощью сценария входа и их описания.

Таблица 2.2 - Параметры, устанавливаемые с помощью сценария входа

Параметр	**Описание**
%HOMEDRIVE%	Имя устройства локального компьютера, связанного с домашним каталогом пользователя
%HOMEPATH%	Полный путь к домашнему каталогу пользователя

%HOMESHARE%	Имя общего ресурса, где находится домашний каталог пользователя
%OS%	Операционная система компьютера пользователя
%PROCESSOR_ARCHITECTURE%	Тип процессора (например, Pentium) компьютера пользователя
%PROCESSOR_LEVEL%	Уровень процессора компьютера пользователя
%USERDOMAIN%	Домен, в котором находится учетная запись пользователя
%USERNAME%	Имя пользователя

2.2 Задание к лабораторной работе № 2

1 Создайте консоль управления локальными пользователями и группами. В консоли должна быть создана «Панель задач», позволяющая только создавать нового пользователя и новую группу.

2 Создайте учетные записи для двух разных пользователей:

– для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем;

– к чему приведет отключение учетной записи пользователя? Как определить, какие записи уже отключены.

3 Создайте локальную группу:

– поместите в локальную группу созданных вами пользователей и пользователя Администратор. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя;

– ознакомьтесь с возможностью вызова оснастки «Локальные пользователи и группы» в составе стандартной оснастки «Управление компьюте-

ром» (для этого получите контекстное меню значка «Мой компьютер» и в нем выберите опцию «Управление»).

4 Вызовите утилиту «Учетные записи пользователей» (находится в «Панели управления»):

– посмотрите возможность создания новой учетной записи;

– изучите возможности изменения пароля, значка для учетной записи, способы входа в систему;

– проверьте действенность возможности смены пользователя без закрытия открытых им программ;

– измените тип одной из созданных вами записей с «ограниченной» на административную. Перейдите в оснастку «Локальные пользователи и группы» и убедитесь, что это привело к помещению пользователя в группу Администраторы. Удалите этого пользователя из группы и убедитесь, что учетная запись изменила тип.

5 Работа с профилями пользователей:

– посмотрите, какие в системе существуют профили;

– в какой папке стандартно хранятся профили пользователей, изучите их состав;

– проверьте возможность очистки «Рабочего стола» от всех значков (или, наоборот, появления значков «Мой компьютер», «Сетевое окружение» на «Рабочем столе»);

- посмотрите возможность настройки «Главного меню» (меню «Пуск»).

6 Создайте профиль одному из созданных вами пользователей, скопировав ему профиль Администратора. Профиль создайте не в стандартной папке:

– продемонстрируйте, что профиль действительно активизируется при регистрации пользователя;

– как сделать профиль обязательным. Продемонстрируйте это на примере другого пользователя.

7 Изучите возможность создания сценариев входа в систему.

8 Ознакомьтесь с возможностями и настройкой подсистемы аудита, продемонстрируйте работу аудита на конкретном примере.

2.3 Ход выполнения работы

Создание новой консоли рассмотрим на следующем примере:

1 Нажать сочетание клавиш на клавиатуре «Win+R» введите «mmc» и нажмите кнопку «Enter». Либо Пуск в строке поиска «mmc» и нажать «Enter».

2 В меню «Консоль» выберите пункт «Добавить/удалить оснастку» , после чего откроется окно «Добавить/Удалить оснастку». В этом окне перечисляются изолированные оснастки и оснастки расширения, которые будут добавлены в консоль . Оснастки можно добавлять к корню консоли управления или к уже имеющимся изолированным оснасткам; это указывается в списке «Оснастки». В нашем случае оставим значение по умолчанию – «Корень консоли».

3 Нажмите кнопку «Добавить». На экране появится окно «Добавить изолированную оснастку» со списком изолированных оснасток, имеющихся в системе.

4 Выполните двойной щелчок на пункте «Управление компьютером». Появится окно с конфигурационными опциями для данной оснастки.

5 Оставьте переключатель в положении «Локальный компьютер». Затем нажмите кнопку «Готово».

6 В окне оснасток выберите пункт «Сертификаты» и нажмите кнопку «Добавить».

7 В следующем окне выберите соответствующий переключатель – «Эта оснастка всегда будет управлять сертификатами для: моей учетной записи пользователя».

8 Нажмите кнопки «Готово» и «Закрыть».

9 В окне «Добавить/Удалить оснастку» (где отображен список подключаемых оснасток) перейдите на вкладку «Расширения». На этой вкладке

приведен список оснасток расширения, которые поставляются вместе с выбранными изолированными оснастками. Если вы не собираетесь подключать все оснастки расширения, сбросьте флажок «Добавить все расширения» (который ставится по умолчанию) и снимите флажки с лишних оснасток. По окончании процедуры нажмите кнопку ОК.

10 Закройте окно добавления оснасток, нажав кнопку ОК. Теперь окно консоли содержит две оснастки — «Управление компьютером» и «Сертификаты» (рисунок 2.2).

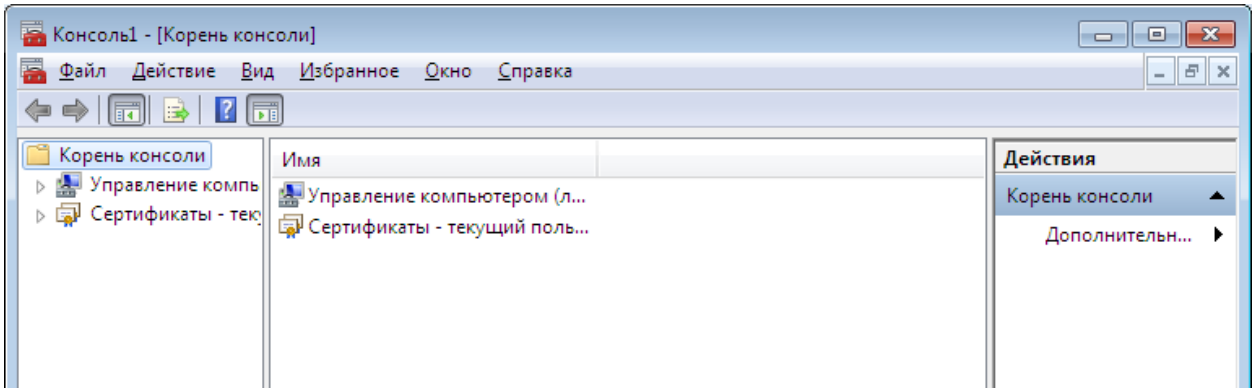

Рисунок 2.2 – Окно консоли

11 Для того чтобы сохранить созданный инструмент, в меню «Консоль» выберите пункт «Сохранить как» и укажите имя файла и папку, в которой будет сохранен файл консоли.

Индивидуальная настройка окон оснасток

После добавления оснасток можно развернуть окна оснасток, чтобы облегчить работу с ними. Для этого выполните следующие действия:

1 В левом подокне (в окне структуры) только что созданной консоли щелкните правой кнопкой мыши на узле «Управление компьютером» и выберите в контекстном меню «Новое окно отсюда». Будет открыто окно «Управление компьютером», представляющее одноименную оснастку.

2 Аналогичные действия выполните для узла «Сертификаты». В новом окне нажмите кнопку «Скрытие или отображение дерева консоли или из-

бранного» на панели инструментов для того, чтобы скрыть панель структуры.

3 Закройте окно, содержащее корень консоли.

4 В меню «Окно» выберите команду «Сверху вниз». Консоль будет выглядеть, как показано на рисунке 2.3.

