Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

А. Ю. Якимук, А. А. Конев

ЗАЩИТА ИНФОРМАЦИИ

Методические указания
по выполнению лабораторной работы
для студентов заочной формы обучения с применением дистанционных образовательных технологий

Томск 2017

Корректор: А. Н. Миронова

Якимук А. Ю., Конев А. А.

Защита информации : методические указания по выполнению лабораторной работы для студентов заочной формы обучения с применением дистанционных образовательных технологий / А. Ю. Якимук, А. А. Конев. – Томск : ФДО, ТУСУР, 2017. – 81 с.

В 2019 г. внесены исправления.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Целью преподавания дисциплины является подготовка бакалавров, способных осуществить базовое администрирование подсистем защиты информации операционной системы Windows. В процессе выполнения работ студенты получат навыки администрирования учетных записей пользователей, работы с оснастками и групповой политикой, а также смогут постигнуть на практике дискреционный принцип разграничения доступа к объектам в системе и способы ограничить программную среду, запретив запуск нежелательных программ.

В данных методических указаниях выполнение задач рассматривается на примере операционной системы Microsoft Windows 8. В более новых версиях выполнение работы осуществляется идентично, а в более старых отличие заключается только в отсутствии возможности поиска необходимой функции через меню «Пуск». Рекомендуется выполнять лабораторные работы на виртуальной машине, в противном случае может возникнуть потеря доступа к хранящимся на компьютере данным.

Одна из самых популярных систем VirtualBox, скачать ее можно по ссылке: https://www.virtualbox.org/wiki/Downloads. Установка системы в созданной виртуальной машине происходит аналогично тому, как она устанавливается на компьютер.

Выбор варианта лабораторной работы осуществляется по общим правилам с использованием следующей формулы:

$$V = (N \times K) \text{ div } 100,$$

где V – искомый номер варианта,

N – общее количество вариантов,

div – целочисленное деление,

при $V = 0$ выбирается максимальный вариант,

K – код варианта.

1 ЛАБОРАТОРНАЯ РАБОТА № 1 «АДМИНИСТРИРОВАНИЕ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ»

Целью лабораторной работы является освоение средств администрирования учётных записей пользователей, изучение основных параметров, определяющих взаимодействие пользователей с операционной системой.

1.1 Руководство по работе с учетными записями

В операционной системе Windows 8 существуют 2 группы пользователей:

– локальные учетные записи;

– учетные записи Microsoft.

Первая группа называется локальной по причине того, что аутентификация происходит на локальном компьютере. Все учетные данные, необходимые для этого (имя пользователя, пароль и параметры учетной записи), хранятся в нем.

В случае работы с учетной записью Microsoft аутентификация пользователей происходит на сервере сети, то есть удаленно. Преимущество данного способа в том, что любой сотрудник предприятия может зайти в сеть с любого компьютера, а не только с закрепленного за ним. Сервер хранит все параметры пользователя, а также при необходимости и документы, с которыми он работает. Однако второй тип пользователей имеет свой недостаток – при отсутствии интернет-соединения или коммутируемом (не устанавливаемом автоматически) соединении аутентификация будет невозможна.

Локальные учетные записи бывают трех видов:

– учетная запись администратора, создаваемая при установке системы и используемая при изменении параметров системы;

– учетная запись пользователя, позволяющая использовать установленные администратором из внешних источников программы и изменять параметры персонализации;

– гостевая учетная запись.

1.1.1 Управление учётными записями локальных пользователей

Рассмотрите механизм работы с учетными записями пользователей, предлагаемых Windows 8. Для этого в меню «Пуск» найдите параметры, связанные с пользователями (рис. 1.1). Рассмотрите предложенные варианты работы с пользователями. Поскольку «Создание новой учетной записи» все равно приведет к пункту «Пользователи» выберем именно его.

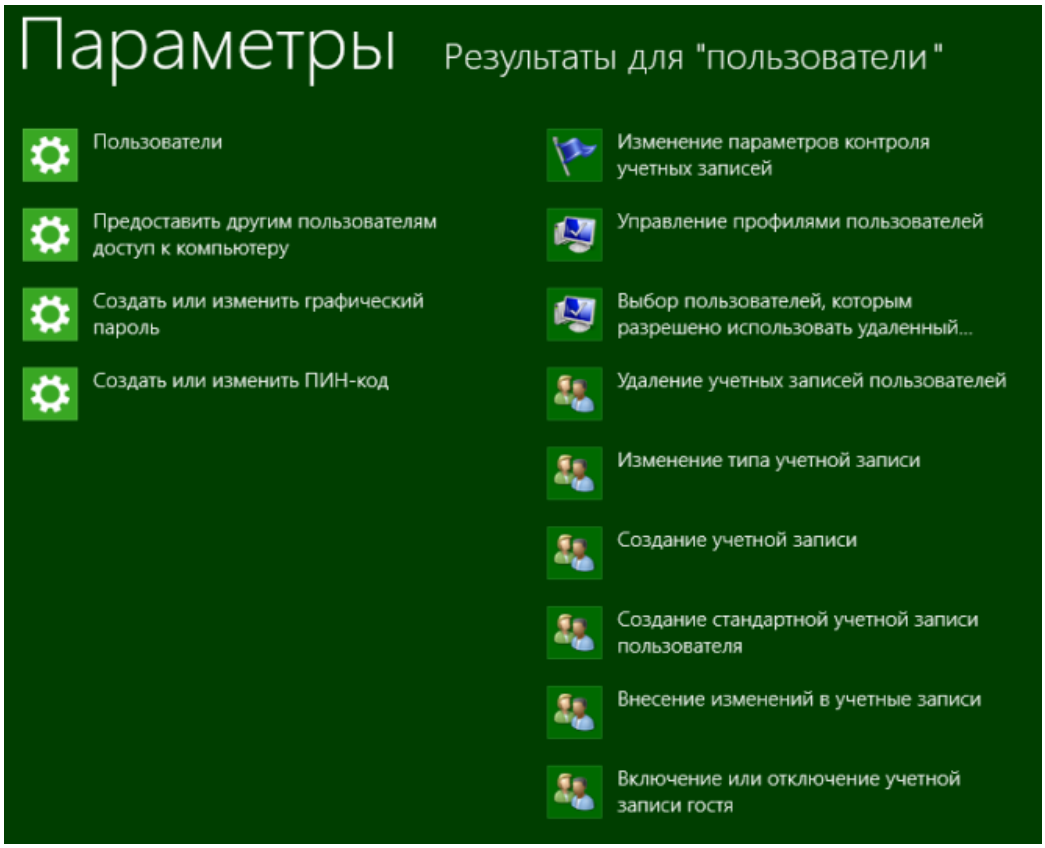

Рис. 1.1 – Результат поиска

В результате проделанных действий откроется вкладка в «Параметрах компьютера», отвечающая за управление учетных записей. В данном разделе будет приведена информация о том, под какой учетной записью был

осуществлен вход, представлены функции по изменению параметров входа, а также все учетные записи на данном компьютере (если таковые имеются), предложено создание новых пользователей (рис. 1.2).

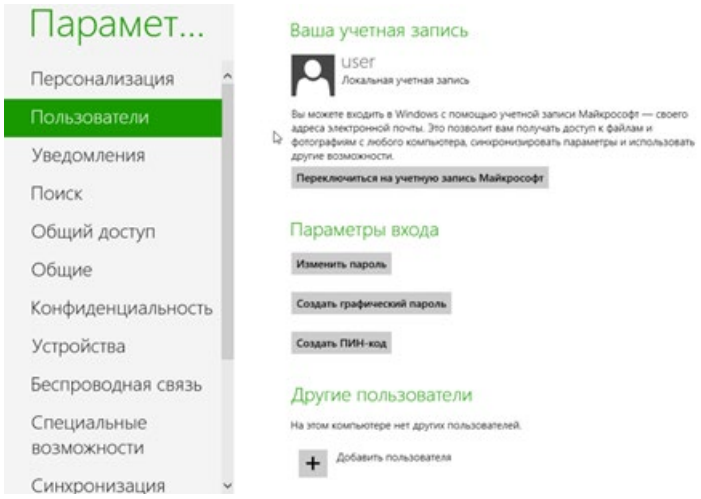

Рис. 1.2 – Вкладка управления пользователями

Выберите действие «Добавить пользователя». В результате поступит предложение создать учетную запись Microsoft и перечислены преимущества данного типа пользователей. Нажмите на ссылку «Вход без учетной записи Майкрософт» (рис. 1.3).

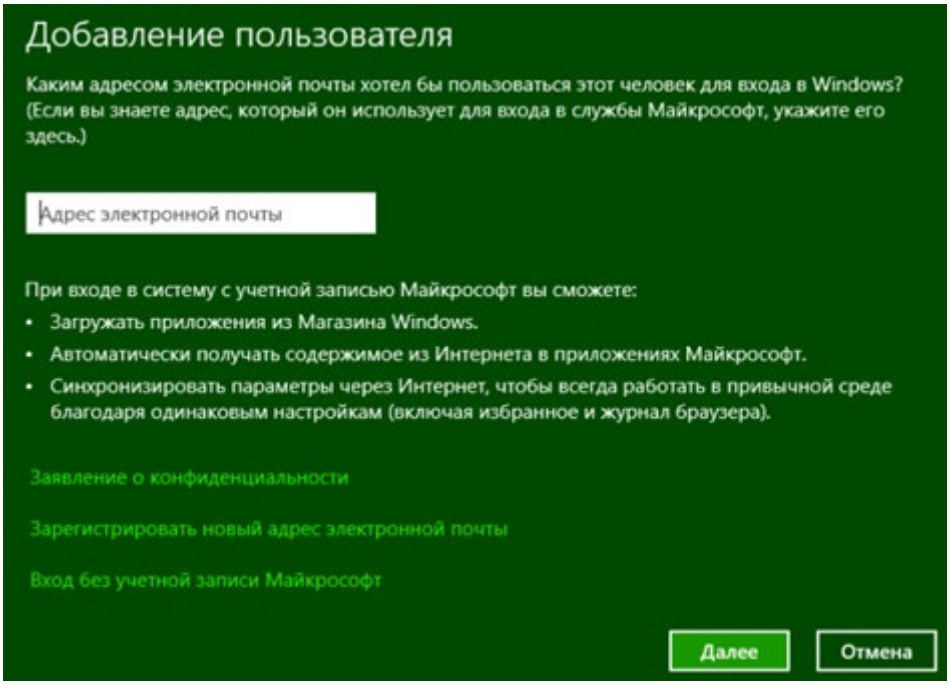

Рис. 1.3 – Добавление пользователя

В результате будет предложено выбрать один из двух вариантов входа в систему (рис. 1.4). Ознакомьтесь с описанием каждого типа записей, после чего создайте локальную учетную запись.

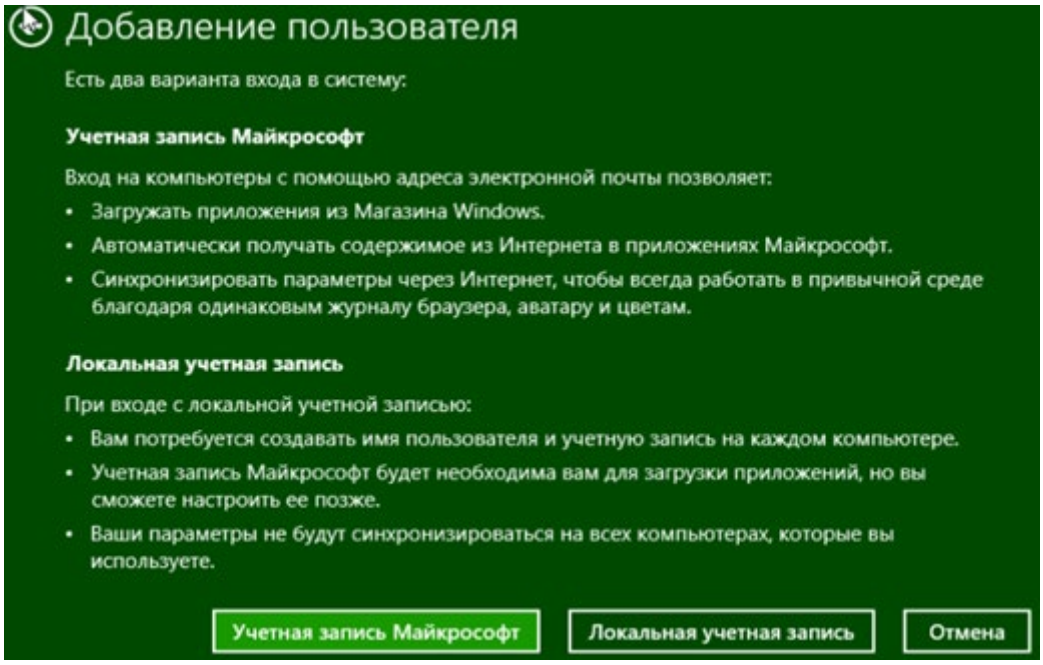

Рис. 1.4 – Выбор варианта учетной записи

После этого потребуется задать имя пользователя и пароль, а также подсказку для пароля. Создайте пользователя по данным требованиям. В конце создания новой учетной записи будет предложено получать отчеты об использовании данным пользователем компьютера. После завершения создания пользователя соответствующая запись появится в перечне учетных записей на данном компьютере.

Запустите Microsoft Management Console (MMC) – компонент Windows, позволяющий администрировать систему. Откройте меню «Пуск – Выполнить – MMC». Для добавления необходимого набора оснасток в меню консоли выберите «Файл – Добавление оснастки». Нажмите на «Добавить» – будет предложен перечень, из которого пользователь может выбрать одну или несколько оснасток.

При сохранении консоли существует возможность установки режима работы пользователя с этой консолью: авторский режим, предоставляющий пользователю полный доступ ко всем функциям MMC, и пользовательский режим.

Существуют три вида пользовательского режима:

– полный доступ (full access) даёт пользователю доступ ко всем командам MMC, но не позволяет добавлять/удалять оснастки или изменять свойства консоли;

– ограниченный доступ, много окон (Limited Access Multiple Windows), позволяет пользователю осуществлять доступ только к областям дерева консоли, которые отображались при сохранении консоли, а также открывать новые окна;

– ограниченный доступ, одно окно (Limited Access Single Window) работает так же, как многооконный ограниченный доступ с той разницей, что пользователь не может открывать новые окна.

Сохраните консоль в авторском и пользовательских режимах (меню «Файл – Параметры») (рис. 1.5).

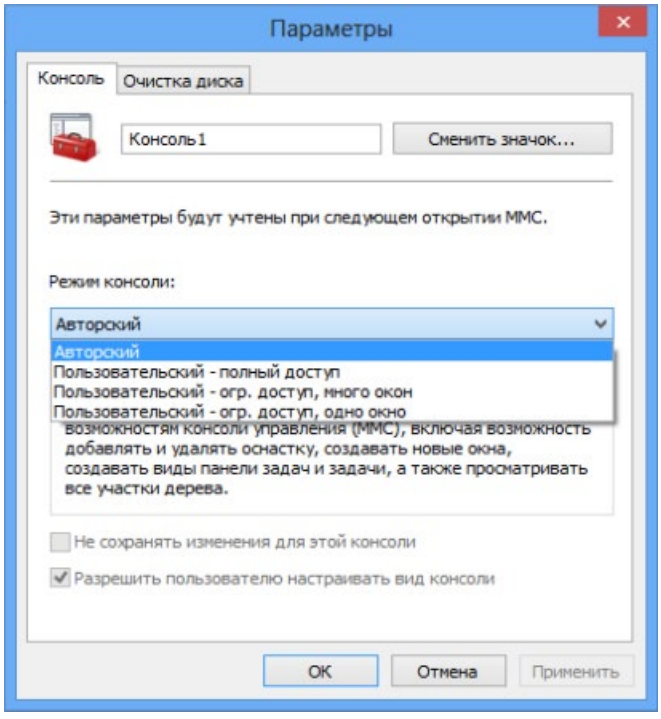

Рис. 1.5 – Параметры режима консоли

Через пункт «Добавить или удалить оснастку» добавьте «Локальные пользователи и группы» (рис. 1.6).

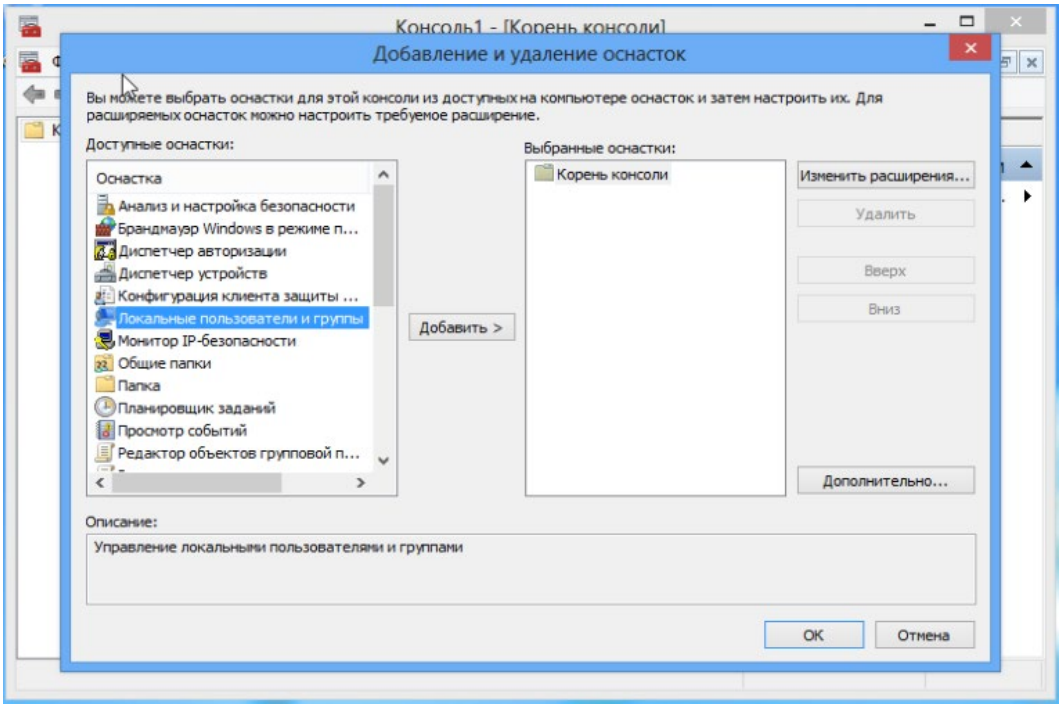

Рис. 1.6 – Добавление оснастки

Через данную оснастку также можно добавить нового пользователя (рис. 1.7).

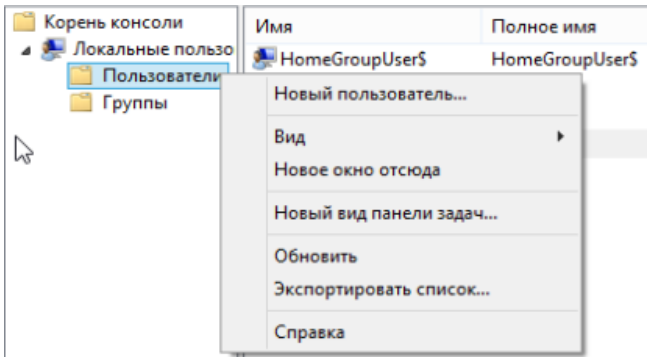

Рис. 1.7 – Добавление пользователя через оснастку

В появившемся окне (рис. 1.8) введите имя учётной записи, а также пароль и его подтверждение. Если администратор устанавливает пользователю временный пароль, то для обязательной смены пароля необходимо

включить параметр «Потребовать смену пароля при следующем входе в систему». Сразу после успешной аутентификации пользователь получает запрос на смену пароля, в ответ на который он должен задать новый пароль. Этот подход необходимо использовать в тех случаях, когда администратор системы не должен знать пароли пользователей.