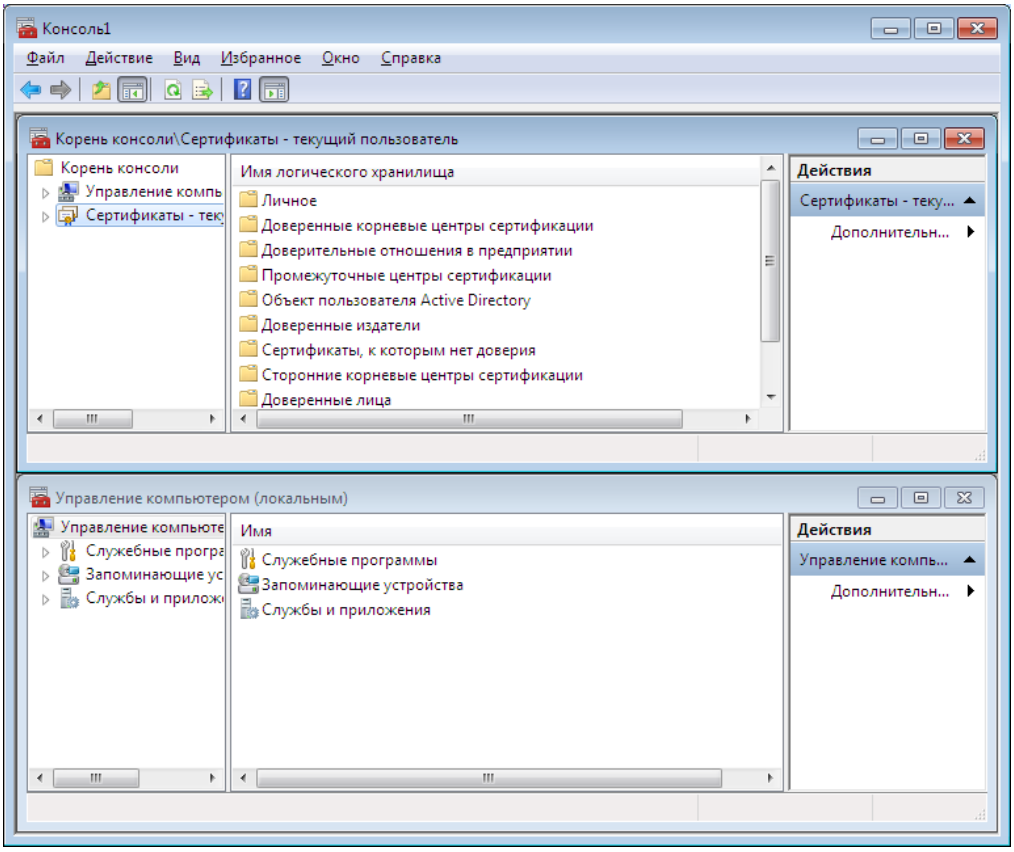

Рисунок 2.3 – Окно консоли (Сертификаты)

Создание панелей задач

Когда требуется создать файл консоли для другого пользователя, полезно предоставить пользователю упрощенный инструмент, позволяющий выполнять только несколько определенных задач. Таким инструментом является панель задач. Панель задач является HTML-страницей, на которой могут быть размещены ярлыки, запускающие команды меню и программы или открывающие ссылки на web-страницы.

Для создания панели задач выполните следующее:

1 В меню «Действие» или в контекстном меню любого узла в окне консоли выберите пункт «Новый вид панели задач».

2 Откроется окно «Мастера создания вида панели задач». Нажмите кнопку «Далее».

В следующем окне мастера будет предложено выбрать стиль отображения и размер панели задач. Затем на панели задач можно указать использование только тех задач, которые связаны с текущим узлом или со всеми узлами дерева. В следующем окне потребуется ввести имя и описание создаваемой панели задач.

Если не требуется добавлять новые задачи на созданную панель, снимите в последнем окне мастера флажок «Запустить мастер создания новой задачи».

В противном случае по завершении работы «Мастера создания вида панели задач» запускается «Мастер создания задач». В ходе этой процедуры следует указать функцию задачи: запуск команды меню, программы или ссылка на web-страницу, ввести путь к исполняемому файлу и параметры запуска.

В остальных окнах мастера примите значения по умолчанию. Если требуется создать несколько задач на одной панели, установите в последнем окне мастера флажок «Запустить этот мастер снова». Затем нажмите кнопку «Готово».

На рисунке 2.4 показана созданная в результате панель задач. В данном окне консоли панель структуры отключена — аналогично тому, как это было сделано в предыдущем разделе. Для удаления лишних меню и панелей инструментов снимите соответствующие флажки в окне «Настройка вида». Если вы хотите еще ужесточить требования, то можете выбрать один из режимов ограничения – «Пользовательский режим – ограниченный допуск».

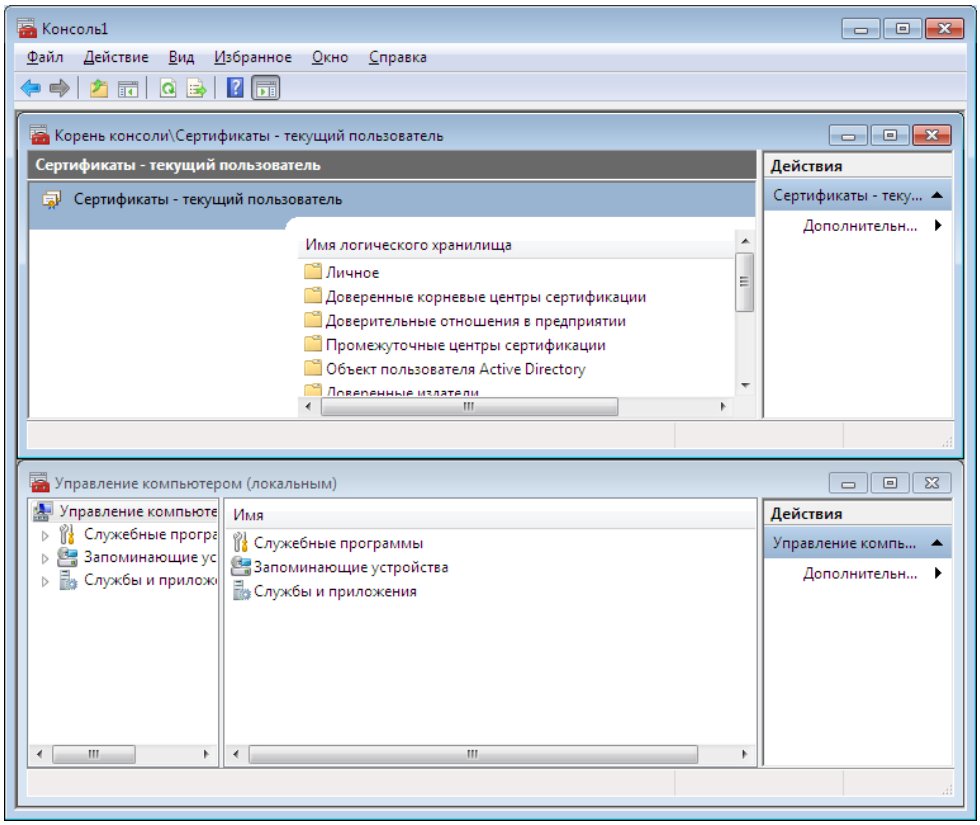

Рисунок 2.4 – Окно консоли

3 Сохраните файл.

Сохраненный файл консоли можно также открыть с помощью Проводника. Для этого выполните двойной щелчок на файле с расширением .msc. Файл консоли будет открыт в среде MMC.

Оснастки Windows 7

В приложении 1 в алфавитном порядке перечислены основные оснастки, которые доступны в системе Windows 7. Для оснасток, включенных в пользовательский интерфейс, указаны названия соответствующих пунктов меню, для остальных оснасток даны их собственные имена. Оснастки, которые можно вызывать непосредственно из меню «Пуск» или из группы «Администрирование» на панели управления, т.е. оснастки, включенные в пользовательский интерфейс при инсталляции системы – отмечены звездочкой.

Типовые задачи администрирования

Создание локальных учетных записей пользователей и групп

Создание учетных записей пользователей и групп занимает важное место в обеспечении безопасности Windows 7, поскольку, назначая им пра-

ва доступа, администратор получает возможность ограничить пользователей в доступе к конфиденциальной информации, разрешить или запретить им выполнить в сети определенное действие, например, архивацию данных или завершение работы компьютера. Обычно право доступа ассоциируется с объектом – файлом или папкой. Оно определяет возможность данного пользователя получить доступ к объекту.

Оснастка «Локальные пользователи и группы

Оснастка Локальные пользователи и группы - это инструмент MMC, с помощью которого выполняется управление локальными учетными записями пользователей и групп – как на локальном, так и на удаленном компьютерах. С ним можно работать на рабочих станциях и автономных серверах Windows 7, как на изолированных, так и рядовых членах домена. На контроллерах домена Windows 7 инструмент Локальные пользователи и группы недоступен, поскольку все управление учетными записями и группами в домене выполняется с помощью оснастки Пользователи и компьютеры Active Directory.

Окно изолированной оснастки «Локальные пользователи и группы» выглядит аналогично показанному на рисунке 2.5.

Папка Пользователи

Сразу после установки системы Windows 7 (рабочей станции или сервера, являющегося членом домена) папка «Пользователи» содержит две встроенные учетные записи – «Администратор» и «Гость». Они создаются автоматически при установке Windows 7. Ниже даны описания свойств обеих встроенных учетных записей:

Администратор – эту учетную запись используют при установке и настройке рабочей станции или сервера, являющегося членом домена. Она не может быть уничтожена, блокирована или удалена из группы Администраторы, ее можно только переименовать.

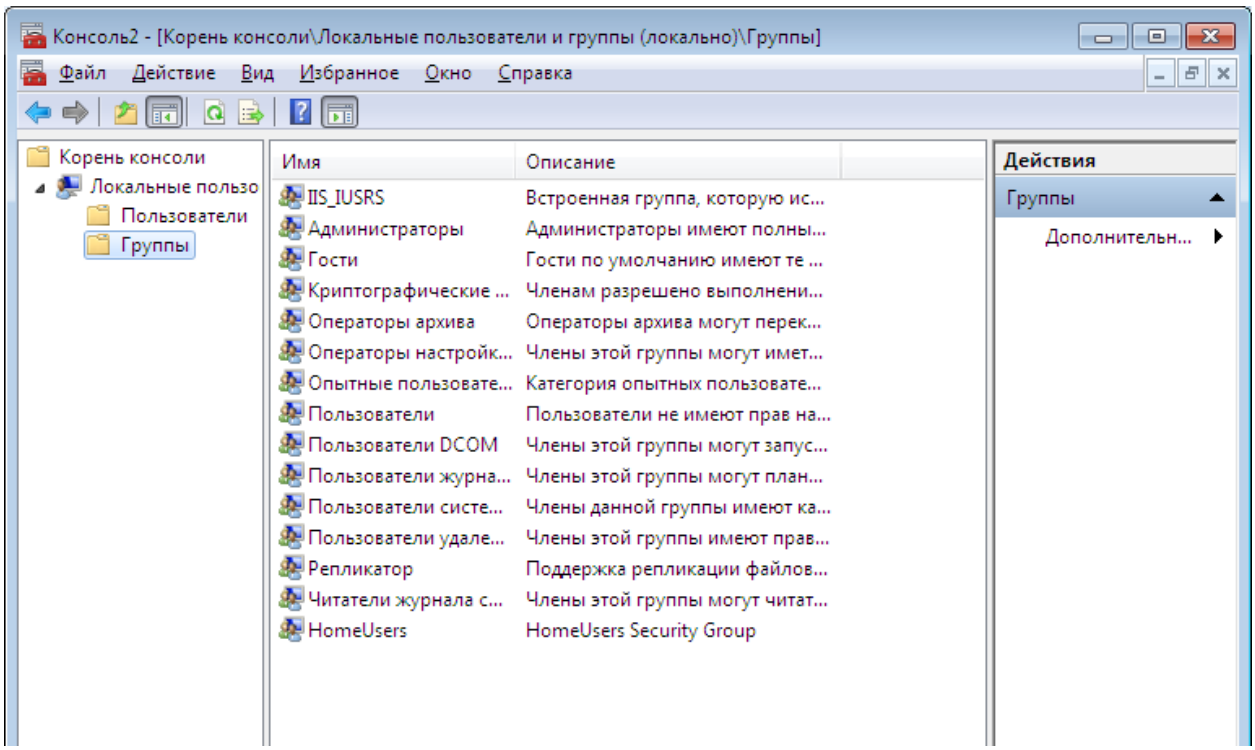

Рисунок 2.5 – Окно консоли (локальные пользователи и группы)

Гость – эта учетная запись применяется в компьютере без использования специально созданной учетной записи. Учетная запись Гость не требует ввода пароля и по умолчанию блокирована.

Папка Группы

После установки системы Windows 7 (рабочей станции или сервера, являющегося членом домена) папка «Группы» содержит шесть встроенных групп. Они создаются автоматически при установке Windows 7. Ниже описаны свойства всех встроенных групп:

– **Администраторы** – ее члены обладают полным доступом ко всем ресурсам системы;

– **Операторы архива** – члены этой группы могут архивировать и восстанавливать файлы в системе независимо от того, какими правами эти файлы защищены;

– **Гости** – эта группа позволяет выполнить регистрацию пользователя с помощью учетной записи Гость и получить ограниченные права на доступ к ресурсам системы;

– **Опытные пользователи**– члены этой группы могут создавать учетные записи пользователей, но они имеют право модифицировать настройки безопасности только для созданных ими учетных записей;

– **Репликатор** – членом группы Репликатор должна быть только учетная запись, с помощью которой можно зарегистрироваться в службе репликации контроллера домена;

– **Пользователи** – члены этой группы могут выполнять большинство пользовательских функций, например, запускать приложения, пользоваться локальным или сетевым принтером, завершать работу системы или блокировать рабочую станцию.

Управление учетными записями

В качестве примера использования оснастки «Локальные пользователи и группы» для работы с учетными записями рассмотрим процедуру создания пользовательской учетной записи.

Для создания учетной записи:

1 В оснастке «Локальные пользователи и группы» установите указатель на папку «Пользователи» и нажмите правую кнопку. В контекстном меню выберите команду «Новый пользователь».

Появится окно диалога «Новый пользователь». В поле «Пользователь» введите имя создаваемого пользователя. В поле «Полное имя» введите полное имя создаваемого пользователя. В поле «Описание» введите описание создаваемого пользователя или его учетной записи. В поле «Пароль» введите пользователя и в поле «Подтверждение», подтвердите его правильность вторичным вводом. Длина пароля не может превышать 14 символов.

Установите или снимите флажки «Потребовать смену пароля при следующем входе в систему», «Запретить смену пароля пользователем», «Срок пароля не ограничен» и «Отключить учетную запись».

Чтобы создать еще одного пользователя, нажмите кнопку «Создать» и повторите шаги с 1 по 3. Для завершения работы нажмите кнопку «Создать» и затем «Закрыть».

Имя пользователя должно быть уникальным для компьютера. Оно должно содержать до 20 символов верхнего и нижнего регистра.

Изменение и удаление учетных записей

Изменять, переименовывать и удалять учетные записи можно с контекстного меню, вызываемого щелчком правой кнопки мыши на имени пользователя, либо – меню «Действие» на панели меню оснастки «Локальные пользователи и группы» (при этом в правом подокне оснастки должна быть выбрана модифицируемая или удаляемая учетная запись пользователя).

Управление локальными группами

Для создания локальной группы:

1 В окне оснастки «Локальные пользователи и группы» установите указатель мыши на папке «Группы» и нажмите правую кнопку. В появившемся контекстном меню выберите команду «Новая группа».

2 В поле «Имя группы» введите имя новой группы.

3 В поле «Описание» введите описание новой группы.

4 В поле «Члены группы» можно сразу же добавить пользователей и группы, которые войдут в данную группу: для этого нужно нажать кнопку «Добавить» и выбрать их в списке.

5 Для завершения нажмите кнопку «Создать» и затем «Закрыть».

Имя локальной группы должно быть уникальным в пределах компьютера, может содержать до 256 символов в верхнем и нижнем регистрах. В имени группы запрещено применение символа обратного слэша (\).

Изменение членства в локальной группе

Чтобы добавить или удалить учетную запись пользователя из группы:

1 В окне оснастки «Локальные пользователи» и группы щелкните на папке «Группы».

2 В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку. В появившемся контекстном меню выберите команду «Добавить» в группу или «Свойства».

3 Для того чтобы добавить новые учетные записи в группу, нажмите кнопку «Добавить». Далее следуйте указаниям окна диалога Выбор: «Пользователи» или «Группы».

4 Для того чтобы удалить из группы некоторых пользователей, в поле «Члены группы» окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку «Удалить».

В локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и глобальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах.

Аудит локальной системы

Аудит – это процесс, позволяющий фиксировать события, происходящие в операционной системе и имеющие отношение к безопасности. Например, попытки создать объекты файловой системы, получить к ним доступ или удалить их. Информация о подобных событиях заносится в файл журнала событий операционной системы.

После включения аудита операционная система Windows начинает отслеживать события, связанные с безопасностью. Полученную в результате информацию можно просмотреть с помощью оснастки «Просмотр событий». В процессе настройки аудита необходимо указать, какие события должны быть отслежены. Информация о них помещается в журнал событий. Каждая запись журнала хранит данные о типе выполненного действия, пользователе, выполнившем его, а также о дате и моменте времени выполнения данного действия. Аудит позволяет отслеживать как успешные, так и неудачные попытки выполнения определенного действия, поэтому при просмотре журнала событий можно выяснить, кто предпринял попытку выполнения неразрешенного ему действия.

Аудит представляет собой многошаговый процесс. Сначала его следует активизировать с помощью оснастки «Групповая политика». По умолчанию аудит отключен, поскольку он снижает производительность системы.

После включения аудита необходимо определить набор отслеживаемых событий. Это могут быть, например, вход и выход из системы, попытки получить доступ к объектам файловой системы и т. д. Затем следует указать, какие конкретно объекты необходимо подвергнуть аудиту и включить его с помощью «Редактора списков управления доступом», ACL.