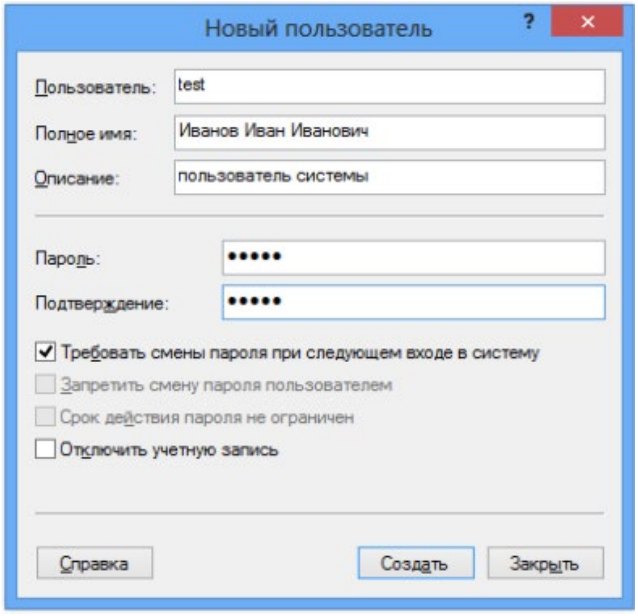

Рис. 1.8 – Настройка параметров учётной записи при её создании

Если пользователь забыл свой пароль, то член группы «Администраторы» может сбросить его старый пароль при помощи функции «Задать пароль», доступной в контекстном меню учётной записи этого пользователя (рис. 1.9). Смените пароль созданной учётной записи.

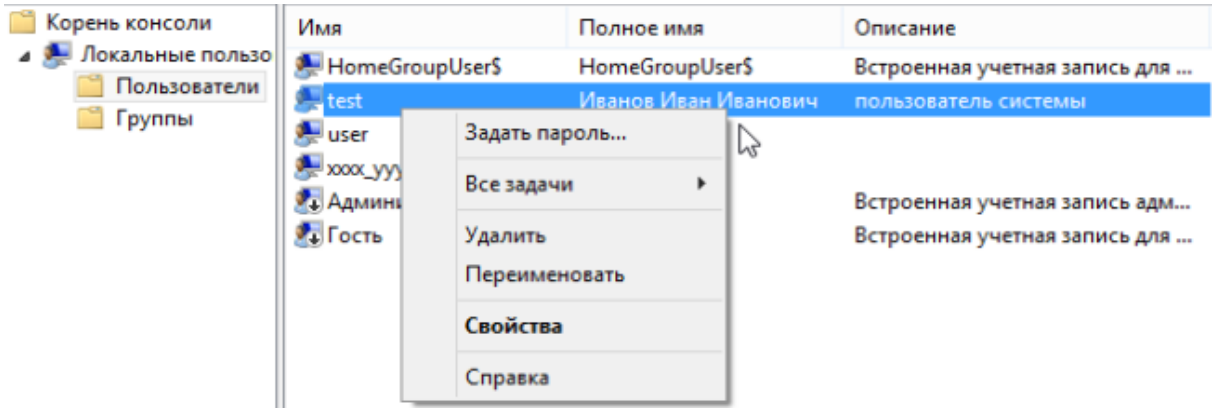

Рис. 1.9 – Задание пароля пользователя администратором

В данный момент времени учетная запись «Администратор» является заблокированной (рис. 1.10). Разблокируйте её, выбрав соответствующий пункт в свойствах учетной записи. Посмотрите, какие еще параметры можно настроить через свойства.

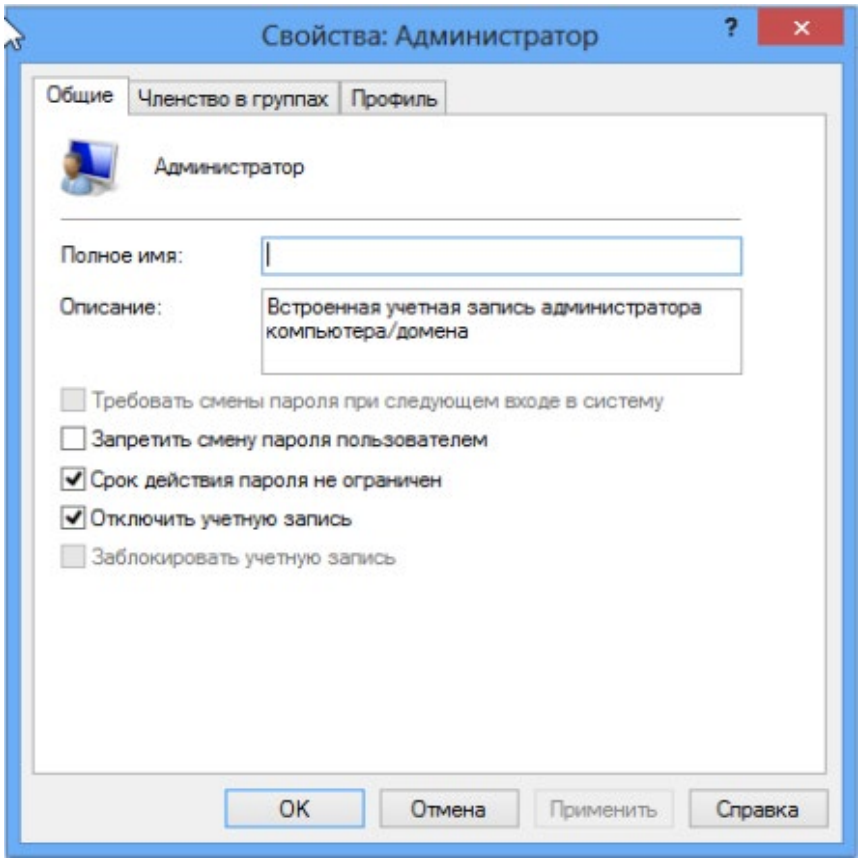

Рис. 1.10 – Изменение свойств администратора

Войдите в систему под созданной учётной записью. При первом входе пользователю будет выдано сообщение о необходимости ввести пароль (рис. 1.11) и окно смены пароля (рис. 1.12). Смените пароль созданной учётной записи.

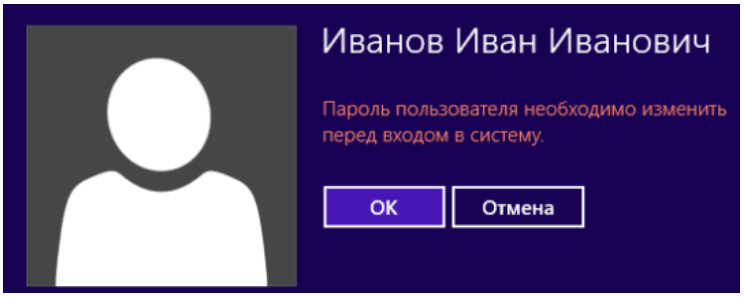

Рис. 1.11 – Сообщение пользователю о необходимости смены пароля

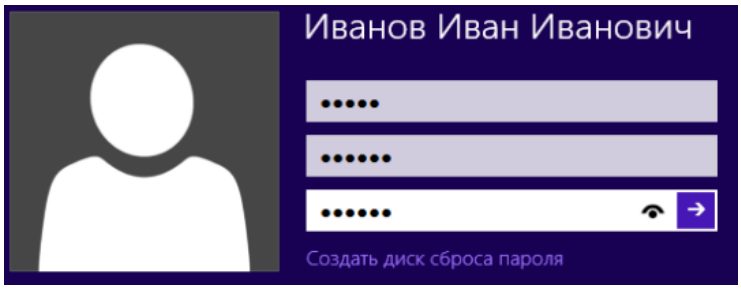

Рис. 1.12 – Окно «Смена пароля»

Для применения к пользователю набора прав и ограничений можно включить его учётную запись в группу пользователей с соответствующим набором прав и ограничений.

Войдите в систему под учётной записью «Администратор». Откройте «Свойства» созданной учётной записи. На вкладке «Членство в группах» добавьте пользователя в группу «Опытные пользователи» (рис. 1.13). Имя группы можно ввести самостоятельно или выбрать из списка, предоставляемого после последовательного нажатия кнопок «Дополнительно» и «Поиск».

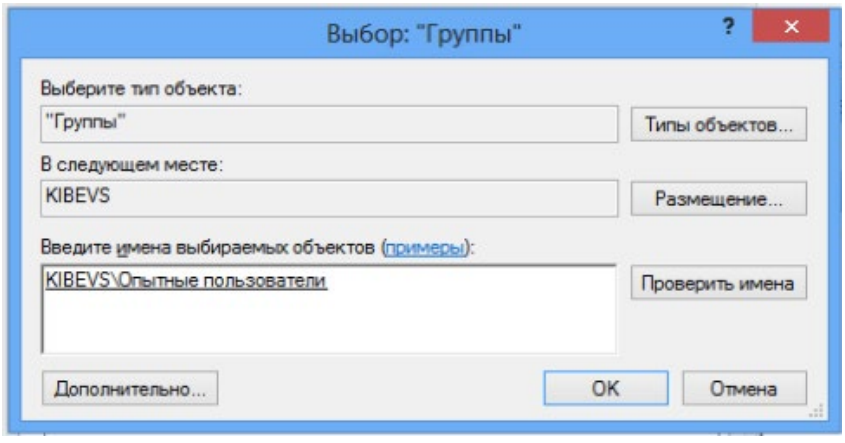

Рис. 1.13 – Добавление группы

В разделе «Группы» откройте «Свойства» группы «Опытные пользователи» и проверьте наличие в группе добавленной учётной записи. Создайте новую группу и добавьте в неё этого же пользователя.

Вызовите командную строку и выполните команду Net user. Консоль выведет перечень всех имеющихся учетных записей (рис. 1.14).

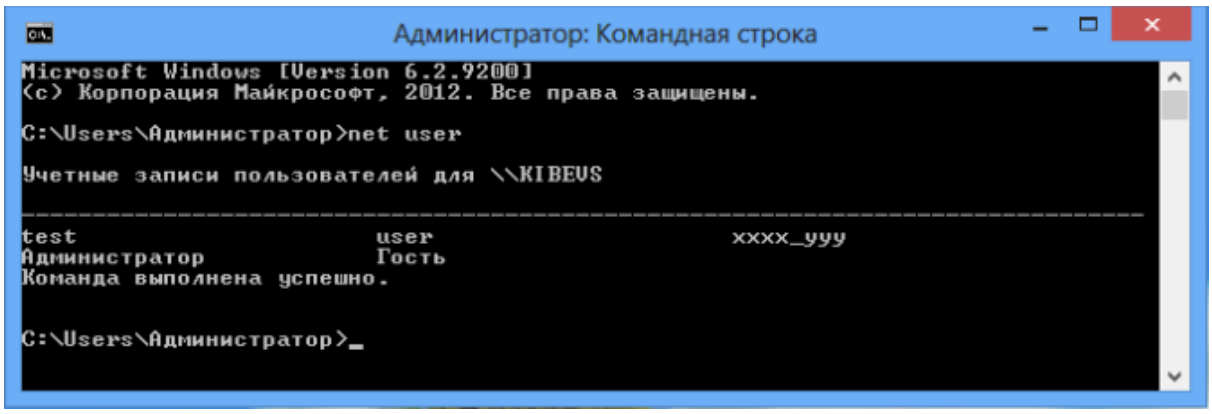

Рис. 1.14 – Список пользователей в командной строке

Создание и изменение учётных записей осуществляется при помощи команды Net user. Подробную информацию о команде можно получить, введя Net user/help (рис. 1.15). Изучите предлагаемые функции команды.

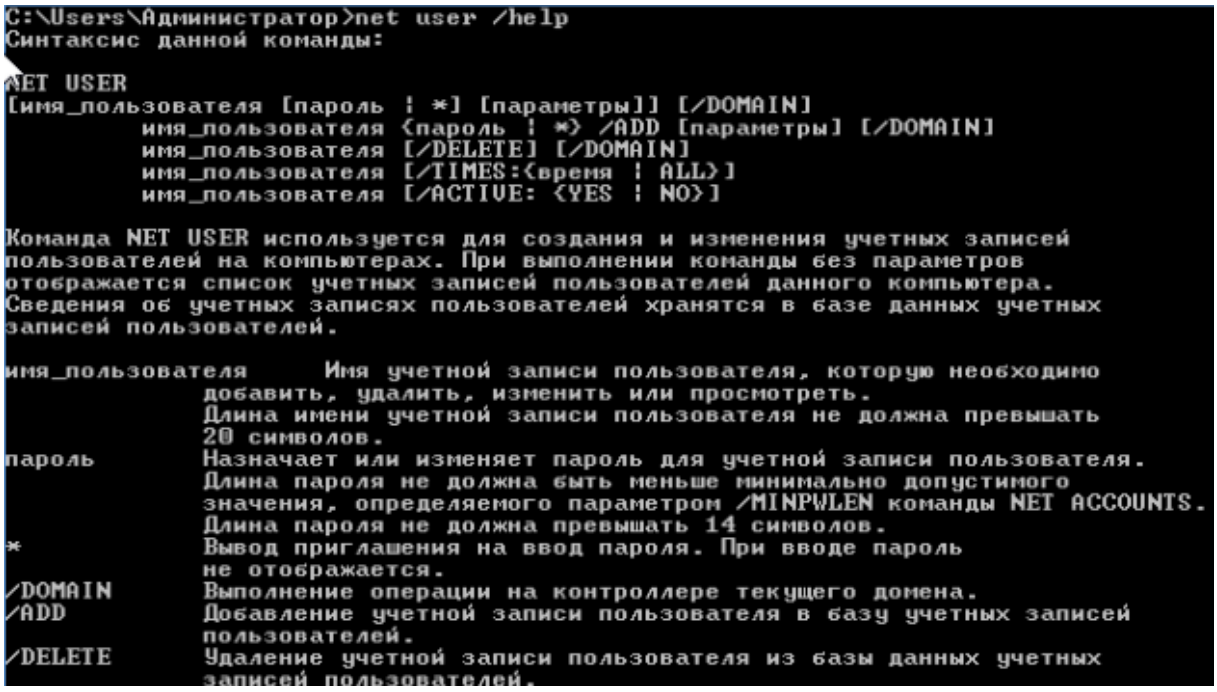

Рис. 1.15 – Справка по команде Net user

Создайте учётную запись пользователя с именем, совпадающим с Вашим именем в кафедральной сети, явно указав пароль. При создании дополнительно к логину укажите полное имя пользователя (рис. 1.16).

Синтаксис команды Net user при создании учётной записи пользователя (имена, написанные кириллицей, вводятся в кавычках):

Net user имя_пользователя {пароль | *} /ADD [параметры].

Для добавления полного имени пользователя нужно в качестве параметра ввести: /FULLNAME:"имя".

```
C:\Windows\system32>net user III 12345 /add /fullname:"Иванов Иван Иванович"
Команда выполнена успешно.
```

Рис. 1.16 – Создание нового пользователя

Проверьте наличие созданной учётной записи в списке пользователей при помощи команды Net user. Команда Net user имя_пользователя, введённая без параметров, позволяет просмотреть информацию об указанном пользователе. Просмотрите информацию о созданной учетной записи.

Возможен ввод пароля без отображения на экране, для этого вместо пароля нужно ввести «*». Измените пароль созданного пользователя при помощи команды Net user имя_пользователя * (рис. 1.17).

```
C:\Windows\system32>net user III *
Введите пароль для пользователя:
Повторите ввод пароля для подтверждения:
Команда выполнена успешно.
```

Рис. 1.17 – Изменение пароля пользователя

Существует возможность установки ограничений на работу пользователя в операционной системе по времени. Для этого используется параметр /TIMES:{промежуток | ALL}. Значение ALL указывает, что пользователь может войти в систему в любое время, а пустое значение указывает, что пользователь не может войти в систему никогда. Ограничьте время работы созданного пользователя рамками рабочего времени (рис. 1.18). Переведите часы на время, не входящее в интервал рабочего, и протестируйте возможность входа пользователя в операционную систему.

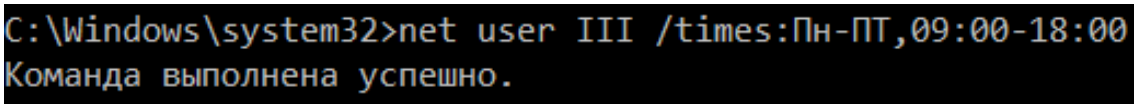

Рис. 1.18 – Задание интервала действия учетной записи

В случае необходимости администратор может заблокировать учётную запись пользователя. Заблокируйте учётную запись созданного пользователя при помощи параметра /ACTIVE:{YES | NO} (рис. 1.19).

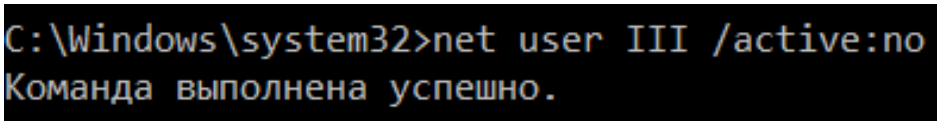

Рис. 1.19 – Блокирование учетной записи

Проверьте применение блокирования к учётной записи при помощи команды Net user имя_пользователя. В выдаваемой о пользователе информации есть графа «Учётная запись активна», показывающая состояние блокирования учётной записи. Разблокируйте учётную запись пользователя.

Если пользователь временно работает в организации, то администратор может ограничить время действия учётной записи пользователя. Для этого служит параметр: /EXPIRES:{дата | NEVER}. Если используется значение NEVER, то время действия учётной записи не имеет ограничений срока действия. Ограничьте время действия учётной записи созданного пользователя (рис. 1.20). Установите системное время на более поздний срок, чем установленное ограничение. Попытайтесь войти в систему под данной учётной записью – операционная система выдаст ошибку (рис. 1.21).

Рис. 1.20 – Ограничение времени действия учётной записи

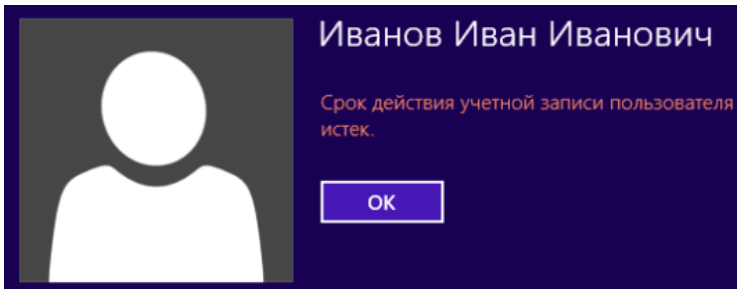

Рис. 1.21 – Ошибка при попытке входа под просроченной учётной записью

Команда Net localgroup служит для создания локальных групп и управления ими. При использовании этой команды без указания параметров выводится перечень групп пользователей, существующих в операционной системе (рис. 1.22). Выведите список всех существующих групп.

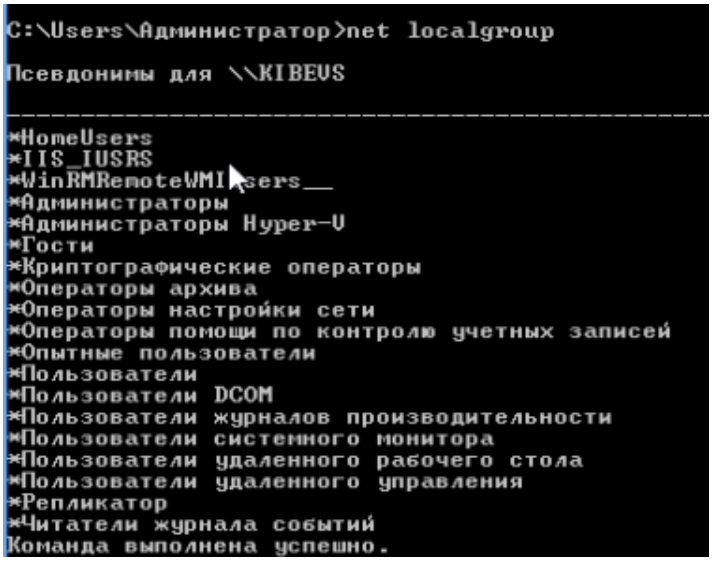

Рис. 1.22 – Список групп

Синтаксис команды Net user при создании локальной группы: Net localgroup имя_группы {/ADD }. Создайте локальную группу Students (рис. 1.23).