Аудит, установленный для родительской папки, автоматически наследуется всеми вновь созданными дочерними папками и файлами. Этого можно избежать, если при создании файла или папки вызвать окно свойств и на вкладке «Аудит» снять флажок «Переносить наследуемый от родительского объекта аудит на этот объект». Если же этот флажок отображен серым цветом или кнопка «Удалить» недоступна, это значит, что настройки аудита уже унаследованы. В этом случае для изменения настроек аудита дочерних объектов нужно изменить настройки аудита родительской папки, и они будут наследоваться всеми дочерними объектами.

Активизация аудита с помощью оснастки «Групповая политика».

Для активизации аудита на изолированном компьютере:

1 Запустите оснастку «Групповая политика» (это изолированная оснастка, которую можно использовать как самостоятельный инструмент). (Можно выполнить команду Пуск | Программы | Администрирование | Локальная политика безопасности.)

2 Откройте папку «Конфигурация компьютера» и последовательно раскройте узлы «Конфигурация Windows», «Параметры безопасности», «Локальные политики», «Политика аудита».

3 На правой панели появится список политик аудита. По умолчанию все они имеют значение «Нет аудита». Для включения аудита следует изменить значения нужных параметров.

4 Выполните двойной щелчок на устанавливаемой политике аудита. Появится окно диалога, с помощью которого можно разрешить аудит. В группе «Вести аудит следующих попыток доступа» установите флажки «Успех» или «Отказ», или оба.

5 Нажмите кнопку ОК.

Настройка и просмотр аудита файлов и папок.

Чтобы настроить, просмотреть или изменить настройки аудита файлов и папок:

1 Установите указатель мыши на файл или папку, для которой следует выполнить аудит, и нажмите правую кнопку. В появившемся контекстном меню выберите команду Свойства. В окне свойств папки или файла перейдите на вкладку «Безопасность».

2 На вкладке «Безопасность» нажмите кнопку «Дополнительно» и затем перейдите на вкладку «Аудит».

3 Если необходимо настроить аудит для нового пользователя или группы, на вкладке «Аудит» нажмите кнопку «Добавить». Появится диалоговое окно «Выбор: Пользователь, Компьютер или Группа». Выберите имя нужного пользователя или группы и нажмите кнопку ОК. Откроется окно диалога «Элемент аудита для». Здесь вы сможете ввести все необходимые параметры аудита. В списке «Применить» укажите, где следует выполнять аудит (это поле ввода доступно только для папок). В группе «Доступ» следует указать, какие события следует отслеживать: окончившиеся успешно, неудачно или оба типа событий. Флажок «Применять этот аудит к объектам и контейнерам только внутри этого контейнера» определяет, распространяются ли введенные вами настройки аудита на файлы и папки, находящиеся ниже по дереву каталогов файловой системы (флажок не установлен). В обратном случае установите флажок (или выберите в списке «Применять» опцию «Только для этой папки»). Это позволит не выполнять аудит для тех объектов файловой системы, которые не представляют интереса. После завершения настройки аудита для папки или файла нажмите несколько раз кнопку ОК, чтобы закрыть все окна диалога.

4 Если вы хотите просмотреть или изменить настройки аудита для уже существующего пользователя или группы, нажмите кнопку «Показать/Изменить». Появится окно диалога «Элемент аудита для». Здесь вы

сможете выполнить все необходимые изменения параметров аудита для выбранного вами пользователя или группы. По окончании внесения изменений нажмите кнопку ОК.

Отключение аудита файлов и папок.

Для отключения аудита файла или папки:

1 Установите указатель мыши на файл или папку, где необходимо отключить аудит, и нажмите правую кнопку. В появившемся меню выберите команду «Свойства». Появится окно свойств файла или папки. Перейдите на вкладку «Безопасность».

2 На вкладке «Безопасность» нажмите кнопку «Дополнительно». В появившемся окне диалога выберите кнопку «Аудит».

3 В поле «Элементы аудита» выберите нужную запись и нажмите кнопку «Удалить». Соответствующая запись будет удалена.

4 Если кнопка «Удалить» недоступна, это значит, что настройки аудита наследуются от родительской папки.

2.4 Контрольные вопросы

1. Для чего предназначена консоль управления?
2. Какие виды пользователей существуют?
3. Что такое групповая политика?
4. Объясните понятие аудита.
5. Из чего состоит и для чего нужен сценарий входа в систему?

3 Доступ к файлам и папкам

Цель работы: получить навыки манипулирования доступа к файлам и папкам.

3.1 Основные понятия

Основа системы безопасности Windows 7 – это файловая система NTFS, поддерживающая безопасность системы на уровне отдельных файлов. На любом дисковом томе, отформатированном для NTFS, во всех папках и файлах имеются списки контроля доступа, или ACL. Списки контроля доступа содержат перечень пользователей и групп, которым разрешен доступ к файлу или папке, а также действий, которые эти пользователи и группы могут совершить с папками.

Стандартные типы разрешений

Есть шесть стандартных типов разрешения, которые применяются к файлам и папкам в Windows 7:

- полный доступ;
- изменять;
- прочитайте и выполните;
- список содержимого папки;
- читать;
- запись.

Каждый уровень представляет собой отдельный набор действий, которые могут выполнять пользователи (таблица 3.1).

Для папок вы также можете установить собственные уникальные разрешения или создать вариацию на любом из стандартных уровней разрешений. В каждом из уровней разрешений множество возможных вариаций. Для получения информации о некоторых из этих дополнительных параметров, обратитесь к Advanced уровню разрешений папки. В следующей таблице представлены доступные стандартные типы разрешений.

Таблица 3.1 – Стандартные типы разрешений

Разрешение	Описание
Полный доступ	Разрешения пользователя (ей): просмотр имен файлов и подпапок перейти к вложенным папкам просматривать данные в файлы папки добавлять файлы и подпапки в папке изменять файлы папки удалите папку и файлы изменение разрешений взять на себя ответственность папки и файлы
Изменять	Разрешения пользователя (ей): просмотреть имена файлов и вложенных папок перейти к вложенным папкам просматривать данные в файлы папки добавлять файлы и подпапки в папке изменять файлы папки удалите папку и файлы
Прочитайте и выполните	Разрешения пользователя (ей): просмотреть имена файлов и вложенных папок перейти к вложенным папкам просматривать данные в файлы папки добавлять файлы и подпапки в папке
Список содержимого папки	Разрешения пользователя (ей): просмотреть имена файлов и вложенных папок перейти к вложенным папкам просмотра папок не разрешать доступ к файлам папки
Читать	Разрешения пользователя (ей): просмотреть имена файлов и вложенных папок перейти к вложенным папкам запуск приложений открытые файлы копировать и просматривать данные в файлы папки
Запись	Разрешениями на чтение, а также позволяет пользователю (ы): создавать папки добавлять новые файлы открывать и изменять файлы удалите файлы

3.2 Задание к лабораторной работе № 3

1. Настроить доступ к папке и файлам.

2. Настроить разрешение доступа к папке и файлам.

3 Включить шифрование содержимого папки.

3.3 Ход выполнения работы

Чтобы настроить разрешения доступа, в первую очередь следует включить вкладку «Безопасность» для окна свойств файлов. Для этого откройте окно «Мой компьютер», нажать на «ALT» , «Панель инструментов» или окно программы Проводник, после чего выберите в строке меню команду «Сервис > Параметры папок». Затем перейти на вкладку «Вид» и снять флажок «Использовать мастер общего доступа» (рисунок 3.1).