Рис. 1.23 – Создание группы

Проверьте наличие созданной группы пользователей при помощи команды Net localgroup. Добавление пользователей в группу осуществляется командой Net localgroup имя_группы имя [...] {/ADD }, где имя [...] – имя одного или нескольких пользователей (имена разделяются пробелами). Добавьте ранее созданного пользователя в группу Students.

Команда Net localgroup имя_группы выводит список пользователей, входящих в указанную группу. Выведите список пользователей группы Students (рис. 1.24).

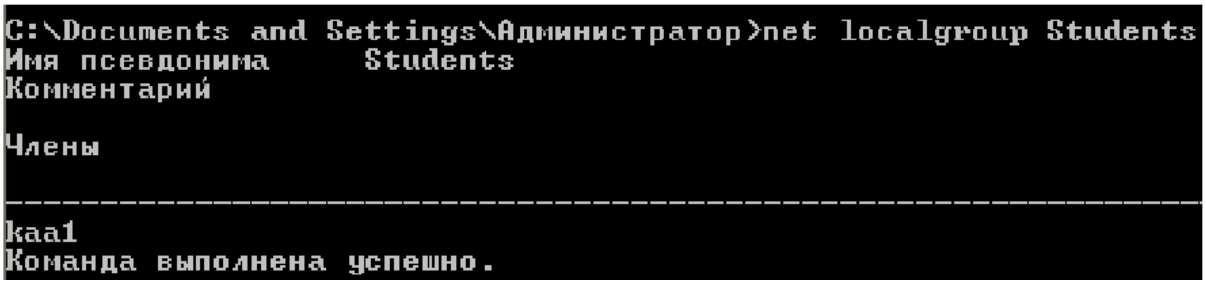

Рис. 1.24 – Просмотр списка пользователей заданной группы

Команда Net localgroup имя_группы выводит список пользователей, входящих в указанную группу. Выведите список пользователей группы Students.

Рис. 1.25 – Исключение пользователя из группы

Для удаления группы используется команда Net localgroup имя_группы {/DELETE}. Удалите группу Students (рис. 1.26).

Рис. 1.26 – Удаление группы пользователей

Проверьте отсутствие группы Students, используя команду вывода списка существующих групп пользователей.

1.1.2 Настройка политики учётной записи

Откройте «Локальную политику безопасности», вызвав её запросом secpol.msc в меню «Пуск». Основное окно «Локальной политики безопасности» представлено на рисунке 1.27. Значения параметров, заданные при настройке политики, будут применяться ко всем пользователям локального компьютера.

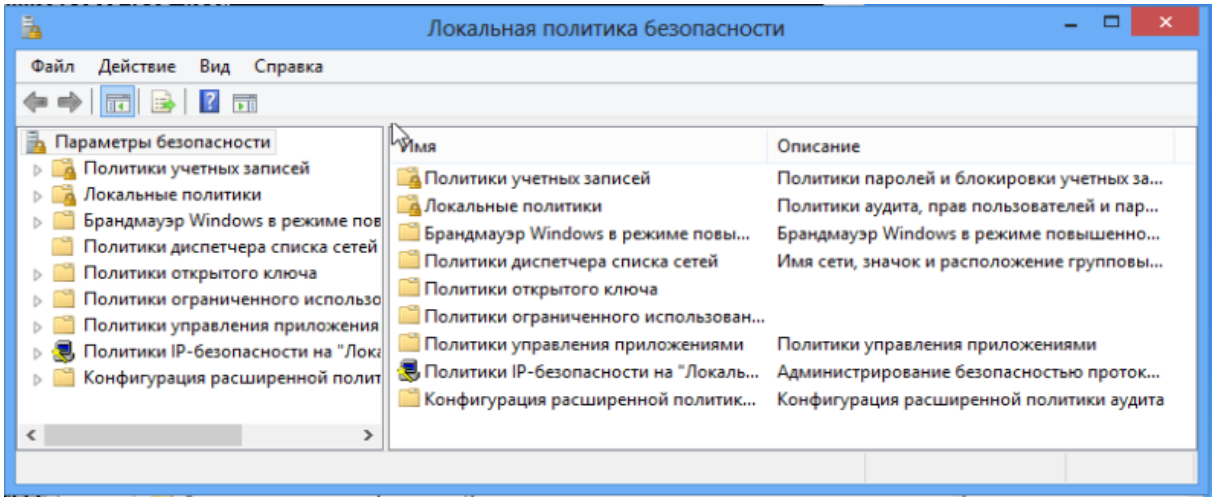

Рис. 1.27 – Локальная политика безопасности

Раздел «Политики учётных записей» «Локальной политики безопасности» включает в себя настройки, применяющиеся к паролям пользователей.

Выберите раздел «Политика паролей» («Параметры безопасности – Политики учётных записей – Политика паролей»). Настройки, входящие в раздел «Политика паролей», представлены на рисунке 1.28.

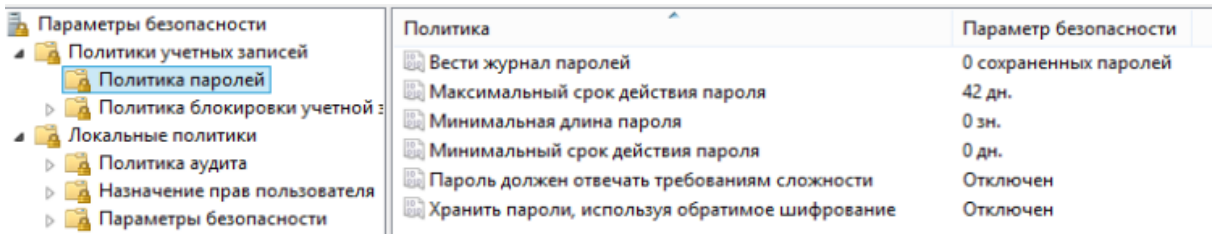

Рис. 1.28 – Политика паролей

Выполните следующие задания:

– установите максимальный срок действия пароля – 30 дней;

– установите минимальную длину пароля – 10 символов;

– для параметра «Вести журнал паролей» установите значение 3 хранимых пароля, означающее, что новый пароль должен отличаться от 3 последних паролей пользователя;

– включите параметр «Пароль должен отвечать требованиям сложности».

Параметр «Пароль должен отвечать требованиям сложности» определяет требования сложности для паролей. Если эта политика включена, то пароли должны удовлетворять следующим минимальным требованиям:

– пароль не может содержать имя учётной записи пользователя или какую-либо его часть;

– пароль должен состоять не менее чем из шести символов;

– в пароле должны присутствовать символы трёх категорий из числа следующих четырёх:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) неалфавитные символы (например, !, $, #, %).

Проверка соблюдения этих требований выполняется при изменении или создании паролей. При помощи этого параметра можно избавиться от легко подбираемых паролей типа «111», «qwerty», «12345» и т. д.

Убедитесь, что для пользователя не включена опция «Срок действия пароля неограничен» в оснастке «Локальные пользователи и группы». Переведите системное время более чем на 30 дней вперёд. Попытайтесь войти под созданной учётной записью. Пользователю будет выдано сообщение об истечении срока действия пароля (рис. 1.29). При смене пароля попытайтесь заменить пароль на более простой (например, abc12345 или включающий

имя учётной записи). В этом случае пользователю будет выдано сообщение об ошибке при смене пароля (рис. 1.30). Введите пароль, удовлетворяющий требованиям.

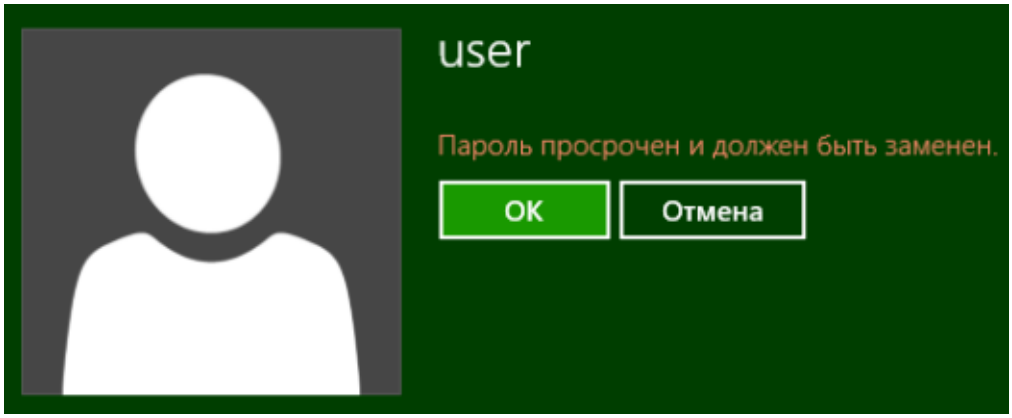

Рис. 1.29 – Сообщение об истечении срока действия пароля

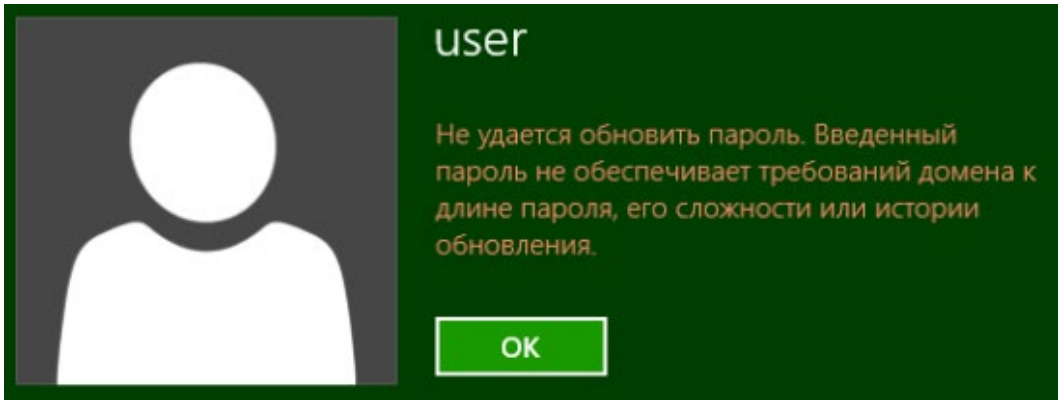

Рис. 1.30 – Сообщение о несоответствии пароля требованиям

Войдите в систему под учётной записью «Администратор». Переведите системное время в исходное состояние. Выберите раздел «Политика блокировки учётной записи» («Параметры безопасности – Политики учётных записей – Политика блокировки учётной записи»). Настройки, входящие в раздел «Политика блокировки учётной записи», представлены на рисунке 1.31.

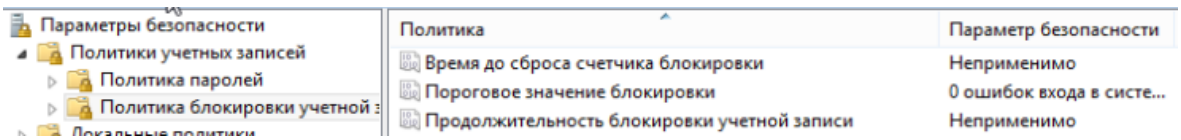

Рис. 1.31 – Политика блокировки учетной записи

Настройте параметры следующим образом:

– установить пороговое значение блокировки, равное 3 ошибкам входа в систему (после 3 неудачных попыток входа учётная запись блокируется);

– установить длительность блокировки в параметре «Блокировка учётной записи на», равную 30 мин (значение 0 означает, что блокировку может снять только администратор);

– установите сброс счётчика блокировки через 15 минут. Если в течение установленного времени будет 3 неудачных попытки входа, то учётная запись блокируется. Если неудачных попыток в течение установленного времени будет меньше, то опять допускается 3 неудачных попытки (значение этого параметра не должно превышать длительность блокировки учётной записи).

Завершите сеанс учётной записи «Администратор». При входе в систему под созданной учётной записью три раза введите неправильный пароль. При следующей попытке входа в систему будет выдано сообщение о блокировании созданной учётной записи (рис. 1.32).

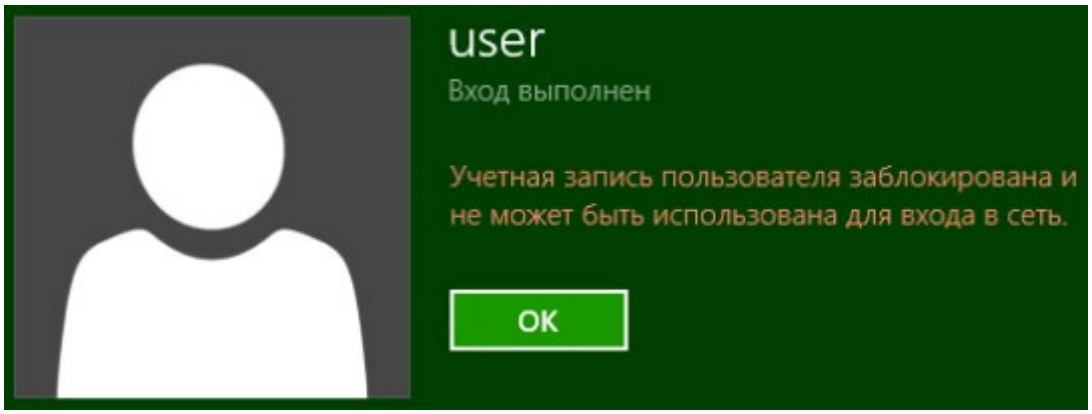

Рис. 1.32 – Сообщение о блокировке учетной записи

Войдите в систему под учётной записью «Администратор». Разблокируйте созданную учётную запись. Для этого в окне «Свойства» этой учётной записи отключите настройку «Заблокировать учётную запись».

Вызовите командную строку. Net accounts используется для обновления базы данных регистрационных записей и изменения параметров входа в сеть (LOGON) и требований к паролям для всех регистрационных записей. При использовании этой команды без указания параметров выводятся текущие значения параметров, определяющих требования к паролям, и другие параметры. Выведите текущие параметры входа в систему (рис. 1.33).

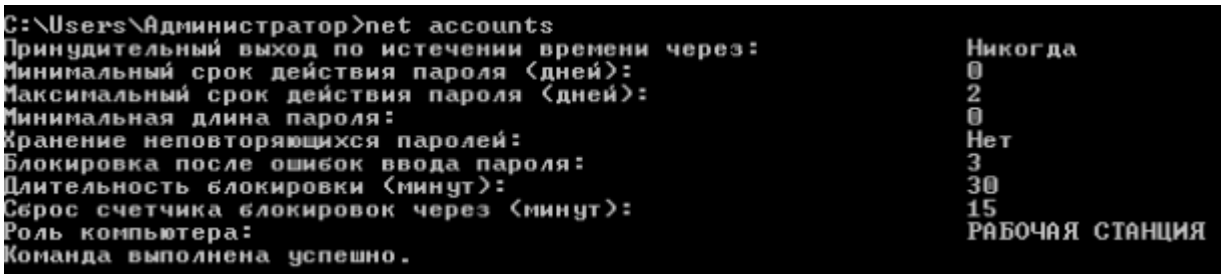

Рис. 1.33 – Просмотр информации о требованиях к качеству паролей

Задайте следующие требования к паролю:

– минимальную длину – 6 символов;

– максимальный срок действия пароля – 40 дней;

– запрет использования 3 последних паролей пользователя.

Применение этих требований производится при помощи следующих параметров команды Net accounts:

/MINPWLEN:длина

/MINPWAGE:дни

/UNIQUEPW:число

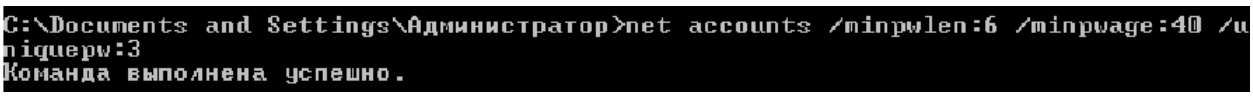

Рис. 1.34 – Изменение требований к качеству паролей

Проверьте изменение требований к качеству паролей.

1.2 Задание

1. В оснастке «Локальные пользователи и группы» создайте новую учётную запись с Вашими инициалами в качестве имени пользователя.

2. Примените к созданной учётной записи настройки, указанные в Вашем варианте (табл. 1.1).

Таблица 1.1 – Варианты заданий работы с пользователями

Параметр \ Вариант	1	2	3	4	5	6	7	8	9	10
Максимальный срок действия пароля	30	90	60	30	90	60	30	90	60	30
Минимальная длина пароля	6	7	8	9	10	6	7	8	9	10
Требовать неповторяемости паролей	6	5	4	3	2	6	5	4	3	2
Пароль должен отвечать требованиям сложности	+	–	–	+	–	–	+	–	+	+
Пороговое значение блокировки	3	4	5	6	7	3	4	5	6	7
Блокировка учётной записи на …	10	20	30	45	60	10	20	30	45	60
Сброс счётчика блокировки через	5	10	15	20	30	10	20	30	45	60
Завершение работы системы	+	+			+		+		+	
Локальный вход в систему	+	+	+	+	+	+	+	+	+	+
Изменение системного времени	+		+		+		+		+	

3. В соответствии с таблицей 1.2 через командную строку создайте учётную запись указанного пользователя и включите её в указанную группу пользователей. Для созданной учётной записи установите указанные параметры.

Таблица 1.2 – Варианты заданий по командной строке

Вариант	Имя	Имя группы	Параметры учётной записи
1	User1	Пользователи	Время входа: пн-пт, с 8 до 17 часов
2	User2	Администраторы	Срок действия – 30.06 текущего года
3	User3	Опытные пользователи	Время входа: пн-сб, с 8 до 17 часов
4	User4	Операторы архива	Время входа: пн-сб, с 7 до 19 часов
5	User5	Гости	Срок действия – 31.12 текущего года
6	User6	Пользователи	Время входа: пн-пт, с 9 до 18 часов
7	User7	Администраторы	Срок действия – 01.09 текущего года
8	User8	Опытные пользователи	Время входа: пн-сб, с 9 до 18 часов
9	User9	Операторы архива	Время входа: пн-вс, с 8 до 20 часов
10	User10	Гости	Срок действия – 28.02 следующего года

Контрольные вопросы

1. Поясните параметр «Потребовать смену пароля при следующем входе в систему».

2. Включение какого параметра разрешает пользователю не изменять пароль по окончании его действия?

3. Какая функция позволяет сбросить забытый пароль пользователя и кто может воспользоваться этой функцией?

4. Какой параметр задаёт периодичность смены пароля?

5. Поясните параметр «Требовать неповторяемости паролей».

6. Поясните параметр «Пароль должен отвечать требованиям сложности» и перечислите минимальные требования, которым должны удовлетворять пароли, если параметр включен.

7. Какие параметры входят в политику блокировки учётной записи?

8. Возможно ли, что учётная запись не будет блокирована при количестве ошибок большем, чем установленное пороговое значение?

9. В каком разделе предоставляется возможность назначать пользователям права, связанные с информационной безопасностью?

10. В каком разделе предоставляется возможность устанавливать параметры операционной системы, связанные с информационной безопасностью?

2 ЛАБОРАТОРНАЯ РАБОТА № 2 «УПРАВЛЕНИЕ ПАРАМЕТРАМИ ОПЕРАЦИОННОЙ СИСТЕМЫ»

Целью лабораторной работы является ознакомление со средствами управления операционной системой Windows 8 – консолью управления и групповой политикой.

2.1 Руководство по использованию оснасток управления системой

Консоль управления Microsoft Management Console (MMC) – это компонент операционных систем семейства Windows NT, предоставляющий администраторам графический интерфейс для настройки системных приложений и прикладных программ.

Оснастка – компонент для MMC, включающий набор параметров какого-либо модуля операционной системы (файловой системы, управления пользователями и т. д.) или прикладного приложения.

Набор параметров для прикладных программ может быть добавлен в оснастку при помощи административных шаблонов – особым образом структурированных файлов с расширением *.adm.

Групповая политика – это набор правил или настроек, в соответствии с которыми производится настройка рабочей среды Windows.

2.1.1 Использование консоли управления MMC

Существующие оснастки MMC расположены на системном диске в каталоге system32. Вызвать оснастки можно в разделе «Администрирование» панели управления через свойства дисков, компьютера и т. п. Кроме того, вызов существующих оснасток возможен через «Пуск – Выполнить», указывая имя оснастки. Откройте, например, оснастку devmgmt.msc – Диспетчер устройств (рис. 2.1).

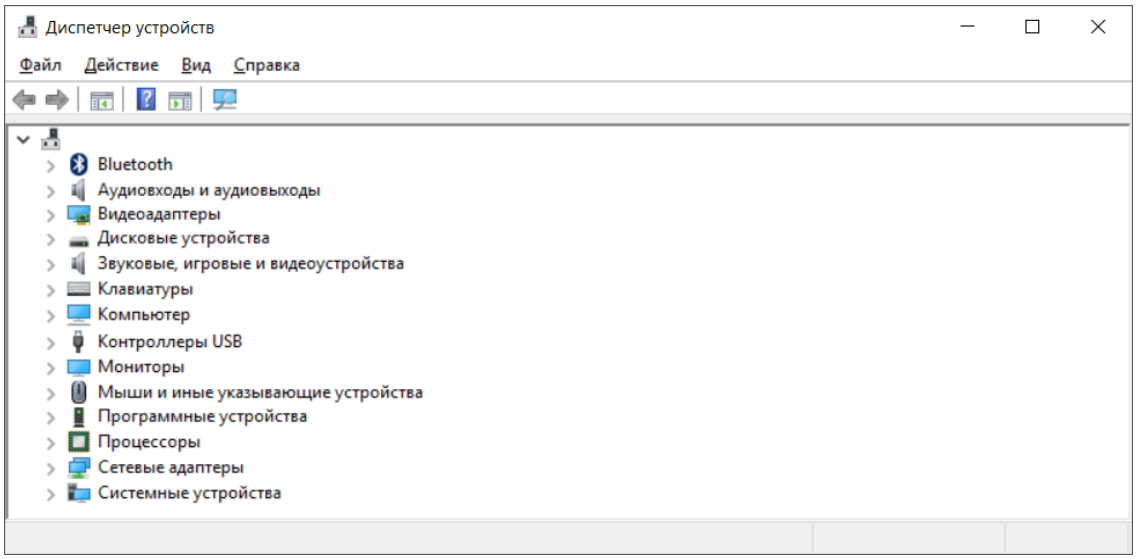

Рис. 2.1 – Оснастка «Диспетчер устройств»

Однако запомнить местонахождение и названия всех оснасток достаточно сложно, поэтому гораздо удобнее использовать консоль управления (рис. 2.2). Вызовите консоль управления MMC и добавьте оснастку «Управление дисками» (рис. 2.3). Для добавления необходимого набора оснасток в меню консоли выберите «Файл – Добавление и удаление оснасток».

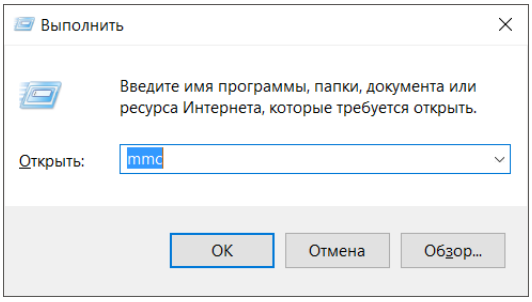

Рис. 2.2 – Вызов консоли управления Microsoft

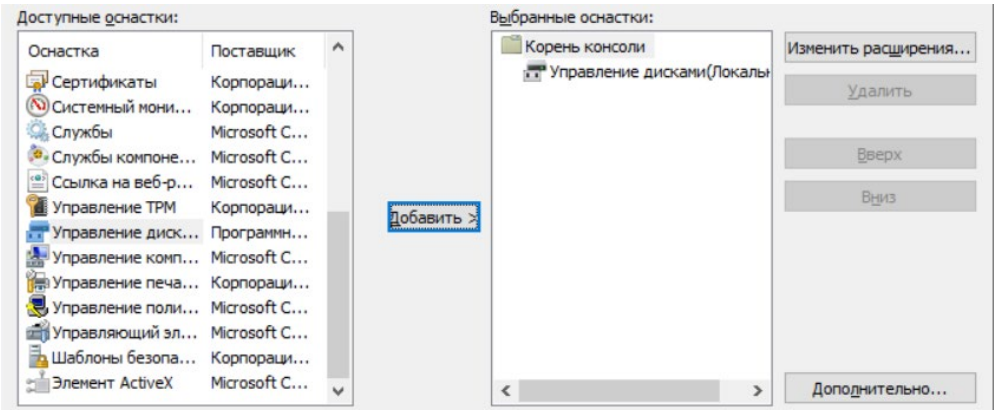

Рис. 2.3 – Процесс добавления новой оснастки в консоль

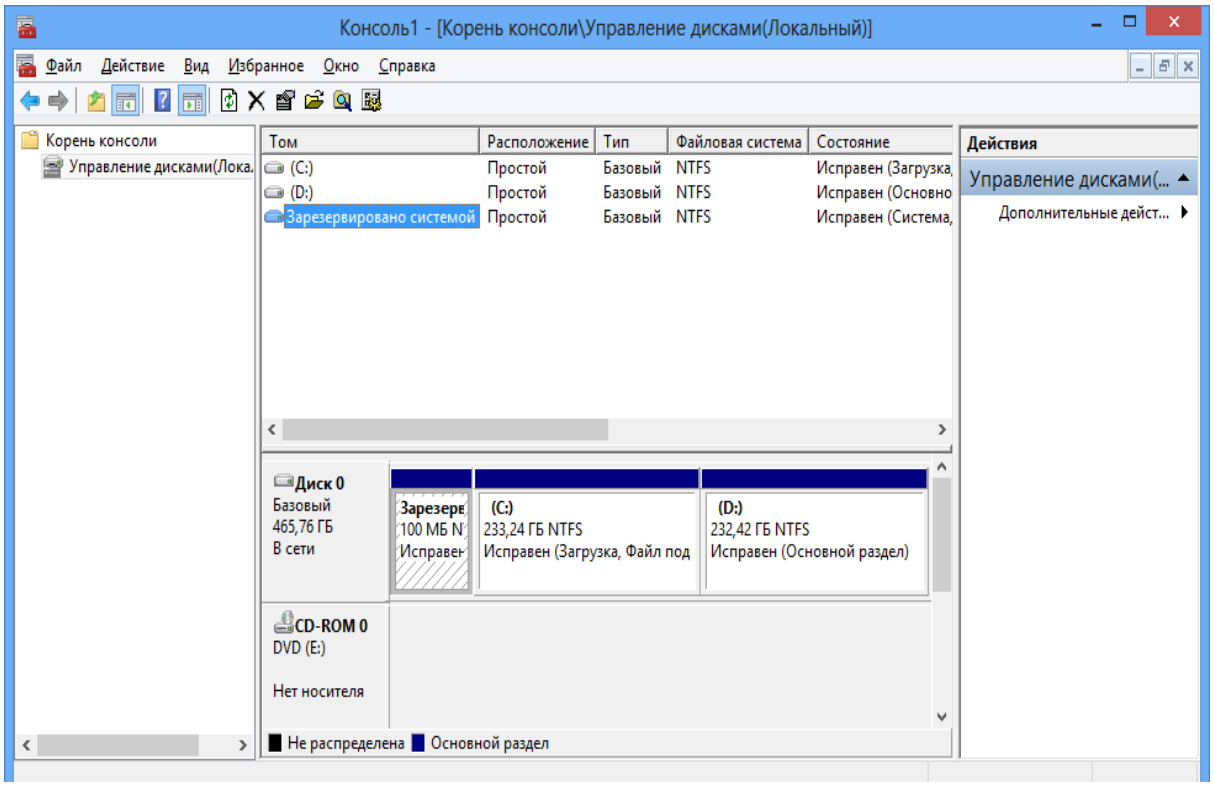

Рис. 2.4 – Управление дисками

При создании логического диска необходимо отформатировать раздел в файловой системе NTFS. В открывшемся окне можно установить размер кластера на диске, присвоить диску собственную метку и др. Добавить раздел можно с помощью контекстного меню (рис. 2.5). При форматировании диска метку раздела назначить как Docs (рис. 2.6).

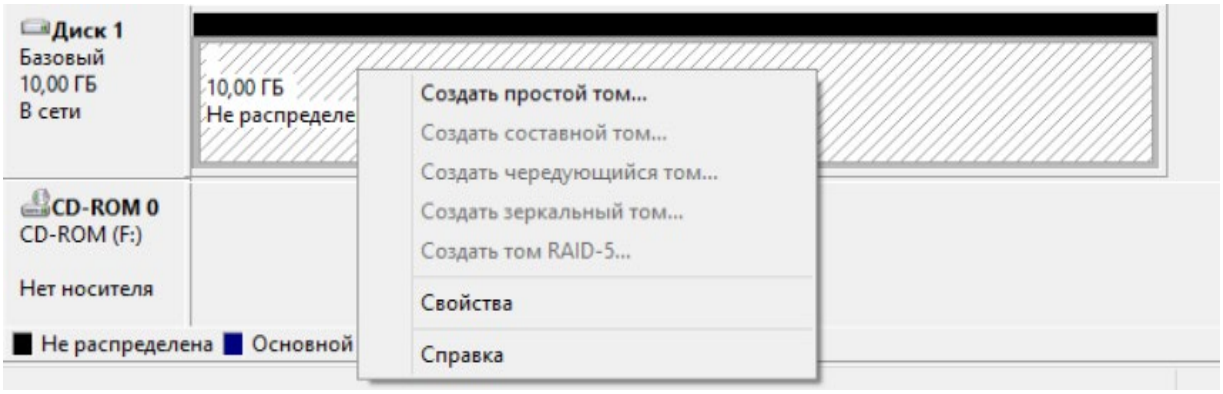

Рис. 2.5 – Создание логического диска

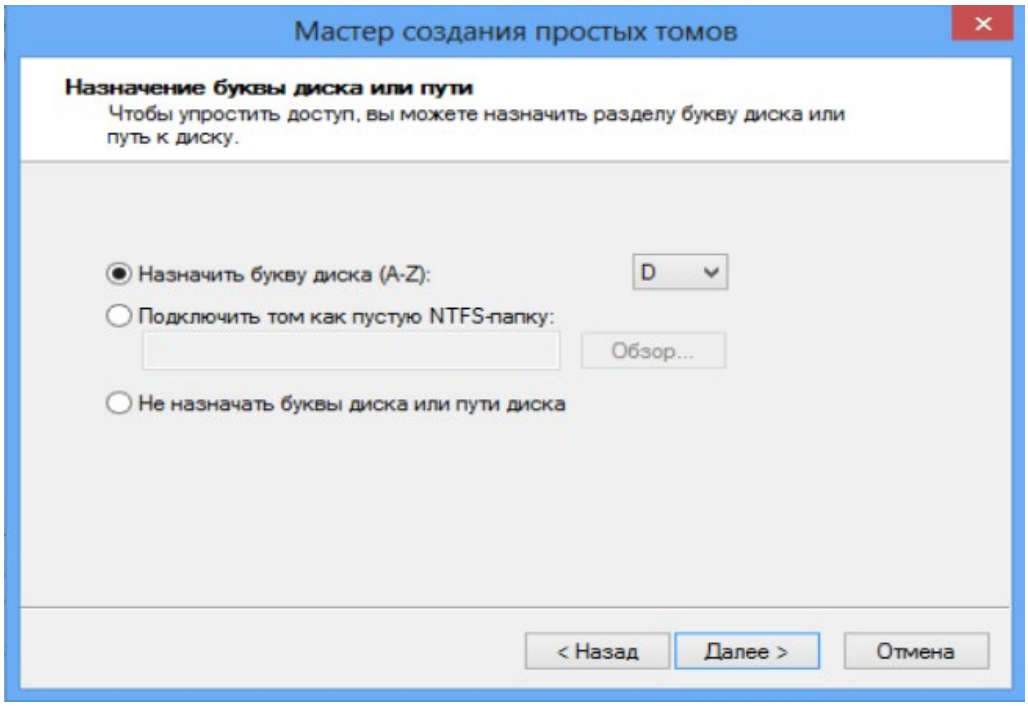

Рис. 2.6 – Создание нового тома

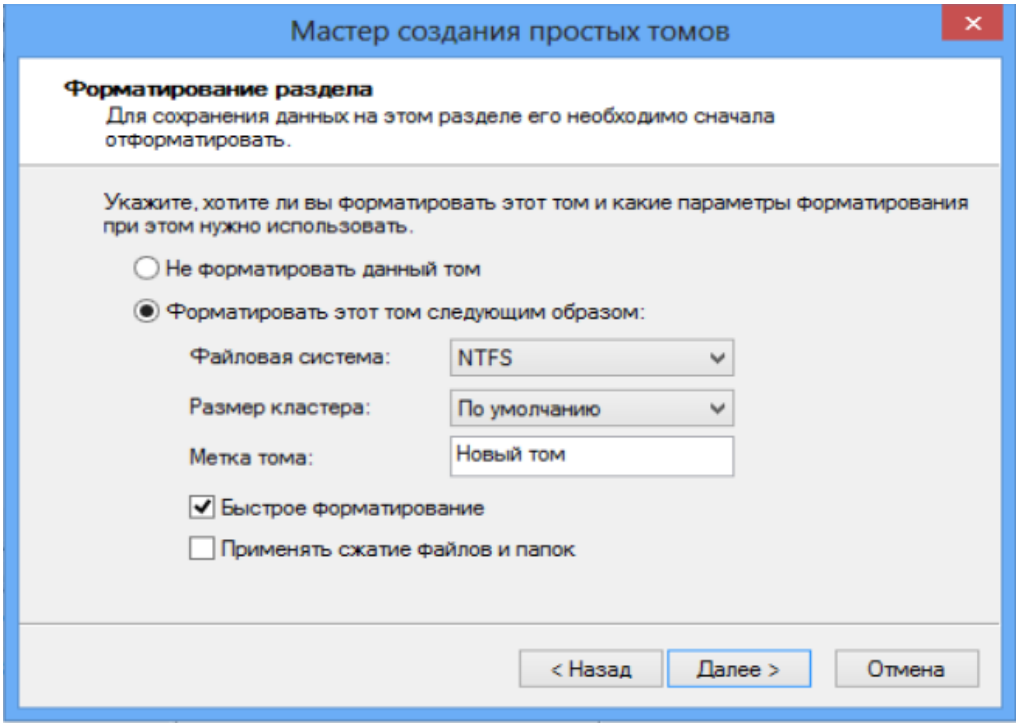

Рис. 2.7 – Форматирование нового логического диска

Измените метку логического диска C:\ на System. Метка существующего диска изменяется на вкладке «Общие» свойств диска (рис. 2.8).

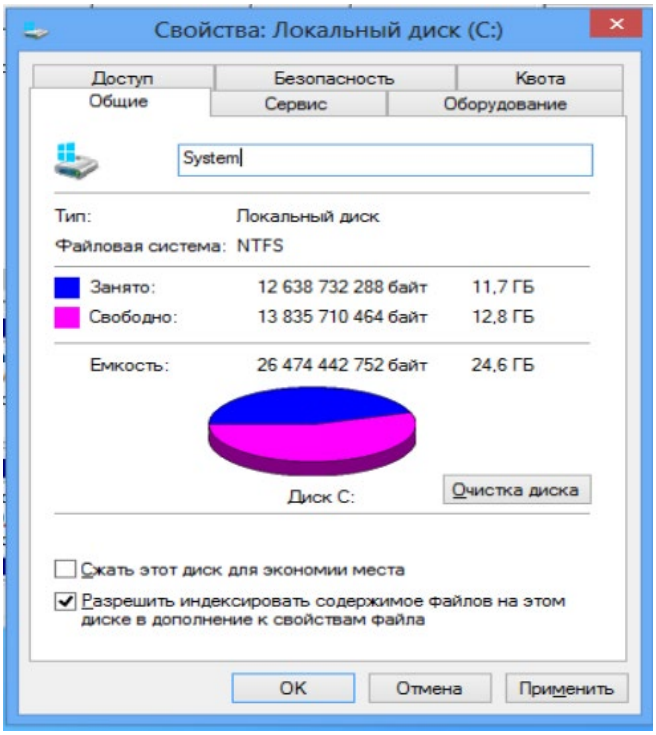

Рис. 2.8 – Окно «Свойства логического диска»

Измените букву диска CD-ROM на E:\. Чтобы изменить букву диска, в контекстном меню диска выберите «Изменить букву диска или путь к диску» (рис. 2.9). При изменении буквы диска необходимо убедиться, что эта буква не задействована.

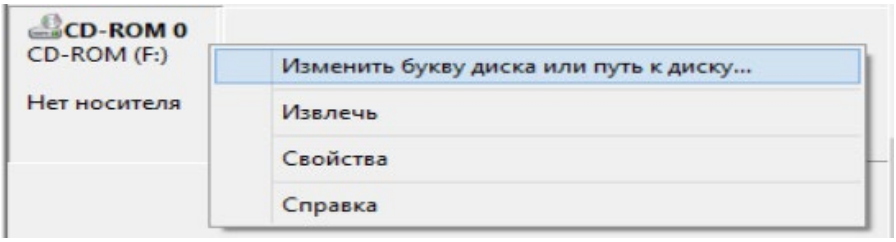

Рис. 2.9 – Контекстное меню управления логическим диском

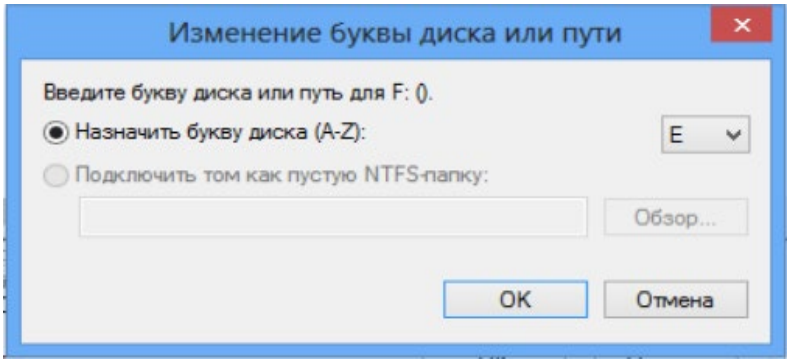

Рис. 2.10 – Изменение буквы диска

2.1.1 Групповые политики

Откройте оснастку «Групповая политика» («Пуск – Выполнить – gpedit.msc»). Оснастка «Групповая политика» состоит из двух основных частей: конфигурация компьютера и конфигурация пользователя.

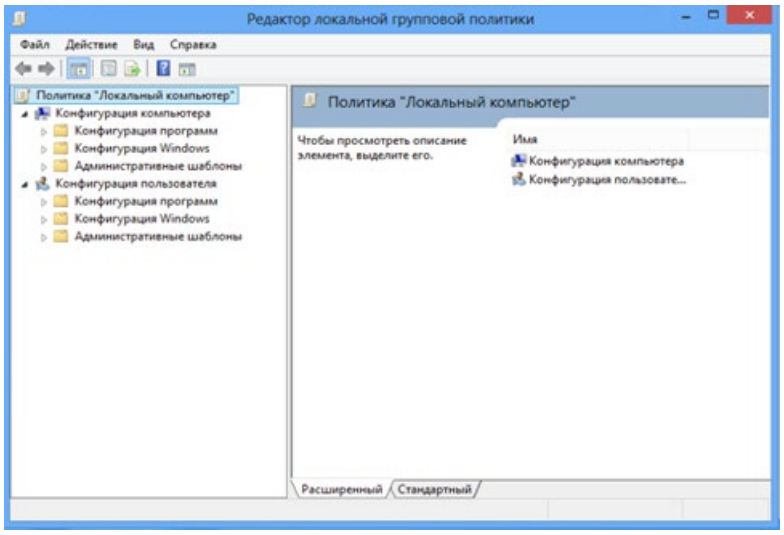

Рис. 2.11 – Редактор групповых политик

«Конфигурация компьютера» используется для задания политики, применяемой к компьютерам, вне зависимости от того, какой пользователь работает на них. «Конфигурация пользователя» используется для задания политики, применяемой к пользователям независимо от того, какой компьютер используется для входа в систему.

Созданная групповая политика может быть экспортирована на другой локальный компьютер. Для того чтобы произвести экспорт данных необходимо в оснастке «Групповая политика» выделить нужный узел и во вкладке «Действие» выбрать пункт «Экспортировать список». В появившемся окне выбрать путь сохранения и указать имя файла.