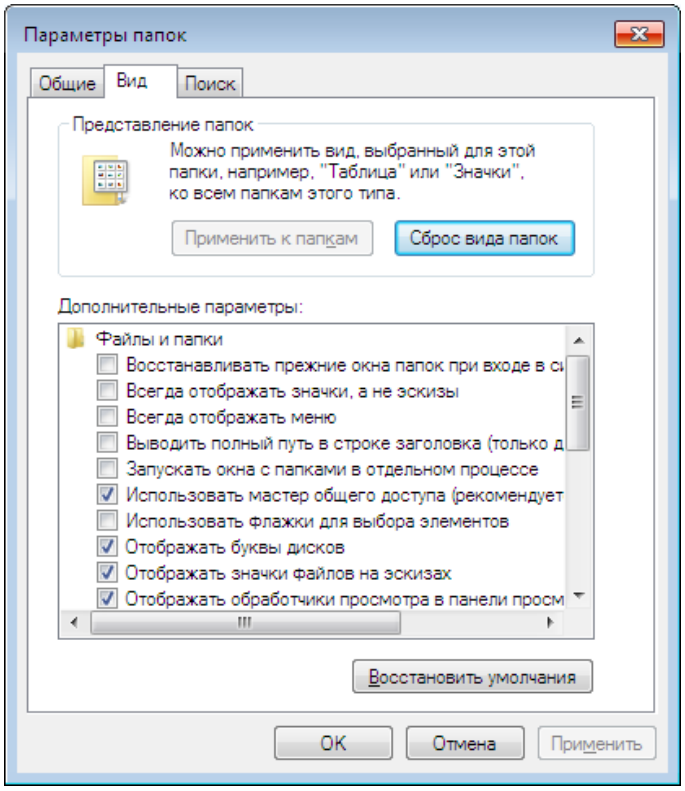

Рисунок 3.1 – Параметры папок

Чтобы указать разрешения «ACL» для файлов и папок, можно использовать любой файловый менеджер, такой как программа «Проводник

Windows» или «Total Commander». Щелкните правой кнопкой мыши на значке папки или файла и выберите команду «Свойства». В открывшемся окне перейдите на вкладку «Безопасность» (рисунок 3.2).

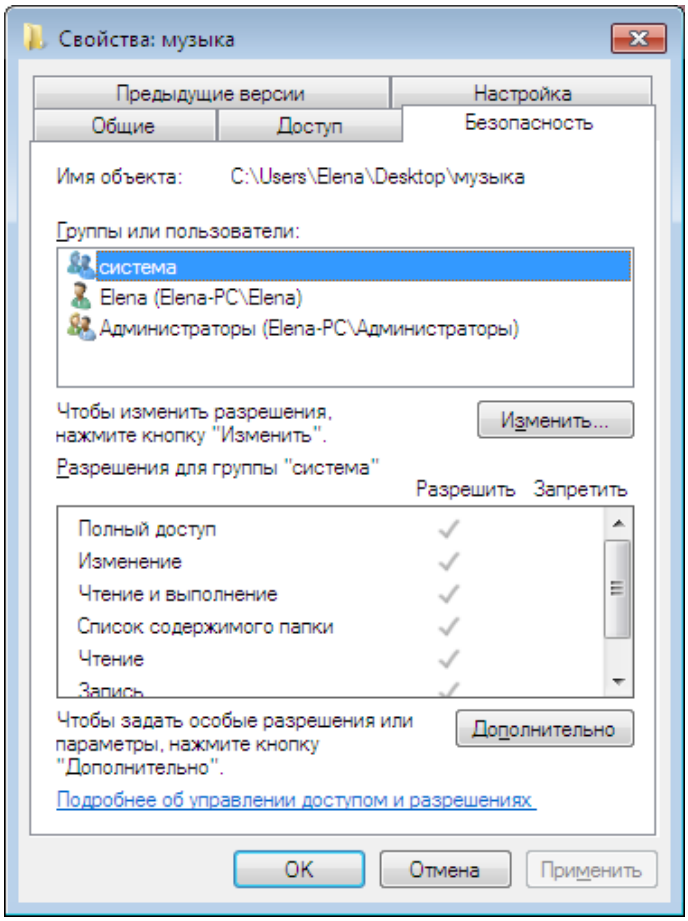

Рисунок 3.2 – Свойства папки музыка

Далее нажать кнопку «Изменить и применить».

Настройка доступа к файлам

Рассмотрим, каким образом можно назначать разрешения доступа для файла с использованием вкладки «Безопасность».

В верхней части окна представлен список пользователей и групп, которым уже определены разрешения для данного файла. Вы можете либо выбрать пользователя и изменить установленные для него разрешения, либо добавить или удалить пользователя (или группу пользователей), что можно сделать с помощью кнопок «Изменить - Добавить и Удалить» (рисунок 3.3).

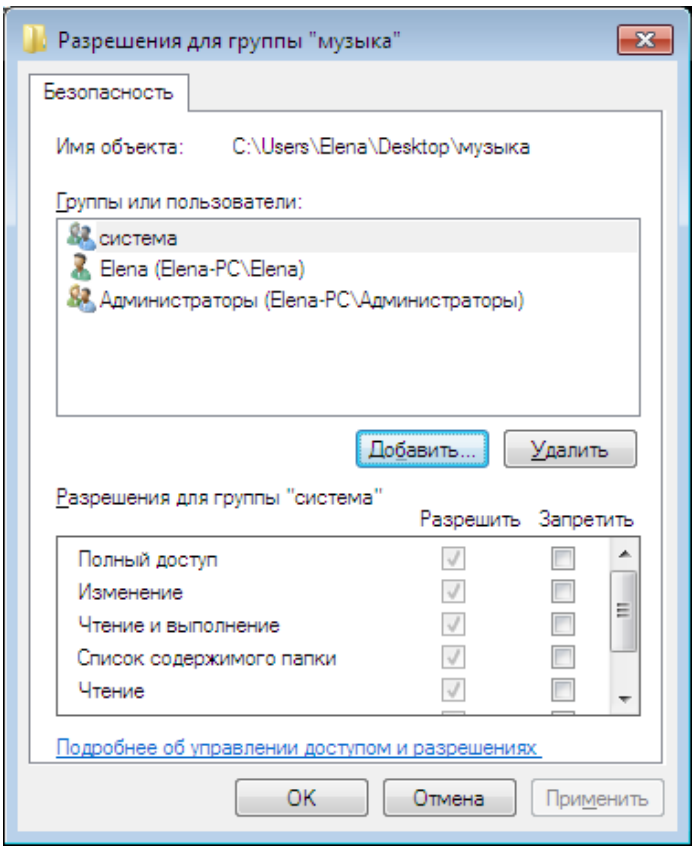

Рисунок 3.3 – Разрешения для группы музыка

Щелкните на кнопке «Добавить» для добавления пользователя. В открывшемся окне «Выбор: Пользователи или Группы» введите имя пользователя или группы в поле «Введите имена выбираемых объектов». Вы должны знать точное имя пользователя или группы. Введя имя пользователя или группы, щелкните «Проверить имена», чтобы удостовериться в существовании такого пользователя или группы. Тип вводимого объекта можно указать, щелкнув на кнопке «Тип объектов» (рисунок 3.4).

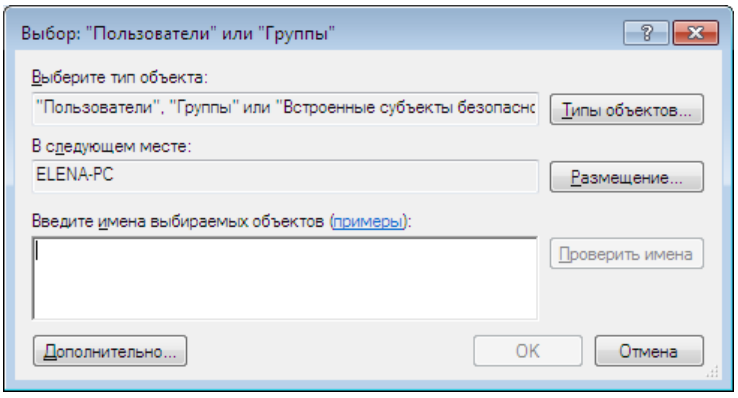

Рисунок 3.4 – Выбор типа объекта

Если пользователь не был обнаружен, щелкните в окне, показанном выше, на кнопке «Дополнительно» и в открывшемся окне – на кнопке «Поиск». При этом в нижней части окна будет представлен список всех групп и пользователей, зарегистрированных в Windows. Выберите в этом списке нужного пользователя или группу и щелкните на кнопке «OK» (рисунок 3.5).