«Конфигурация компьютера» по умолчанию состоит из следующих разделов: конфигурация программ, конфигурация Windows и административные шаблоны.

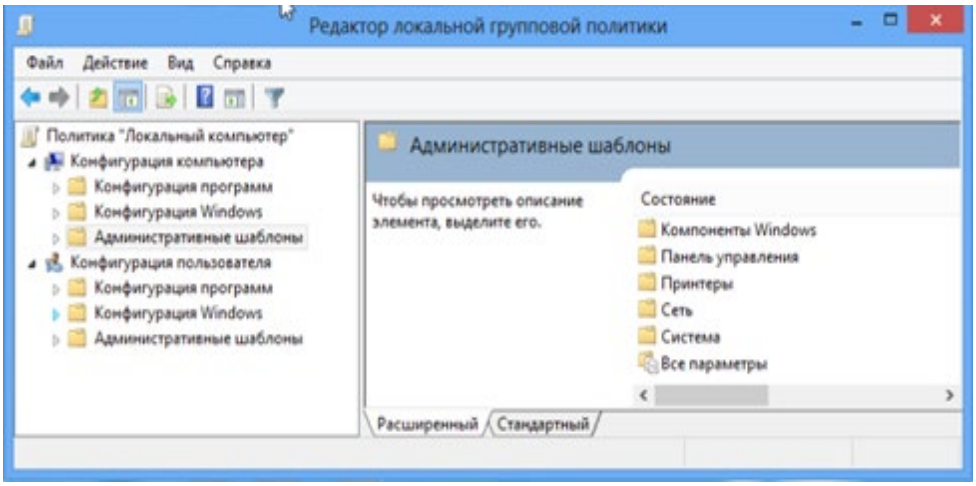

Рис. 2.12 – Раздел «Административные шаблоны»

Средствами виртуальной машины подключите компакт-диск. В разделе «Административные шаблоны» выберите подраздел «Компоненты Windows – Политики автозапуска». Включите параметр «Выключение автозапуска» (рис. 2.13) Чтобы проверить выполнение данного параметра, необходимо повторно вставить диск в CD-привод. Система не будет производить его автозапуск, как это делалось раньше.

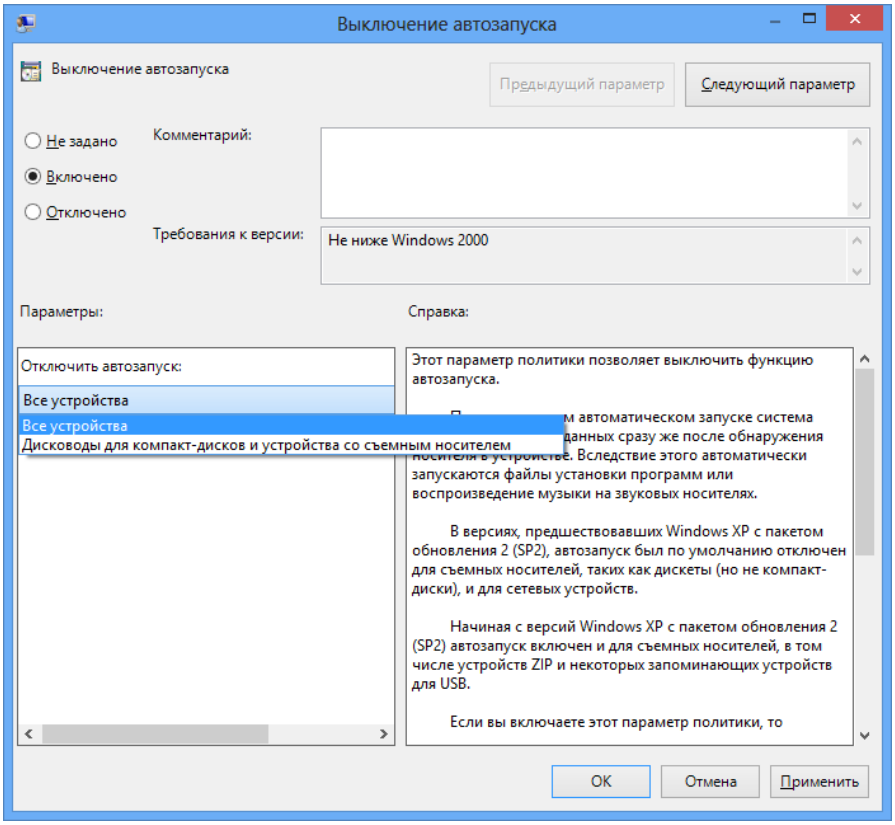

Рис. 2.13 – Выключение автозапуска носителя

В разделе «Система» откройте подраздел «Вход в систему» и выберите параметр «Выполнять эти программы при входе в систему». Включите этот параметр и добавьте несколько программ, которые будут запускаться при входе пользователя в систему (рис. 2.14, 2.15). Добавленные программы будут запускаться при каждом входе пользователя в систему. Для проверки повторно войдите в систему.

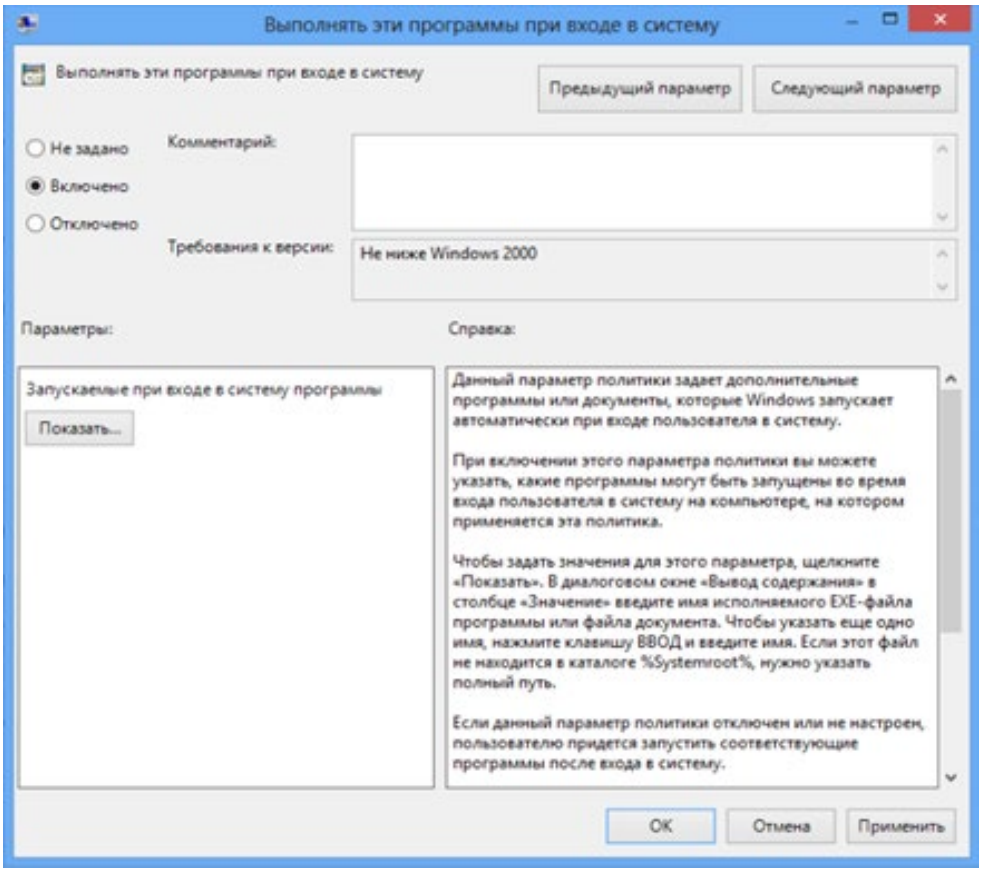

Рис. 2.14 – Включение параметра

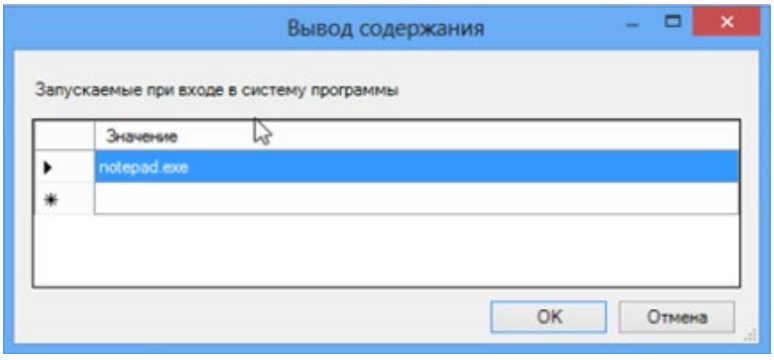

Рис. 2.15 – Список запускаемых программ

«Конфигурация пользователя» по умолчанию состоит из тех же разделов, что и «Конфигурация компьютера». При помощи параметров групповой политики существует возможность ограничения доступа пользователя к логическим дискам. Можно скрыть выбранный диск из «Проводника», а также запретить доступ к нему.

Выберите параметр «Запретить доступ к дискам через «Мой компьютер», расположенный в подразделе «Компоненты Windows – Проводник» и запретите доступ к логическому диску D:\ (рис. 2.16).

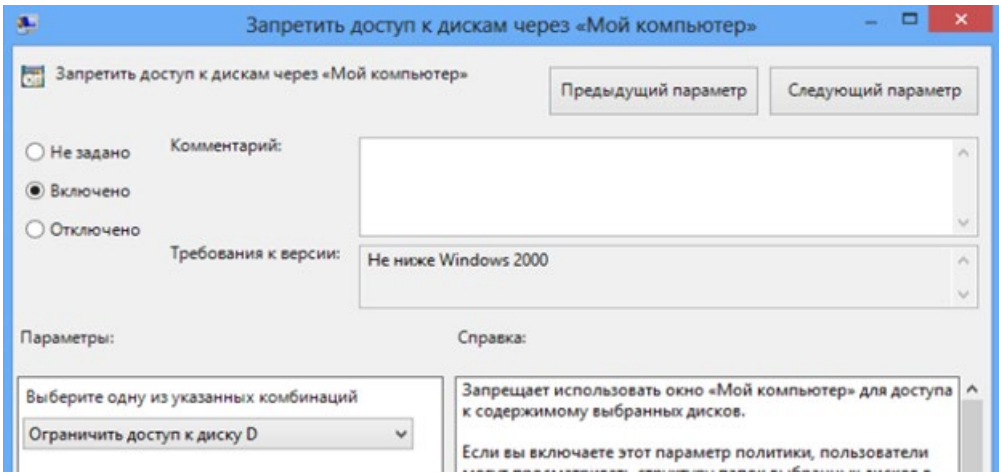

Рис. 2.16 – Включение ограничения доступа к диску D

Попытайтесь открыть диск D:\ через «Мой компьютер» (рис. 2.17) и командную строку (рис. 2.18). В первом случае система откажет в доступе, а во втором – доступ будет предоставлен (т. к. доступ запрещён только через «Проводник»).

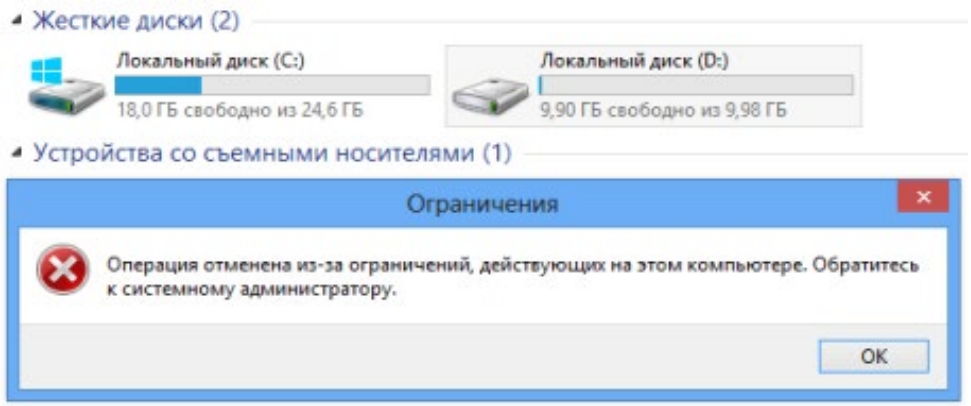

Рис. 2.17 – Попытка доступа через проводник

Рис. 2.18 – Попытка доступа через командную строку

Ограничение доступа к средствам администрирования возможно за счёт запрета доступа к «Панели управления». Включите параметр «Запретить доступ к панели управления», находящийся в подразделе «Панель управления». Попытайтесь открыть «Панель управления» – будет возвращена ошибка доступа (рис. 2.19).

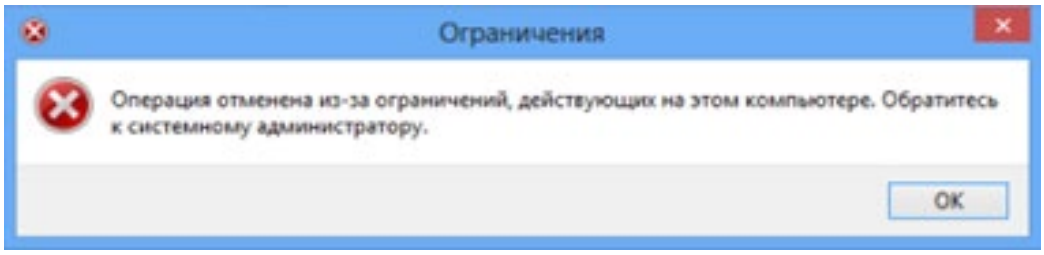

Рис. 2.19 – Ошибка при открытии панели управления

Для полного запрета использования командной строки включите параметр «Запретить использование командной строки» в подразделе «Система». Попытайтесь запустить cmd.exe (рис. 2.20).

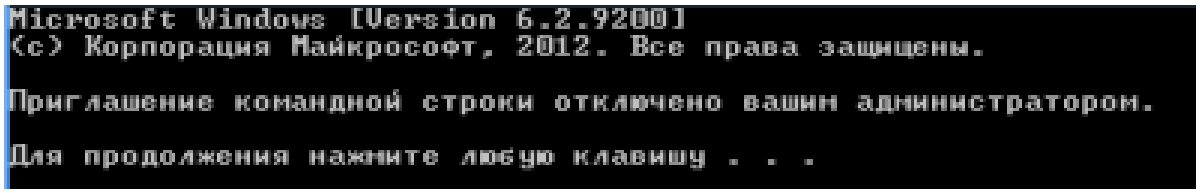

Рис. 2.20 – Попытка запуска командной строки

Кроме того, в подразделе «Система» можно запретить использование редактора реестра. Для этого нужно включить параметр «Сделать недоступными средства редактирования реестра». Включите данный параметр и попытайтесь запустить редактор реестра C:\Windows\regedit.exe.

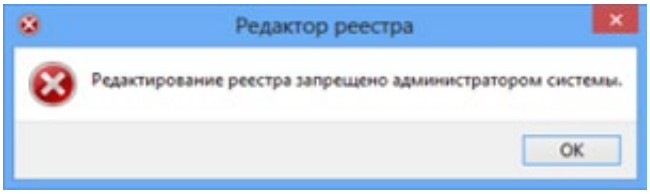

Рис. 2.21 – Попытка запуска реестра

Добавление и удаление шаблонов может производиться через контекстное меню раздела «Административные шаблоны» (рис. 2.22). В появившемся контекстном меню выберите «Добавление и удаление шаблонов». В появившемся окне можно удалить любой шаблон, а также добавить новый шаблон политики.

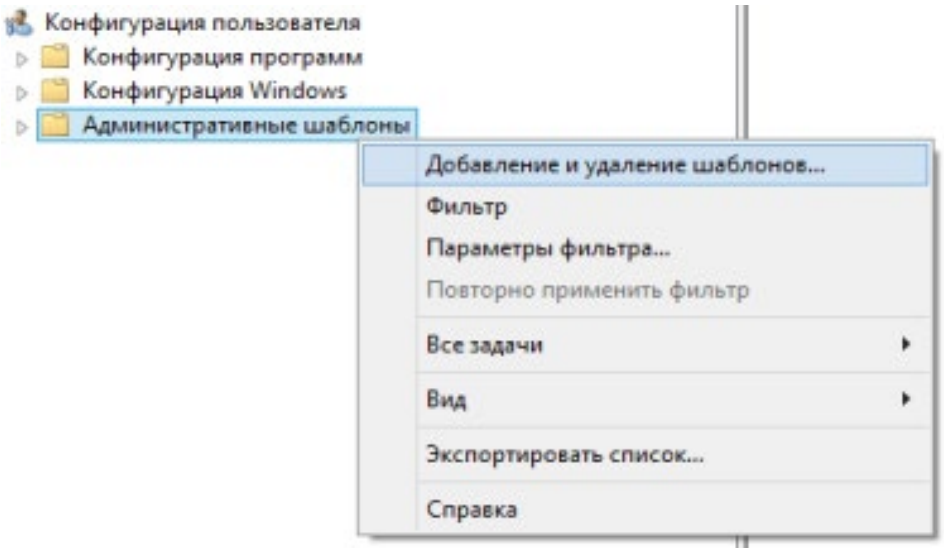

Рис. 2.22 – Контекстное меню административных шаблонов

2.2 Задание

Создайте новую консоль. Добавьте в корень консоли оснастки «Редактор объекта групповой политики» и «Результирующая политика». Установите параметры групповой политики и сохраните консоль в режиме, указанном в Вашем варианте (табл. 2.1).

Таблица 2.1 – Варианты работы с групповыми политиками

Вариант	Режим работы	Параметры групповой политики
1	Авторский	Запретить редактирование реестра. Ограничить размер профиля пользователя значением 5 МБ
2	Пользовательский – полный доступ	Запретить использование командной строки. Запретить изменение рисунка рабочего стола
3	Пользовательский – многооконный	Запретить использование сочетаний клавиш, включающих кнопку «Windows». Удалить имя пользователя из меню «Пуск»
4	Пользовательский – однооконный	Запретить использование диспетчера задач. Установить обязательный запрос пароля при выходе из спящего режима
5	Авторский	Запретить доступ к «Панели управления». Запретить запуск «Блокнота»
6	Пользовательский – полный доступ	Установить запрос пароля при выходе из экранной заставки. Удалить «Завершение сеанса» из меню «Пуск»
7	Пользовательский – многооконный	Скрыть диск D: (CD-привод) из окна «Мой компьютер». Удалить значок «Мои документы» с «Рабочего стола»
8	Пользовательский – однооконный	Удалить «Общие документы» из окна «Мой компьютер». Скрыть общие группы программ из меню «Пуск»
9	Авторский	Запретить доступ к диску C: из окна «Мой компьютер». Удалить «Сетевые подключения» из меню «Пуск»
10	Пользовательский – полный доступ	Запретить вызов «Свойств» объекта «Мой компьютер». Установить очистку списка последних использовавшихся документов при выходе из системы

Контрольные вопросы

1. Для чего применяется MMC?

2. Что такое оснастка?

3. Чем отличается авторский режим консоли MMC от пользовательского режима?

4. Чем отличается пользовательский многооконный режим консоли MMC от пользовательского однооконного режима?

5. В чём состоит отличие конфигурации компьютера от конфигурации пользователя в групповой политике?

6. Каким образом можно отключить автозапуск компакт-дисков через групповую политику?

7. Каким образом можно включить автозапуск программ через групповую политику?

8. Для чего предназначены административные шаблоны, создаваемые для групповых политик?

9. Каким образом можно добавить новый шаблон в групповую политику?

10. Для чего предназначена оснастка «Результирующая политика»?

3 ЛАБОРАТОРНАЯ РАБОТА № 3 «ДИСКРЕЦИОННЫЙ МЕХАНИЗМ РАЗГРАНИЧЕНИЯ ДОСТУПА»

Целью лабораторной работы является практическое изучение дискреционного механизма разграничения доступа на основе встроенных средств операционной системы Windows 8, позволяющих управлять доступом к файлам и папкам файловой системы NTFS.