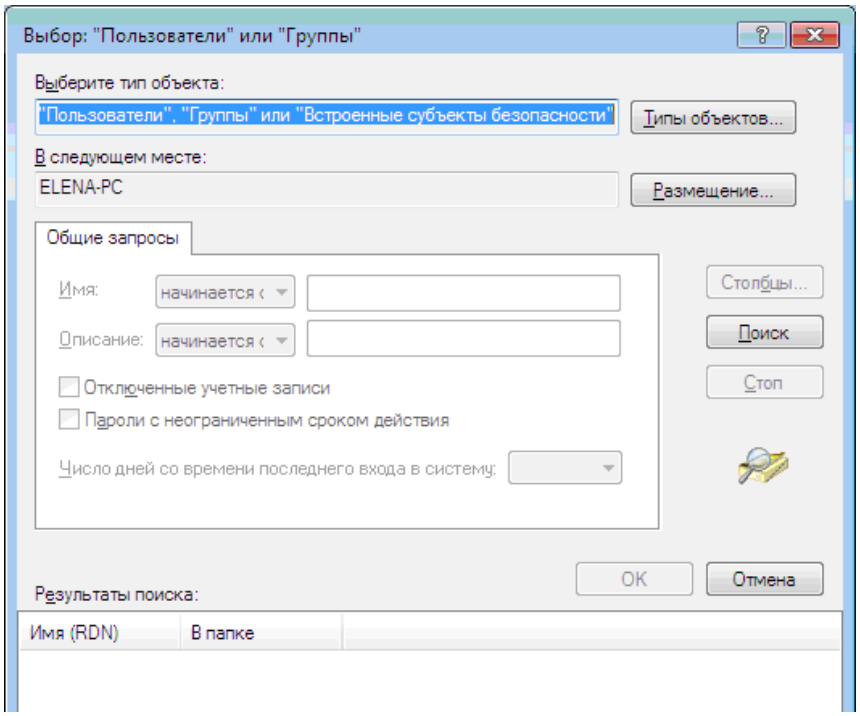

Рисунок 3.5 – Поиск пользователя или группы

На вкладке «Безопасность» окна свойств файла, в поле «Группы» или «Пользователи» нужно выбрать имя пользователя или группы, а в нижней части окна следует установить флажок «Разрешить» или «Запретить».

При указании разрешения «Полный доступ» автоматически устанавливаются флажки все «Разрешить» для выбранного пользователя или группы.

Если флажок «Разрешить» или «Запретить» не установлен, это по умолчанию фактически выбран режим «Запретить». Если разрешение не определено, то оно, наследуется от родительской папки, в которой содержится файл. Если доступ к папке предоставлен, а к файлу, расположенному в папке, разрешение не указано, то оно будет унаследовано от папки и доступ к файлу

будет разрешен. Поэтому, чтобы запретить доступ к файлу, нужно установить флажок «Запретить» непосредственно для файла.

Разрешения доступа к папкам

Общий принцип назначения разрешений доступа к папкам - тот же, что и при выполнении аналогичной процедуры для файлов. Рассмотрим пример.

Щелкните правой кнопкой мыши на нужной папке и выберите команду «Свойства» после чего перейдите на вкладку «Безопасность».

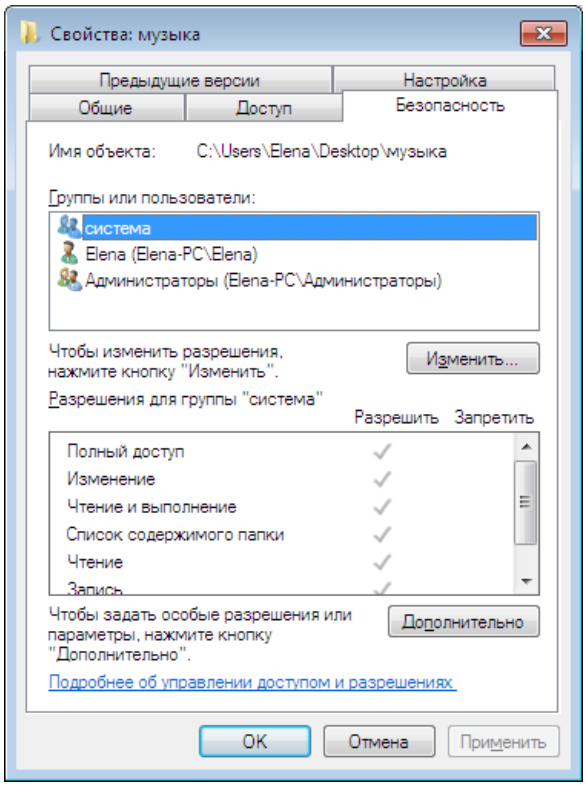

Рисунок 3.6 – Свойства папки музыка

В верхней области окна представлен список пользователей и групп пользователей, для которых уже настроено разрешение доступа к выбранной папке. Теперь можно выбрать пользователя, чтобы изменить установленные для него разрешения, либо добавить или удалить пользователя (группу пользователей) с помощью кнопок «Добавить» или «Удалить». При этом список стандартных разрешений для папок несколько отличается от списка стандартных разрешений для файлов.

Точно так же, как и для файлов, процесс назначений разрешений происходит методом установки или снятия флажков области окна «Разрешения». Для того чтобы назначить разрешения с использованием дополнительных параметров, щелкните на кнопке «Дополнительно».

В открывшемся окне выберите пользователя или группу и щелкните на кнопке «Изменить разрешения» (рисунок 3.7).

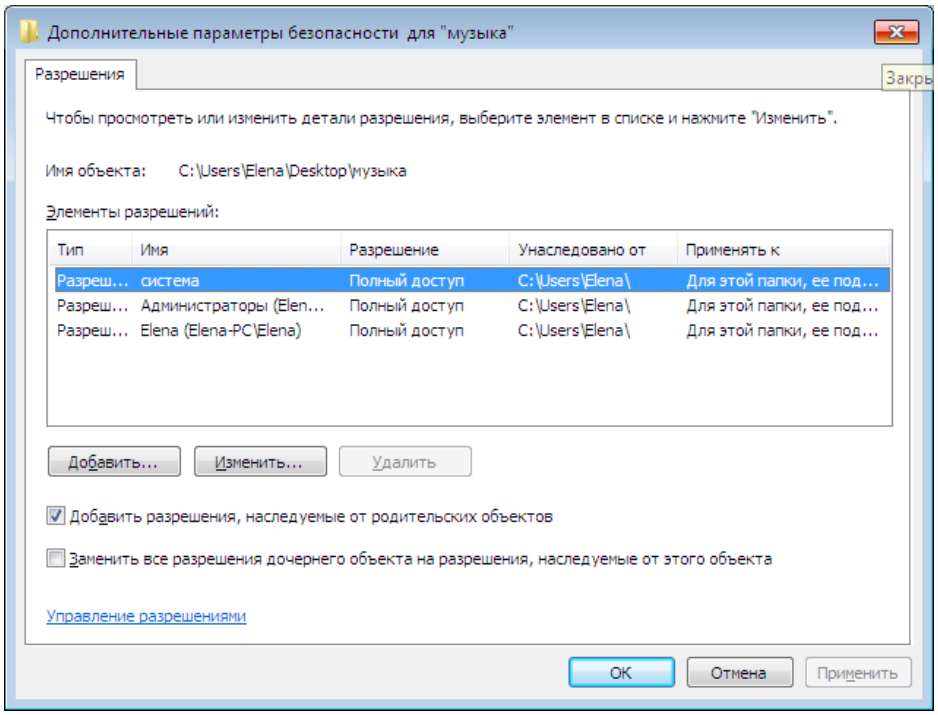

Рисунок 3.7 – Дополнительные параметры безопасности

В новом окне будет представлен список расширенных разрешений доступа к папке (рисунок 3.8). В раскрывающемся списке «Применять» можно указать область действия специальных разрешений для папки:

- только для этой папки;
- для этой папки, ее подпапок и файлов;
- для этой папки и ее подпапок;
- для этой папки и ее файлов;
- только для подпапок и файлов;
- только для подпапок;
- только для файлов.

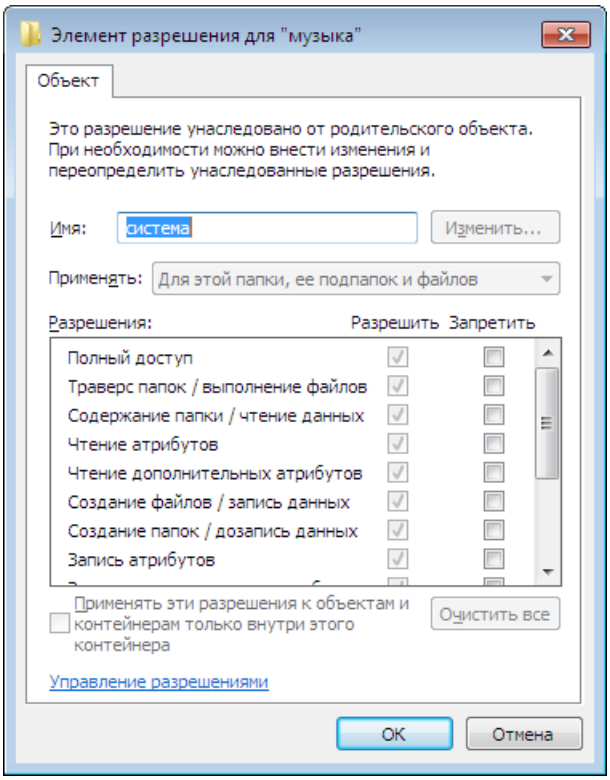

Рисунок 3.8 – Список расширенных разрешений доступа к папке

Установите флажок «Применять эти разрешения к объектам и контейнерам только внутри этого контейнера», чтобы заданные разрешения распространялись только на вложенные папки, но не на вложенные в них папки и другие вложенные объекты.