3.1 Руководство по разграничению доступа

Основная задача механизмов управления доступом состоит в разграничении доступа субъектов (пользователей и запускаемых ими процессов) к защищаемым информационным и техническим ресурсам – объектам. Задача логического управления доступом состоит в том, чтобы для каждой пары «субъект-объект» определить множество допустимых операций (зависящее, быть может, от некоторых дополнительных условий) и контролировать выполнение установленного порядка.

В системе не должна предоставляться возможность несанкционированного обмена данными между пользователями (при этом механизм санкционированного обмена данными должен предоставляться). Кроме того, прикладной пользователь не должен иметь доступ к настройкам, связанным с безопасностью системы.

Войдите в операционную систему под учётной записью «Администратор».

Для применения правил разграничения доступа необходимо воспользоваться вкладкой «Безопасность». Если она отключена, её необходимо активировать. Для этого необходимо в разделе «Параметры папки» (введите в поиске меню «Пуск») включить опцию «Использовать мастер общего доступа» (рис. 3.1).

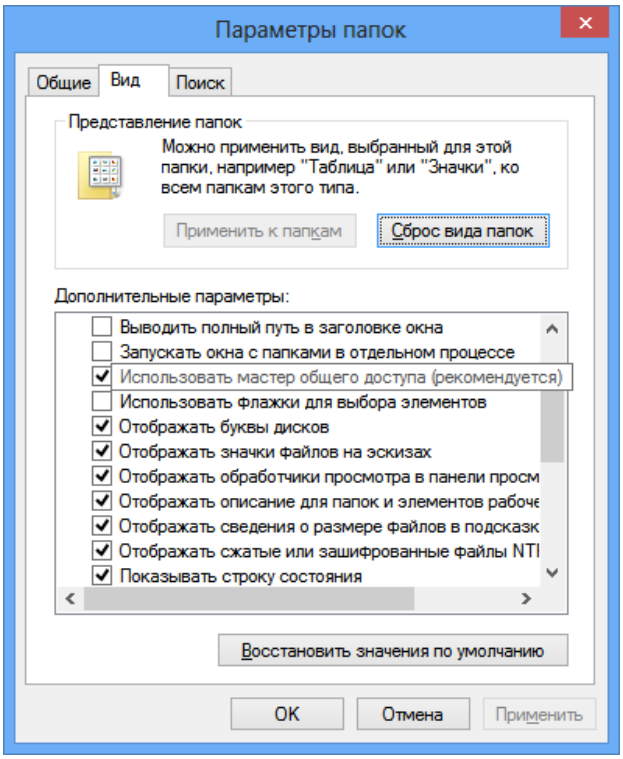

Рис. 3.1 – Раздел «Свойства папки»

3.1.1 Основные права доступа к файловым объектам

В NTFS все разрешения сводятся к шести стандартным разрешениям («Полный доступ», «Изменить», «Чтение и выполнение», «Список содержимого папки», «Чтение», «Запись»). Данные разрешения могут предоставляться пользователю (или группе пользователей) на доступ к объектам – каталогам и файлам. Право «Полный доступ» не только включает в себя все остальные разрешения, но и позволяет управлять разграничением доступа к данному объекту.

Назначение прав доступа пользователей осуществляется для каждого объекта. Назначить или изменить права доступа можно в «Свойствах» выбранного каталога или файла во вкладке «Безопасность». Сначала необходимо выбрать пользователя (или группу), которому будут назначаться разрешения.

Откройте вкладку «Безопасность» в «Свойствах» каталога «C:\Список содержимого папки». Для изменения списка пользователей, имеющих право

на доступ к объекту, нажмите на кнопку «Добавить» и выберите пользователя user (рис. 3.2).

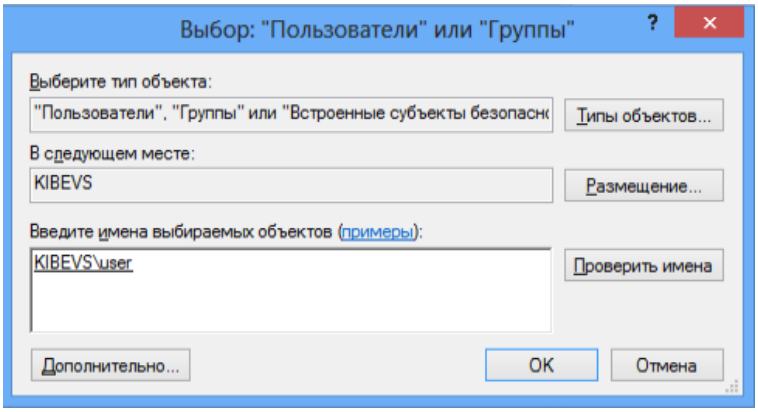

Рис. 3.2 – Добавление нового пользователя

Установите пользователю user разрешение «Список содержимого папки» на доступ к текущему каталогу «C:\Список содержимого папки» (рис. 3.3).

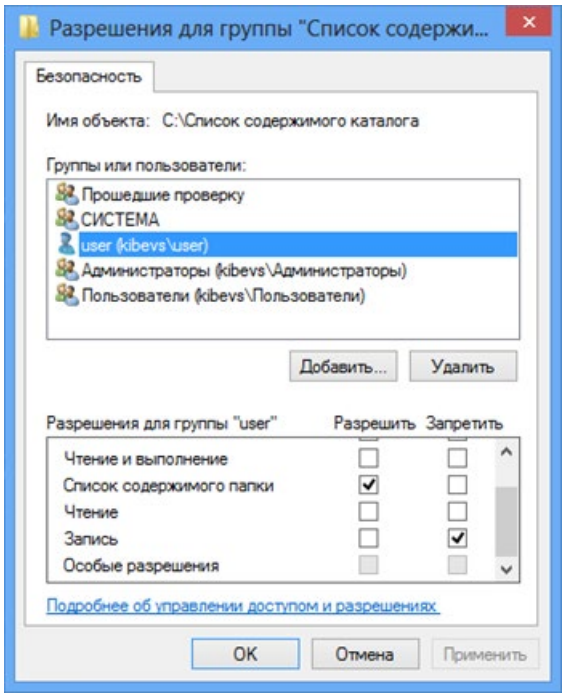

Рис. 3.3 – Установка разрешения «Список содержимого папки»

Аналогично для пользователя user установите разрешения на каталоги «Чтение», «Чтение и выполнение», «Запись», «Изменение» и «Полный доступ», соответствующие названиям этих каталогов (рис. 3.4–3.8).

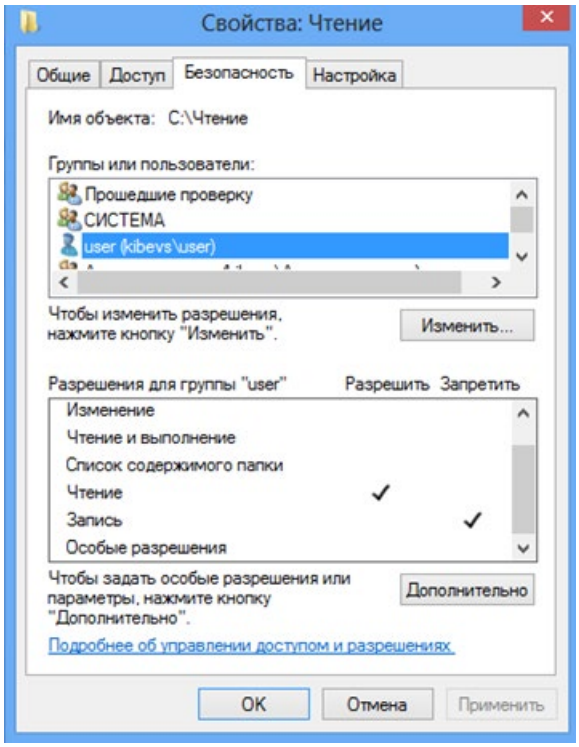

Рис. 3.4 – Установка разрешения «Чтение»

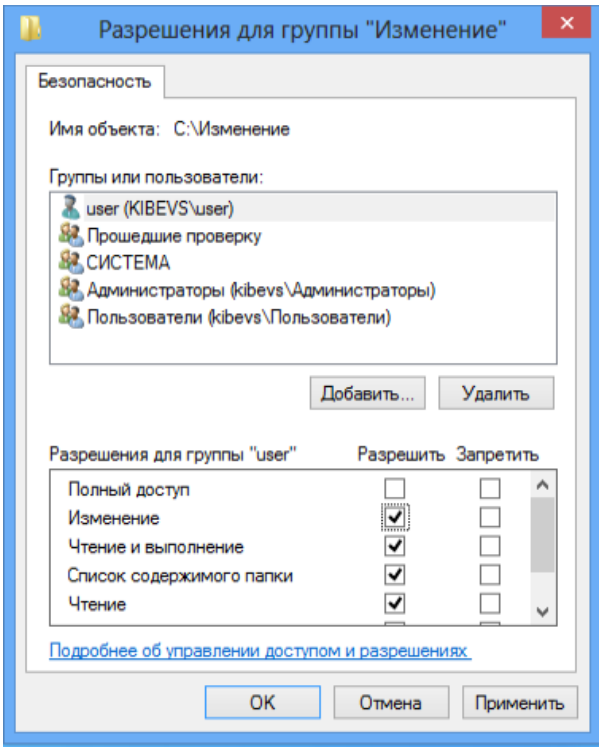

Рис. 3.5 – Установка разрешения «Изменить»

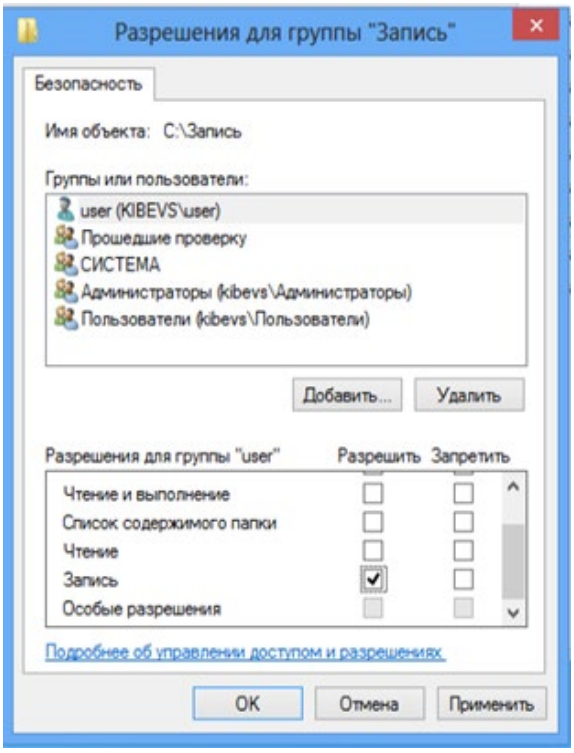

Рис. 3.6 – Установка разрешения «Запись»

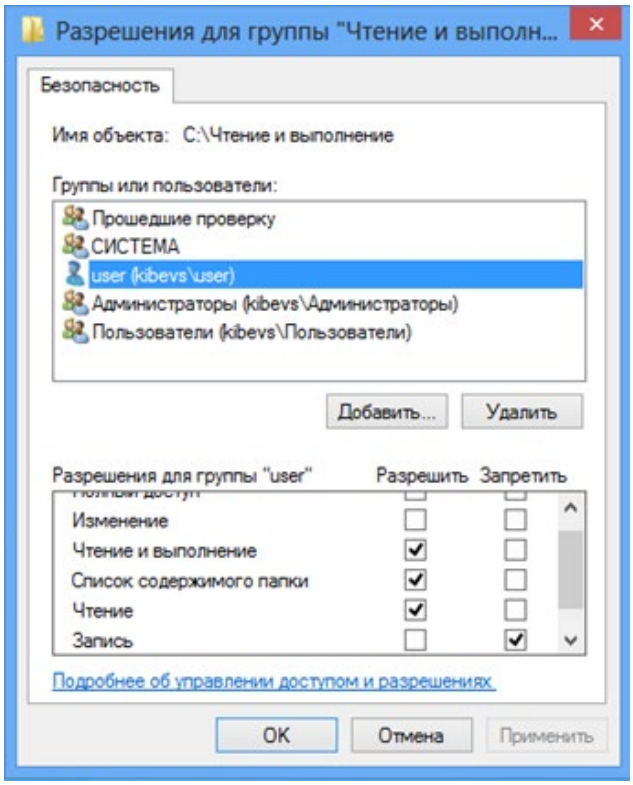

Рис. 3.7 – Установка разрешения «Чтение и выполнение»

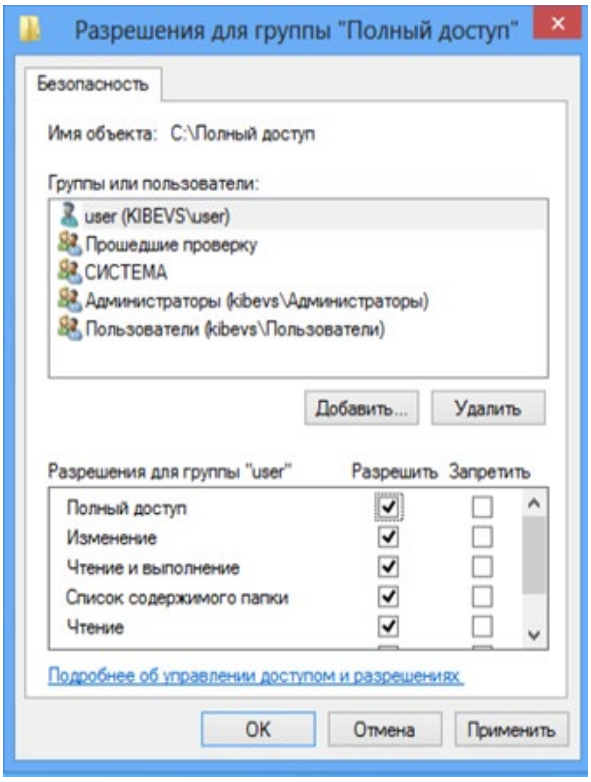

Рис. 3.8 – Установка разрешения «Полный доступ»

Разрешение «Список содержимого папки» предоставляет возможность просмотреть перечень объектов в данном каталоге. Войдите в соответствующий каталог и попытайтесь скопировать файл. Операционная система выдаст ошибку доступа к этому файлу (рис. 3.9). Попытайтесь открыть текстовый файл.

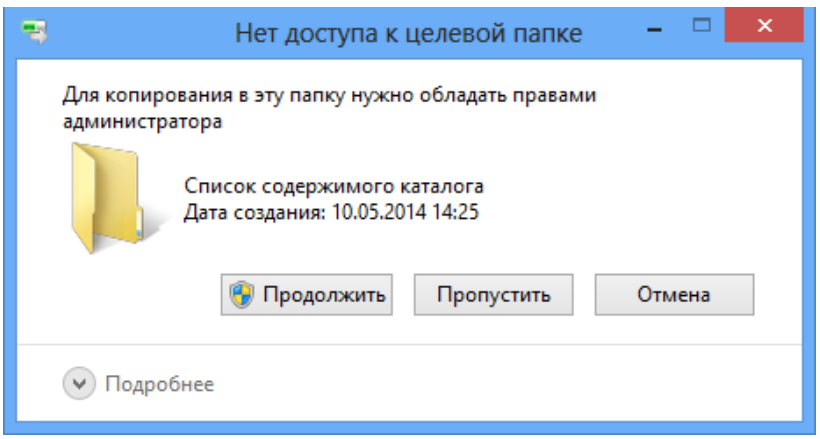

Рис. 3.9 – Ошибка доступа к копированию в папку

Разрешение «Чтение» предоставляет возможность открывать в данном каталоге все файлы, кроме исполняемых. Войдите в соответствующий каталог и откройте текстовый файл. Измените текст в открытом файле и попытайтесь сохранить его. Операционная система выдаст ошибку доступа на создание файла. Попытайтесь запустить исполняемый файл для проверки отказа в доступе.

Разрешение «Чтение и выполнение» предоставляет возможность открывать в данном каталоге все файлы. Войдите в соответствующий каталог и запустите исполняемый файл. Откройте текстовый файл, измените в нём текст и попытайтесь сохранить для проверки отказа в доступе на сохранение.

Разрешение «Запись» предоставляет возможность добавления файлов в данный каталог без права на доступ к вложенным в него объектам, в том числе на просмотр содержимого каталога. Попытайтесь войти в данный каталог. Операционная система выдаст ошибку доступа к каталогу (рис. 3.10).

Для проверки возможности добавления файла создайте файл с именем «Запись» (например, на «Рабочем столе») и попытайтесь перетащить его в каталог «Запись». Операционная система выдаст ошибку копирования, т. к. файл с таким именем в каталоге существует. Переименуйте файл и повторно попытайтесь его перетащить – копирование выполнится (кроме того, наличие файла в каталоге можно проверить под учётной записью «Администратор»).

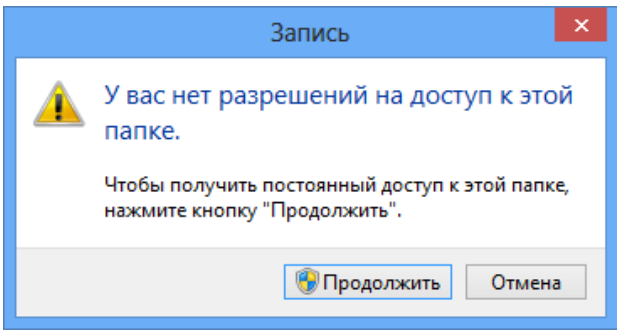

Рис. 3.10 – Ошибка доступа к каталогу

Разрешение «Изменить» предоставляет возможность открывать и создавать (изменять) файлы в данном каталоге. Войдите в соответствующий каталог и запустите исполняемый файл. Откройте текстовый файл, измените в нём текст и сохраните его, создайте новый файл в каталоге. Откройте вкладку «Безопасность» у каталога «Изменение» или у любого вложенного файла и попытайтесь изменить права доступа к нему. Изменить права доступа нельзя (параметры включения разрешений неактивны), т. к. разрешение «Изменить» не включает возможность управления правами доступа (рис. 3.11).

Разрешение «Полный доступ» предоставляет все возможности для работы с каталогом и вложенными файлами, включая изменение разрешений. Для проверки откройте вкладку «Безопасность» каталога «Полный доступ» или у любого вложенного файла и измените права доступа к нему.

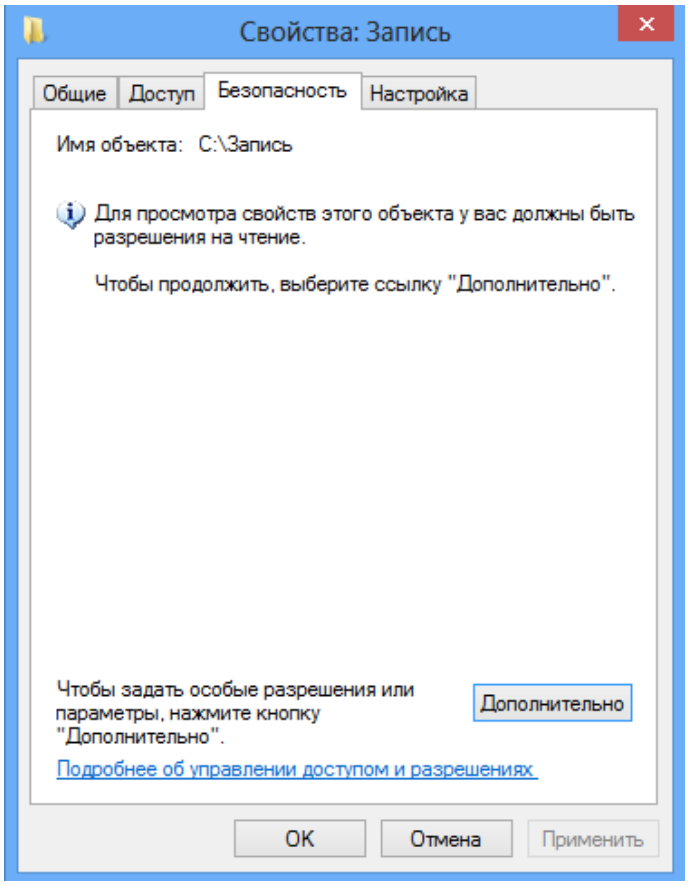

Рис. 3.11 – Невозможность изменения разрешений на доступ

3.1.2 Элементы разрешений на доступ

Каждое стандартное разрешение состоит из нескольких элементов. Элементы разрешений позволяют более гибко настраивать права доступа пользователей. Войдите под учётной записью «Администратор».

Просмотреть элементы разрешений на доступ можно, нажав на кнопку «Дополнительно» во вкладке «Безопасность» и выбрав любой элемент разрешений (рис. 3.12). Наборы элементов, включаемых в стандартные разрешения, приведены на рисунках 3.13–3.18.

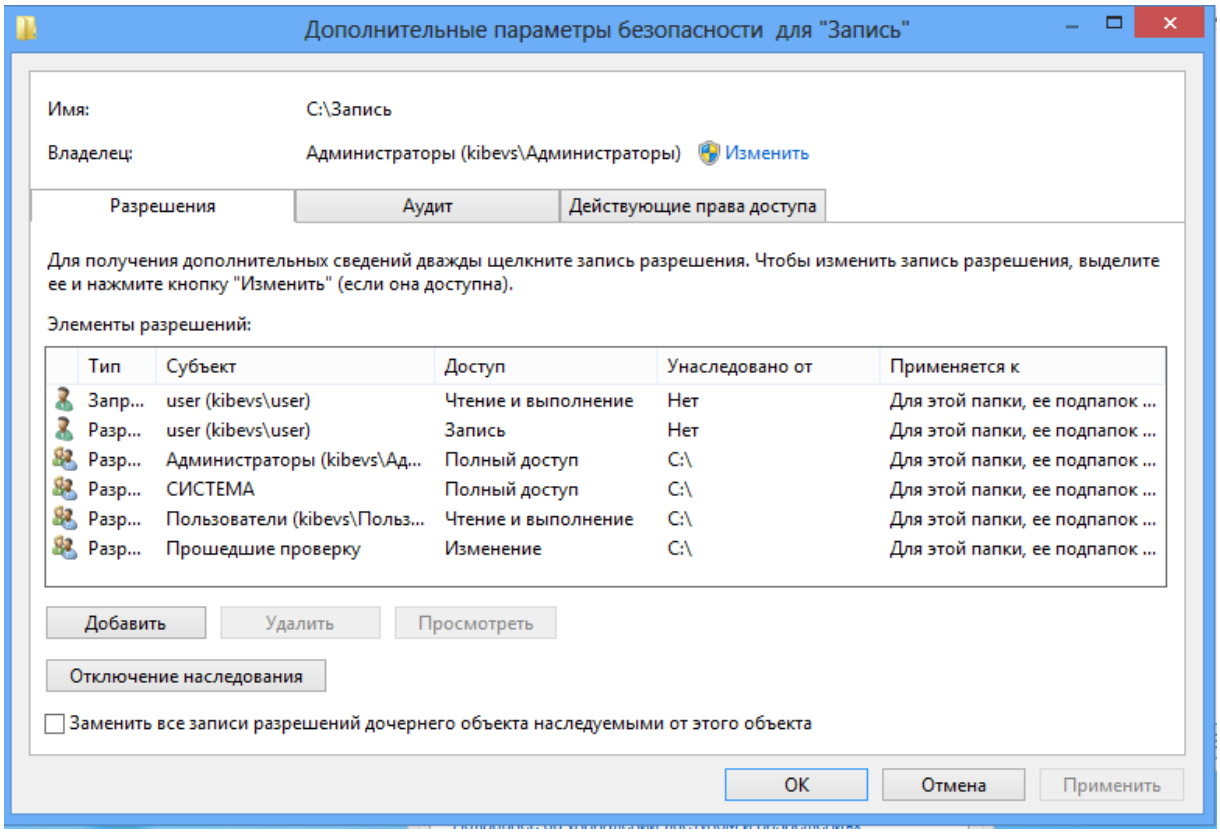

Рис. 3.12 – Дополнительные параметры безопасности

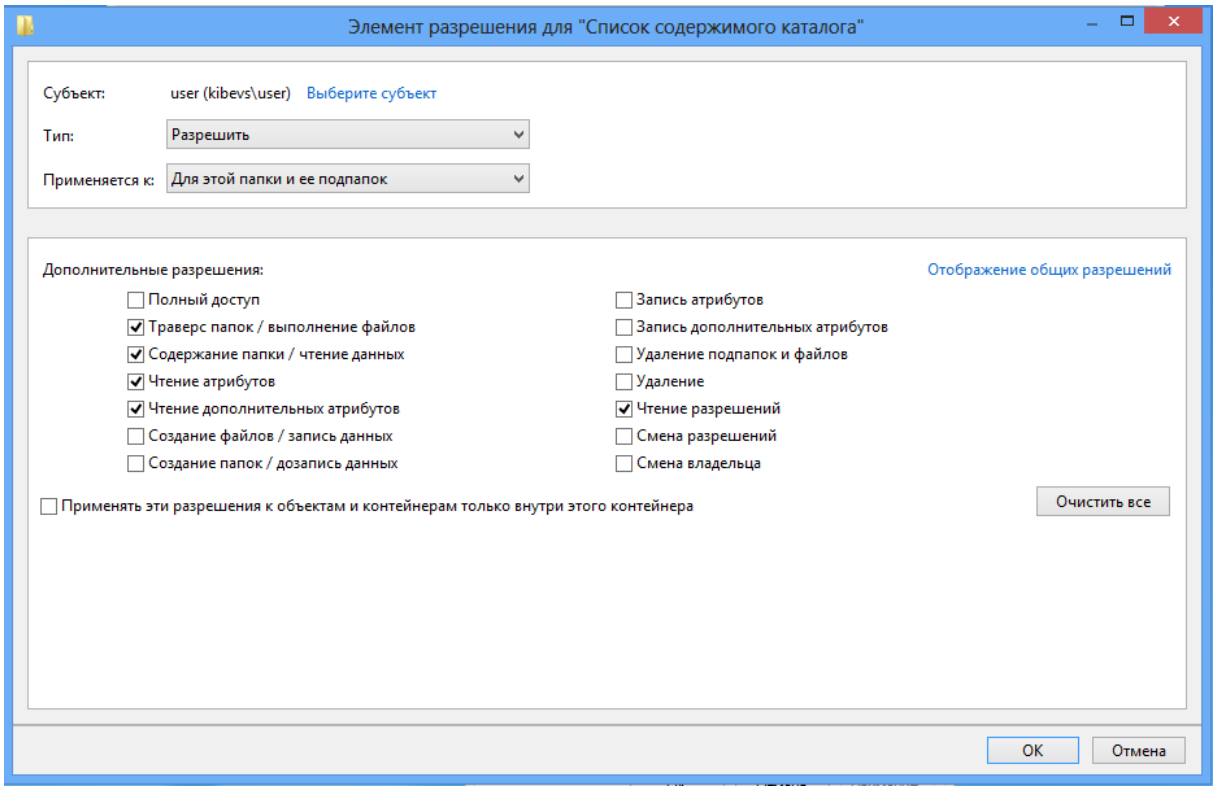

Рис. 3.13 – Элементы разрешений для «Списка содержимого папки»

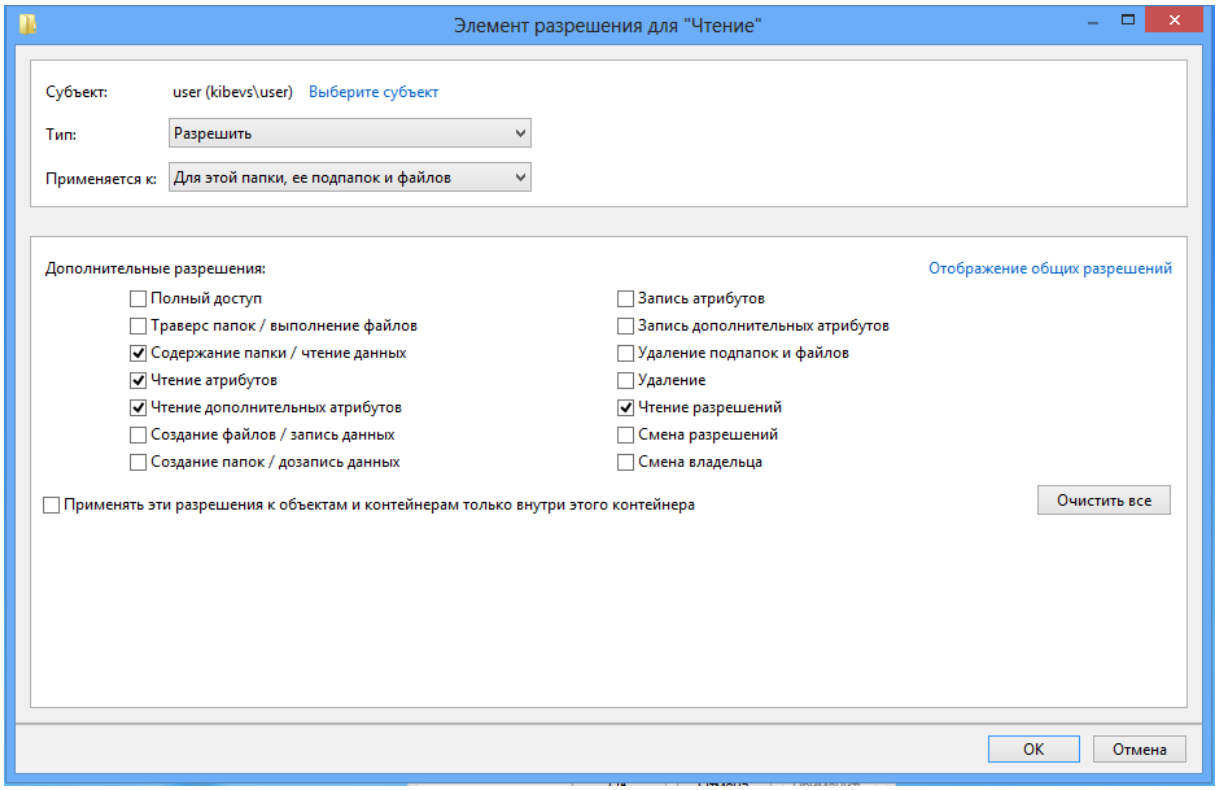

Рис. 3.14 – Элементы разрешений для «Чтения»

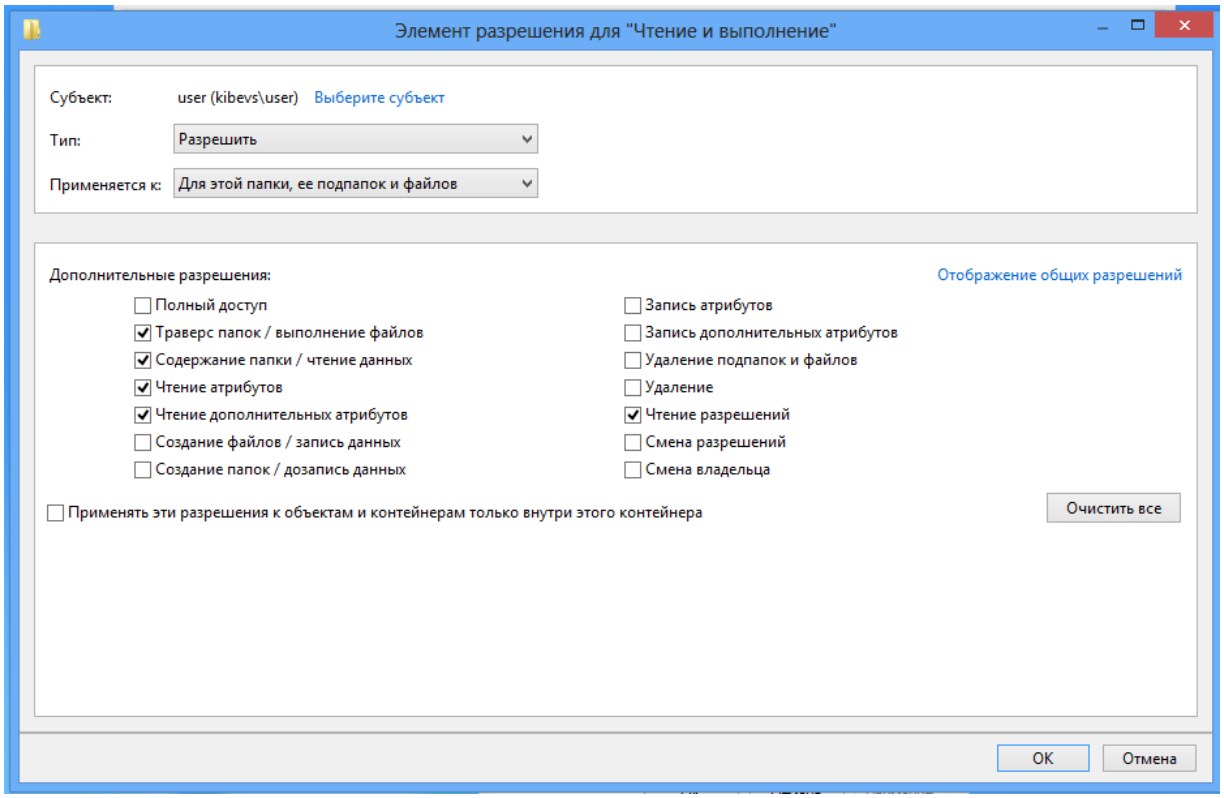

Рис. 3.15 – Элементы разрешений для «Чтения и выполнения»

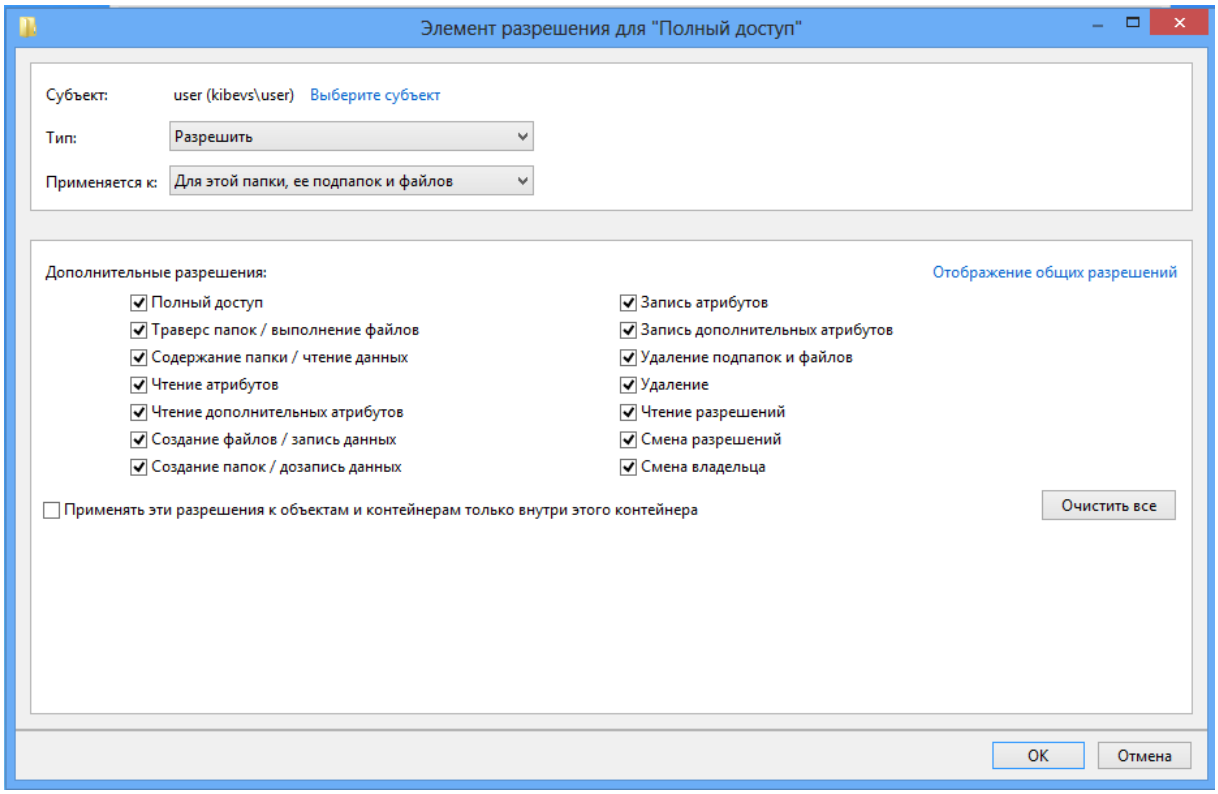

Рис. 3.16 – Элементы разрешений для «Полного доступа»

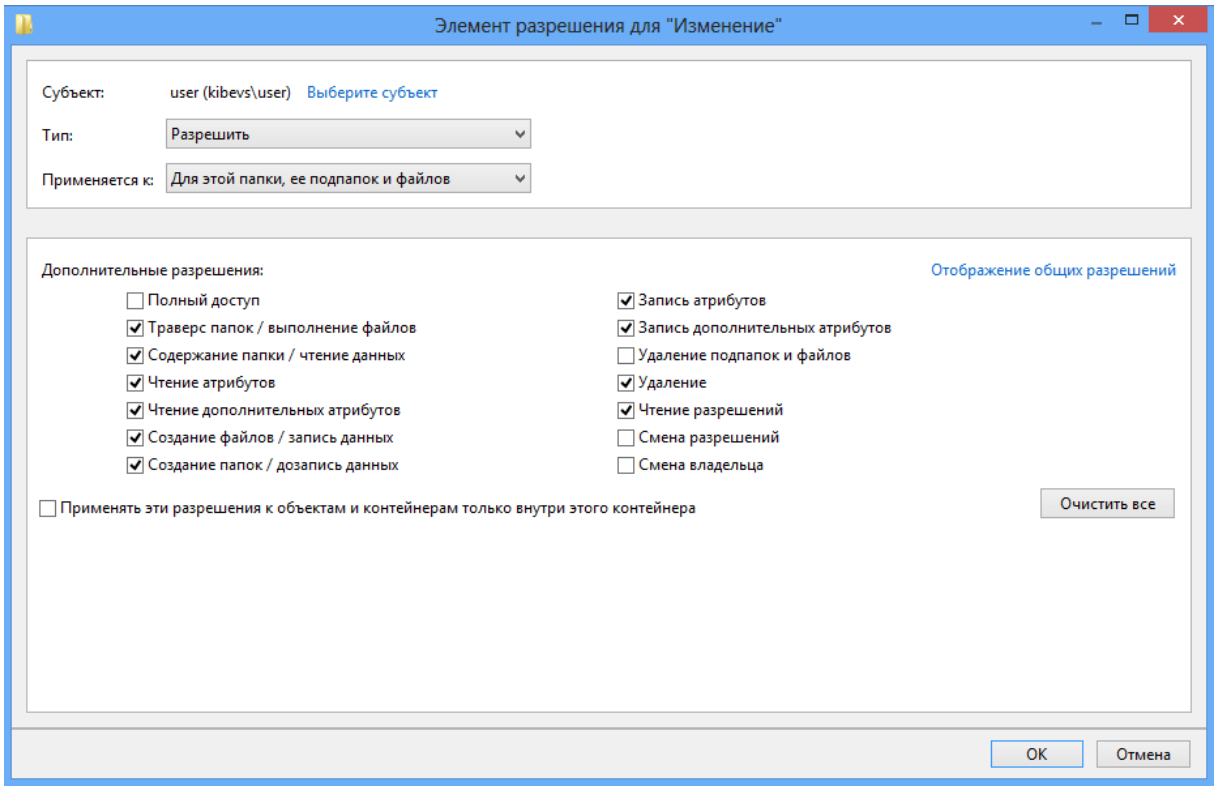

Рис. 3.17 – Элементы разрешений для «Изменить»

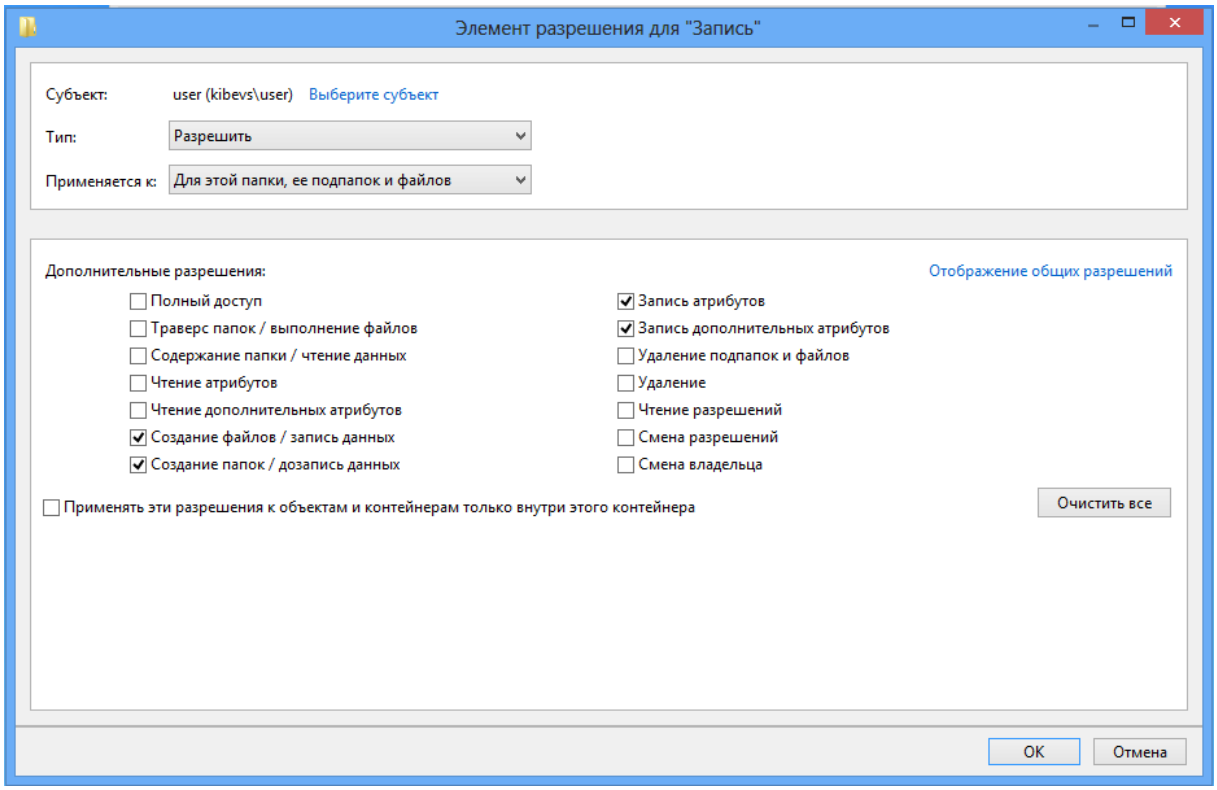

Рис. 3.18 – Элементы разрешений для «Записи»

Использование возможностей элементов разрешений наиболее оправдано при разграничении доступа на удаление файла или каталога. Через элементы разрешений запретите пользователю user удаление каталога «Изменение», а также разрешите запись атрибутов на каталог «Чтение» (рис. 3.19).