Наследование разрешений

Концепция наследования разрешений имеет важное значение для системы безопасности Windows 7. Наследование означает, что для файлов или папок могут использоваться не собственные разрешения, а разрешения, назначенные для папки, в которой расположены эти файлы и папки.

Вы создали папку «Музыка», для которой были указаны определенные разрешения доступа. По умолчанию любые папки, которые будут созданы в папке «Музыка» (т.е. вложенные папки), а также все файлы, содержащиеся в самой папке «Музыка» или расположенных в ней подпапках, будут иметь те же разрешения доступа, что и папка «Музыка». Если вложенным папкам будут присвоены другие разрешения, то они будут объединены с разрешениями папки «Музыка». В результате параметры доступа к вложенной папке будут

представлять собой набор из разрешений доступа, назначенных для этой папки и разрешений, наследованных от папки «Музыка».

Необходимо отменить наследование разрешений родительской папки для некоторых вложенных файлов и папок. Перейдите на вкладку «Безопасность» данной папки и щелкните на кнопке «Дополнительно». Снимите флажок «Добавить разрешения, наследуемые от родительских объектов».

При этом на экране появится окно предупреждения, в котором нужно щелкнуть на кнопке «Добавить» (рисунок 3.9).

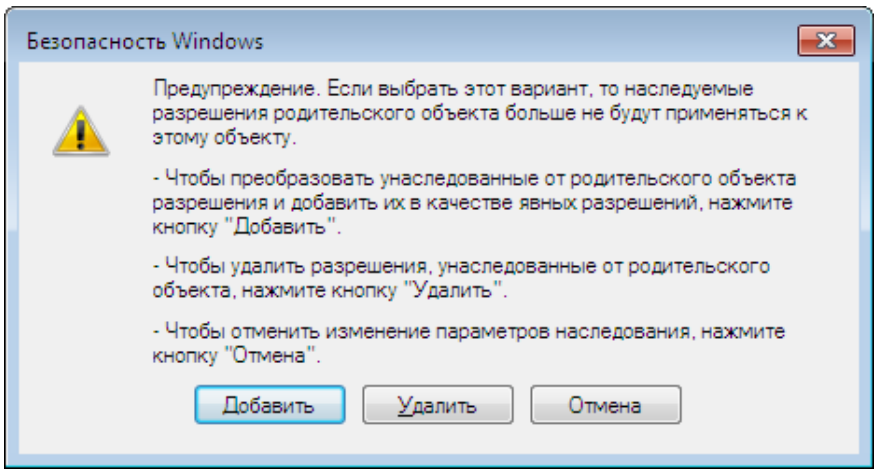

Рисунок 3.9 – Безопасность Windows

Выберите нужного пользователя или группу и щелкните на кнопке «Изменить».

В области применять выберете значение «Только для этой папки», после чего в поле «Разрешения» указать все необходимые разрешения доступа (рисунок 3.10).

Также может возникнуть вопрос отмены наследования разрешений родительской папки для всех вложенных файлов и (или) папок.

Для этого необходимо перейти на вкладку «Безопасность» конкретного файла или папки, щелкнуть на кнопке «Дополнительно» и в появившемся окне «Дополнительные параметры безопасности» и снимите флажок «Доба-

вить разрешения, наследуемые от родительских объектов», добавляя их к явно заданным в этом окне.

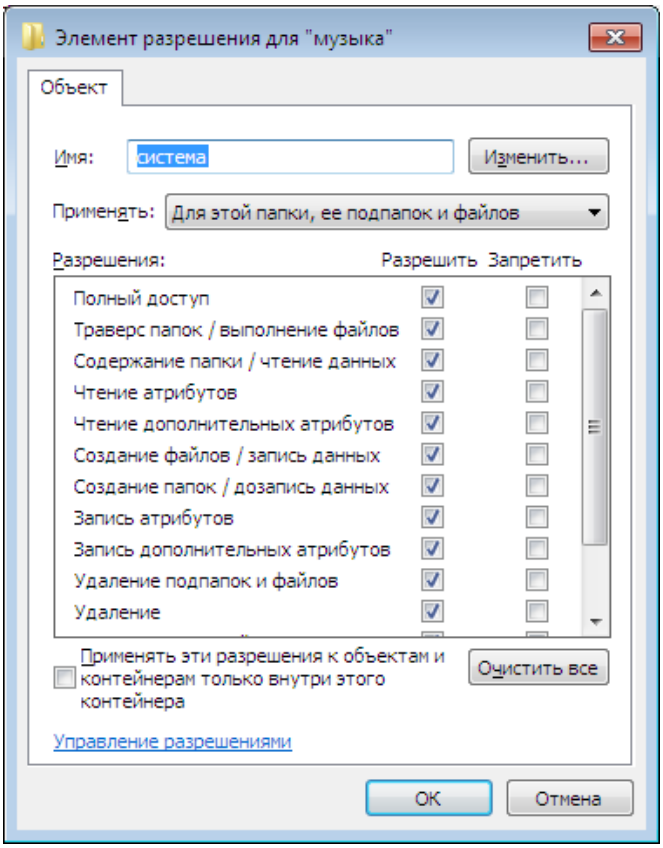

Рисунок 3.10 – Элемент разрешения для папки музыка

Для того чтобы разобраться в типах разрешений, назначенных файлам и папкам, необходимо перейти на вкладку «Безопасность» в окне свойств файла или папки. Флажки для всех разрешений, присвоенных благодаря функции наследования, будут выделены серым цветом и недоступны для выбора. Это позволяет определить, какие разрешения были заданы непосредственно на уровне файлов и папок, а какие наследуются от родительской папки.

Шифрованная файловая система (EFS)

Windows 7 включает в себя шифрованную файловую систему (EFS), которая позволяет пользователям шифровать и расшифровывать файлы, которые хранятся на томе NTFS. С помощью EFS, папки и файлы хранятся защищено от злоумышленников, которые могут получить несанкционирован-

ный физический доступ к устройству, например, кражи компьютера или съемного диска.

EFS использует процесс, известный как шифрование с открытым ключом. В шифровании с открытым ключом, пользователь имеет 2 ключа: открытый ключ, известный также как сертификат и закрытый ключ. Открытый ключ доступен для всех. Пользователи могут использовать открытый ключ для шифрования данных. Секретный ключ хранится в личном хранилище сертификатов пользователя. Закрытый ключ расшифровывает данные, которые были зашифрованы с использованием открытого ключа. Первый раз, когда пользователь шифрует файлы на компьютере под управлением Windows 7, компьютер создает EFS сертификат и закрытый ключ. Это позволяет зашифровать данные на внешнем жестком диске. EFS шифрование работает так, что если пользователь имеет доступ на чтение файлов на флэш-накопителе, он не может на самом деле открыть файл, если не имеет соответствующий сертификат шифрования.

Вы можете зашифровать файл с EFS с помощью следующих шагов:

– щелкните правой кнопкой мыши папку или файл, который вы хотите зашифровать, и выберите пункт «Свойства»;

– перейдите на вкладку «Общие» и нажмите кнопку «Другие….»;

– выберите «Шифровать содержимое для защиты данных» поле, а затем нажмите кнопку «ОК» (рисунок 3.11, 3.12).

Зашифрованные значки файлов окрашены в зеленый цвет в Windows Explorer. Чтобы расшифровать файлы и папки, просто следуйте инструкциям, приведенным выше, но снимите флажок «Шифровать содержимое для защиты данных» флажок.

Если зашифрованный файл должен быть общим с другим пользователем на одном компьютере, они должны экспортировать свой EFS сертификат. Затем нужно импортировать его и добавить сертификат в общий файл.

Когда вы зашифруете папку или файл, вы должны создать резервную копию сертификата шифрования. Если ваш сертификат и ключ потерян или

поврежден, и вы не имеете резервной копии, вы не сможете получить доступ к папкам и файлам, что у вас в зашифрованном виде.

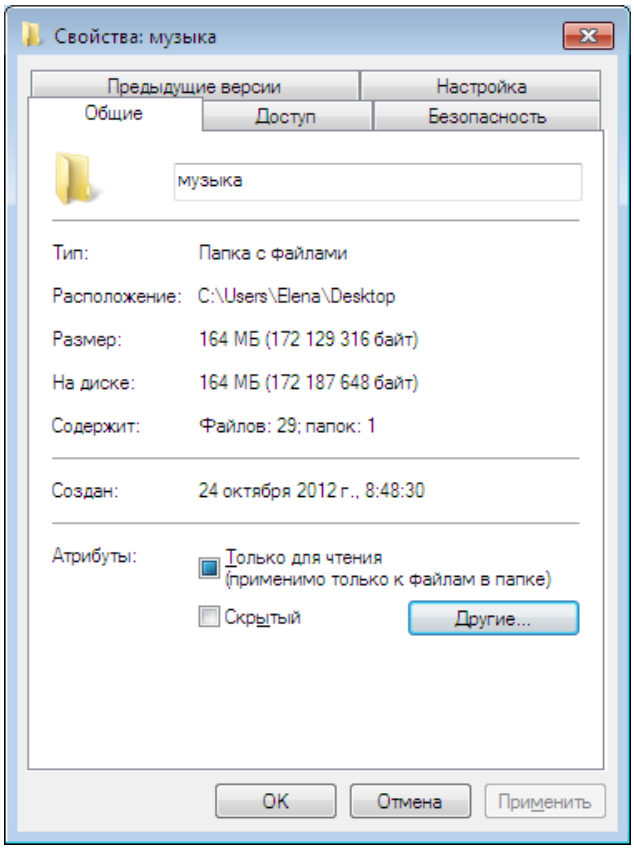

Рисунок 3.11 – Свойства папки музыка

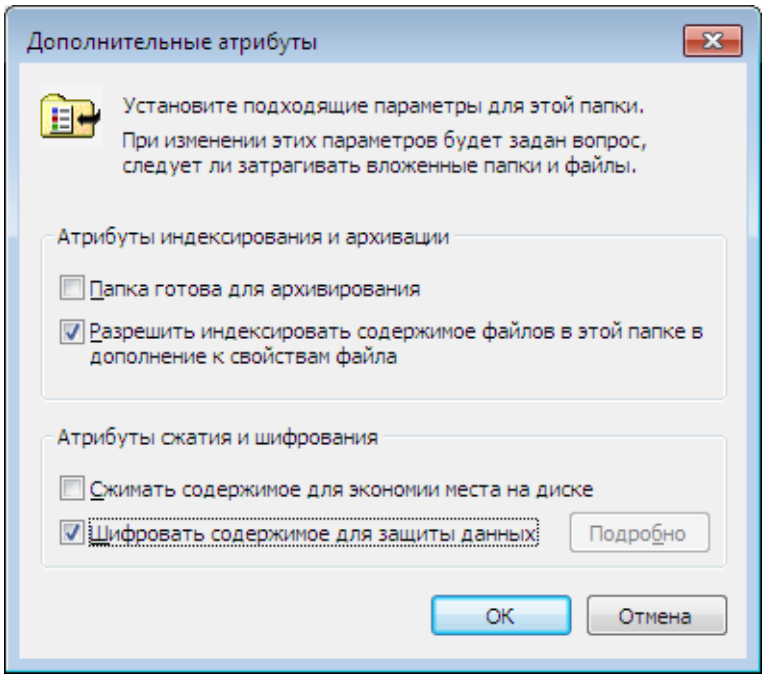

Рисунок 3.12 – Дополнительные атрибуты

3.4 Контрольные вопросы

1. Что такое список контроля доступа?
2. Какие бывают типы доступа?
3. Какие носители информации можно шифровать с помощью EFS?
4. Какое количество папок можно зашифровать с помощью EFS?
5. Объясните концепцию наследования разрешений.

Список использованных источников

1 Коньков, К.А. Основы организации операционных систем Microsoft Windows [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/department/os/osmswin/.

2 Мак-Клар, С. Секреты хакеров. Безопасность сетей – готовые решения / Мак-Клар С., Скембрей Дж., Курц Дж. . – М.: Издательский дом «Вильямс», 2002. – 736 с.

3 Мак-Клар, С. Секреты хакеров. Безопасность Windows 2003 — готовые решения / С. Мак-Клар, Дж. Скембрей, Дж. Курц. – М.: Издательский дом «Вильямс», 2004. – 512 с.

4 Дейтел, Х.М. Операционные системы. Основы и принципы. / Х.М. Дейтел, П.Дж. Дейтел. – М. : Бином, 2006. – 1024 с.

5 Руководство по безопасности Windows® 7 [Электронный ресурс]. – Режим доступа: http://technet.microsoft.com/ru-ru/library/ee914622.aspx.

6 Таненбаум, Э. Современные операционные системы / Э. Таненбаум. – СПб.: Питер, 2010. – 1120 с.

Приложение А

Оснастки системы Windows 7

Таблица А.1 – Оснастки системы

Оснастка	Назначение
Служба работы с факсами (Fax Service Management)	Служит для управления службой и устройствами факсимильной связи
Анализ и настройка безопасности (Security Configuration and Analysis)	Служит для управления безопасностью системы с помощью шаблонов безопасности
Групповая политика (Group Policy)	Служит для назначения сценариев регистрации, групповых политик для компьютера и пользователей некоторого компьютера сети; позволяет просматривать и изменять политику безопасности, политику аудита и права пользователей
Дефрагментация диска (Disk Defragmenter)	Служит для анализа и дефрагментации дисковых томов
Диспетчер устройств (Device Manager)	Содержит список всех устройств, подключенных к компьютеру, и позволяет их конфигурировать
Локальные пользователи и группы (Local Users and Groups)	Служит для управления локальными учетными записями пользователей и групп
Общие папки Shared Folders)	Отображает совместно используемые папки, текущие сеансы и открытые файлы
Оповещение и журналы производительности (Performance Logs and Alerts)	Конфигурирует журналы данных о работе системы и службу оповещений
Папка (Folder)	Служит для добавления новой папки в дерево
Просмотр событий (Event Viewer)*	Служит для просмотра и управления системным журналом, журналами безопасности и приложений

Продолжение таблицы А.1

Сведения о системе (System Information)	Отображает информацию о системе
Сертификаты (Certificates)	Служит для управления сертификатами
Системный монитор (Performance)*	Используется для сбора и просмотра в реальном времени данных, характеризующих работу памяти, дисков, процессора и других компонентов системы
Служба индексирования (Indexing Service)	Служит для индексирования документов различных типов с целью ускорения их поиска
Служба компонентов (Componenet Services)*	Конфигурирует и управляет службами компонентов COM+
Службы (Services)*	Запускает, останавливает и конфигурирует службы (Services) Windows
Ссылка на ресурс web (Link to Web Address)	Служит для подключения webстраниц (html, asp, stml)
Управление дисками (Disk Management)	Служит для управления дисками и защитой данных, для разбиения дисков на логические тома, форматирования, управления совместным доступом, квотами и т. д.
Управление компьютером (Computer Management)	Предоставляет функции администрирования системы. Содержит в своем составе ряд изолированных оснасток и оснасток расширения
Управление политикой безопасности IP (IP Security Policy Management)	Служит для управления политиками IPSec для безопасного соединения с другими компьютерами
Управление съемными носителями (Removable Storage Management)	Служит для управления съемными носителями информации
Управляющий элемент (WMI Control)	Служит для конфигурирования средств Windows Management Instrumentation и управления ими
Шаблоны безопасности (Security templates)	Обеспечивает возможность редактирования файлов-шаблонов безопасности
Элемент ActiveX (ActiveX Control)	Подключение к дереву консоли различных элементов управления ActiveX

Приложение Б

Содержимое папки локального профиля пользователя

Таблица Б.1 - Содержимое папки локального профиля пользователя

Подпапка	Содержимое
Application Data	Данные, относящиеся к конкретному приложению, например, индивидуальный словарь. Разработчики приложений сами принимают решение, какие данные должны быть сохранены в папке профиля пользователя.
Cookies	Служебные файлы, получаемые с просматриваемых с веб-серверов
Local Settings	Данные о локальных настройках, влияющих на работу программного обеспечения компьютера
NetHood	Ярлыки объектов сетевого окружения
PrintHood	Ярлыки объектов папки принтера
Recent	Ярлыки недавно используемых объектов (например, недавно редактированных текстовых документов)
SendTo	Ярлыки объектов, куда могут посылаться документы (появляются в контекстном меню файла или папки при выборе опции Отправить)
Главное меню (Start Menu)	Ярлыки программ
Избранное (Favorites)	Ярлыки часто используемых программ и папок
Мои документы (My documents)	Данные о документах и графических файлах, используемых пользователем
Рабочий стол (Desktop)	Объекты рабочего стола, включая файлы и яр-
Подпапка	Содержимое
Шаблоны (Templates)	Ярлыки шаблонов (например, программ из пакета Microsoft Office)