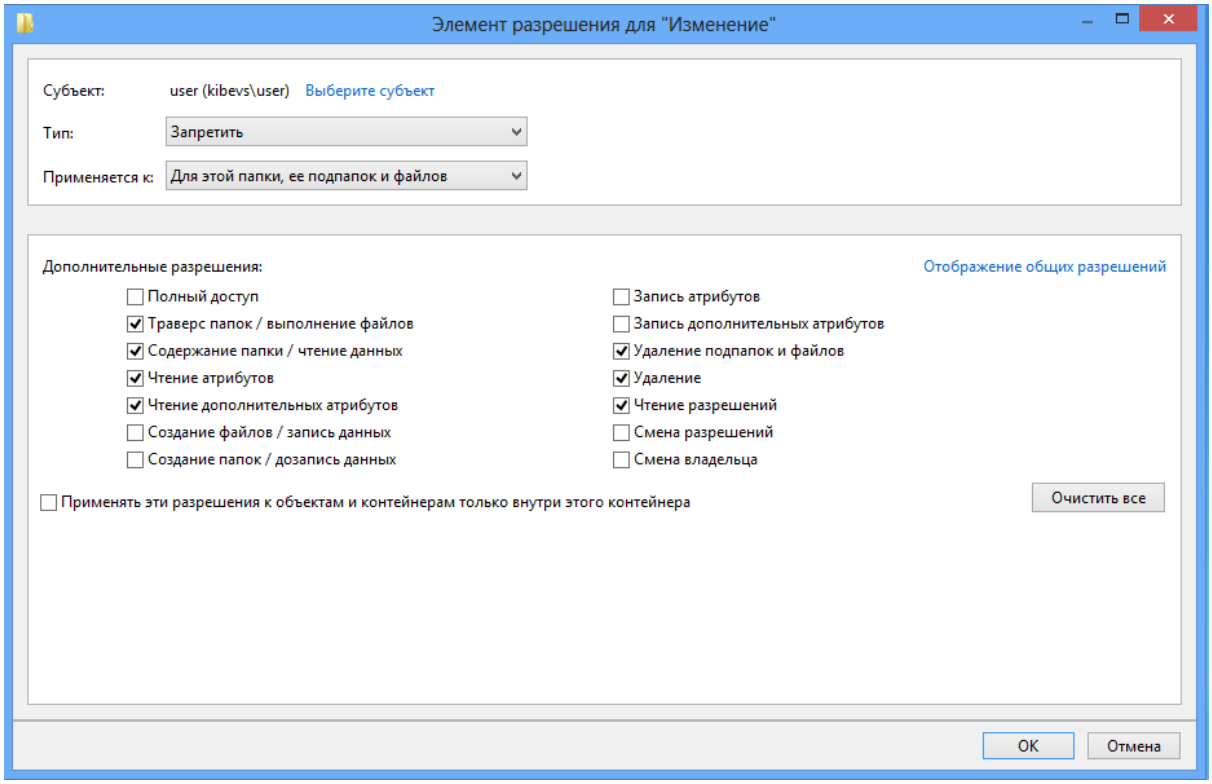

Рис. 3.19 – Запрет удаления

Для проверки установленных прав доступа войдите под учётной записью user. Попытайтесь удалить файл из каталога «Чтение». Операционная система выдаст ошибку доступа на удаление (рис. 3.21).

Измените атрибуты файла в каталоге «Чтение» (например, атрибут «Скрытый» в свойствах файла). Примените сделанные изменения. Измените дополнительные атрибуты текстового файла в каталоге «Чтение» (например, автора документа во вкладке «Сводка» свойств файла). Попытайтесь применить сделанные изменения. Операционная система выдаст ошибку сохранения дополнительных атрибутов (рис. 3.22).

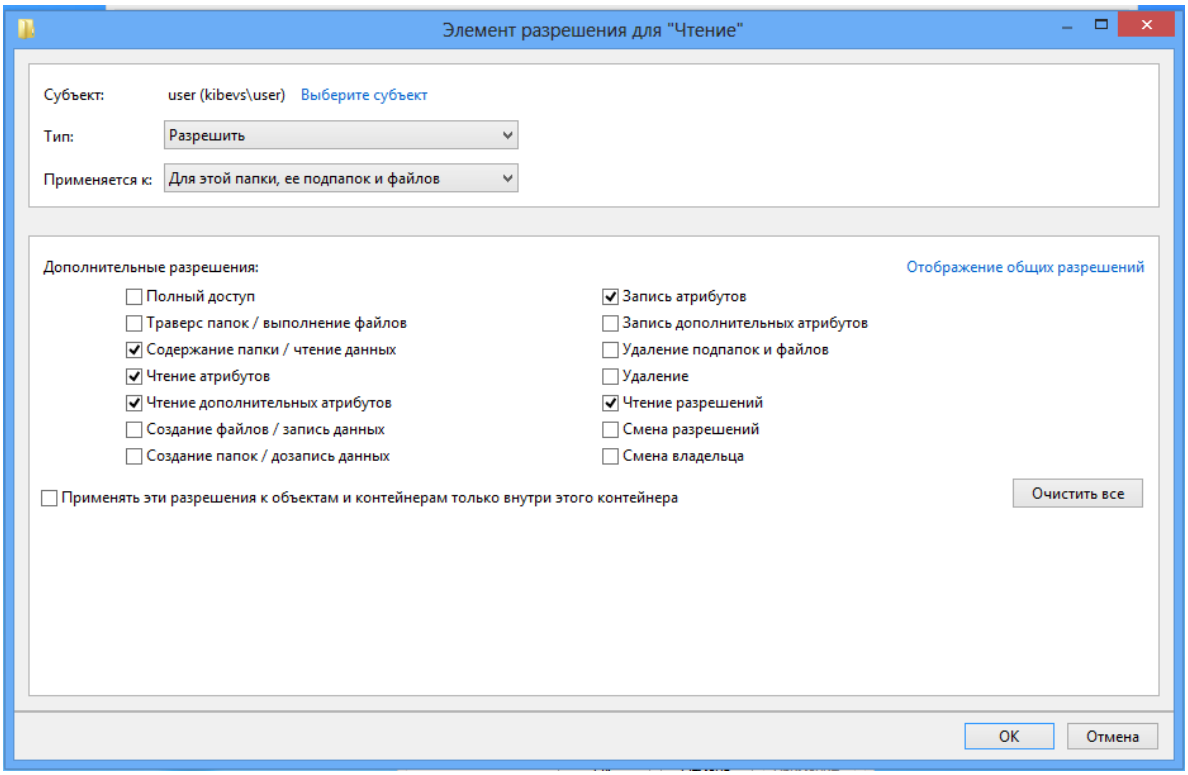

Рис. 3.20 – Разрешение записи атрибутов

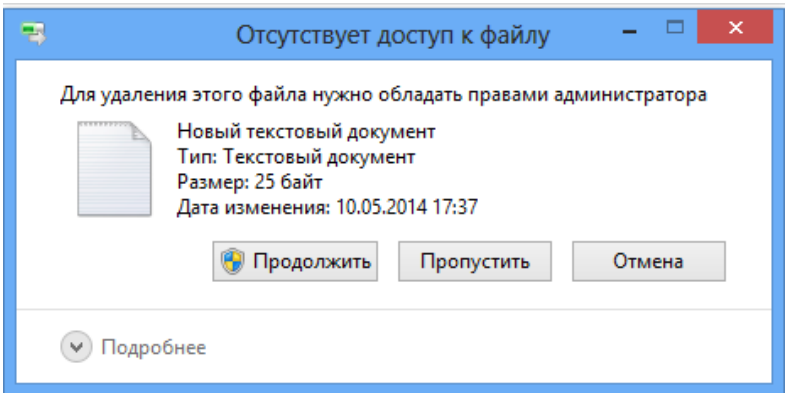

Рис. 3.21 – Ошибка доступа на удаление файла

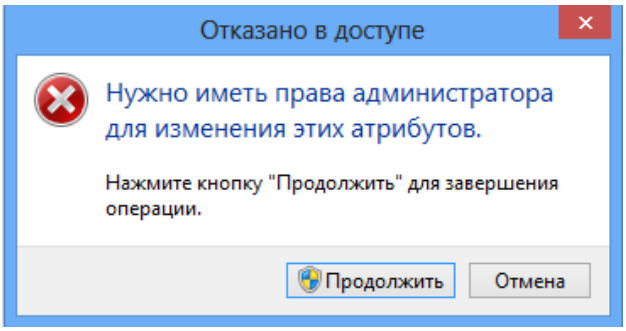

Рис. 3.22 – Ошибка доступа на изменение дополнительных атрибутов

3.1.3 «Владелец» файла

В файловой системе NTFS у каждого объекта есть владелец. Владелец управляет назначением разрешений на доступ к объекту независимо от установленных разрешений. Создайте под учётной записью user в каталоге «Изменение» новый каталог (например, «Новая папка») и в нём текстовый файл (например, «test.txt»). Скопируйте в созданный текстовый файл информацию из файла «Изменение». Откройте вкладку «Владелец» файла test.txt. В ней указывается текущий владелец объекта (рис. 3.23). Предоставьте полный доступ к созданному каталогу пользователю user1 (рис. 3.24).

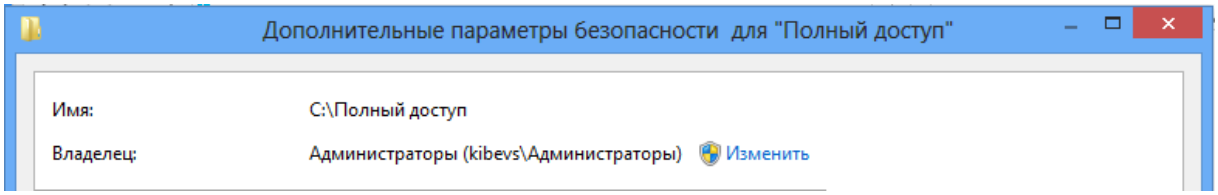

Рис. 3.23 – Значение «Владелец» для каталога

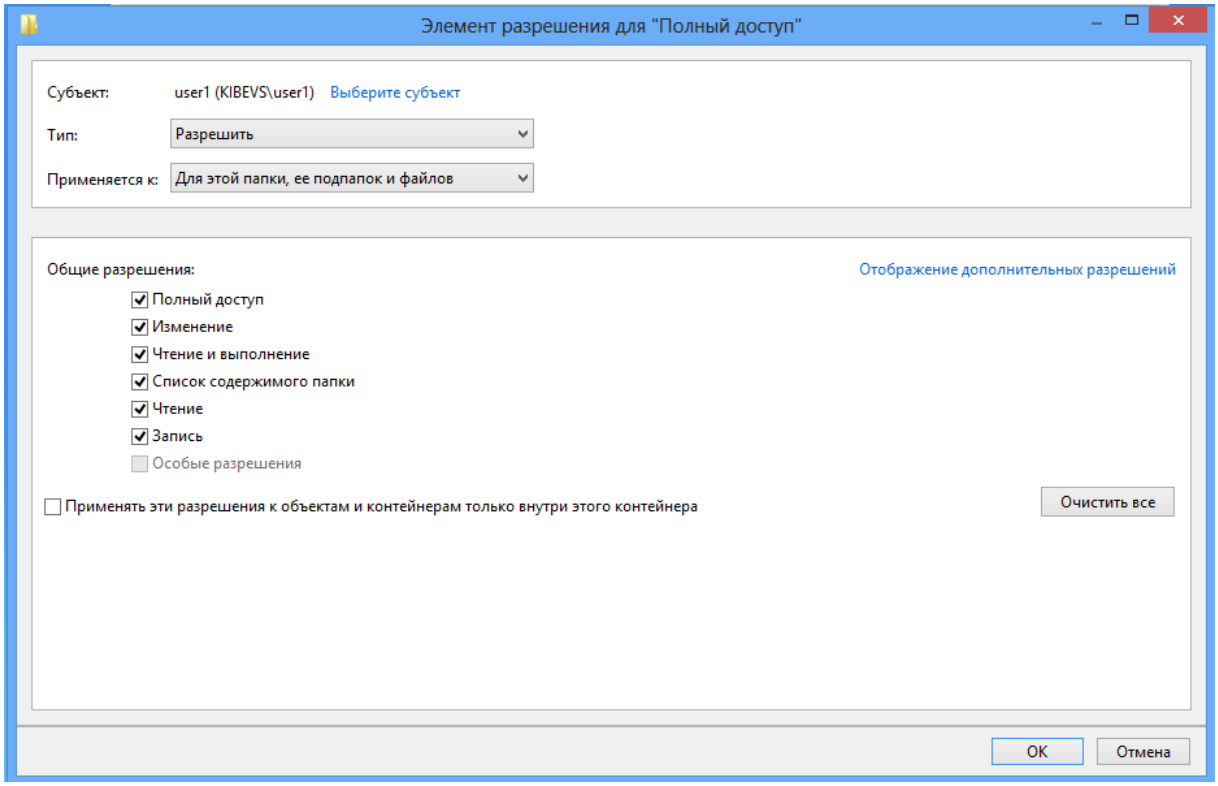

Рис. 3.24 – Предоставление прав пользователю user1

Войдите под учётной записью user1. Попытайтесь перейти в каталог «C:\Изменение\Новая папка» при помощи иерархического представления каталогов в «Проводнике». Переход невозможен, потому что у пользователя user1 нет доступа к промежуточным каталогам. Попытайтесь перейти в тот же каталог, указав его полный путь в адресной строке «Проводника» (рис. 3.25).

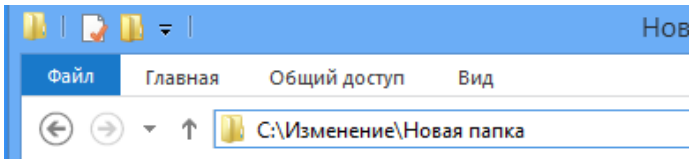

Рис. 3.25 – Доступ к каталогу через адресную строку

Откройте файл test.txt. Таким образом, пользователь user может несанкционированно предоставить доступ пользователю user1 к конфиденциальной информации.

Наличие полного доступа у пользователя user1 к каталогу test позволяет ему изменять разрешения. Запретите доступ пользователя «Администратор» к файлу test.txt (рис. 3.26).

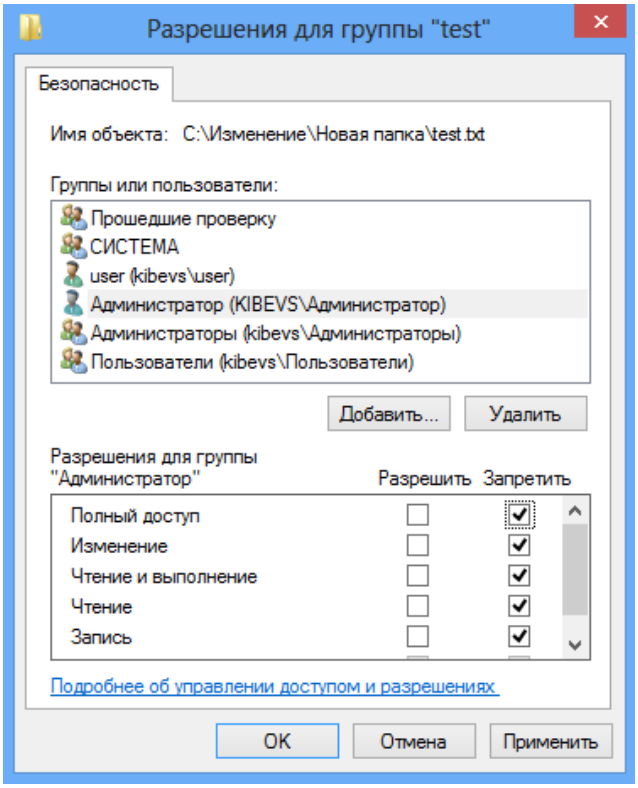

Рис. 3.26 – Запрет доступа к файлу

Дополнительно разрешение «Полный доступ» даёт возможность смены владельца файла. Смените владельца файла test.txt на пользователя user1 (рис. 3.27).

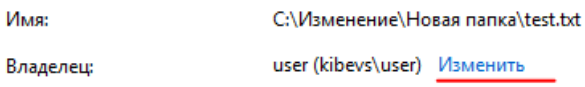

Рис. 3.27 – Смена владельца файла

Попытайтесь изменить владельца другого файла/каталога, к которому нет полного доступа (например, диска D:\). Операционная система выдаст ошибку изменения владельца (рис. 3.28).

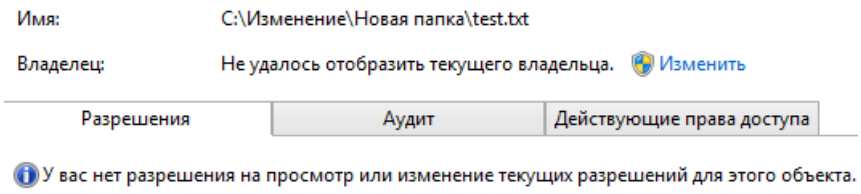

Рис. 3.28 – Ошибка смены владельца файла

Войдите под учётной записью «Администратор». Попытайтесь получить доступ к файлу test.txt. Несмотря на то, что «Администратор» не может получить доступ к файлу, он может сменить владельца. Измените владельца файла на группу «Администраторы». Закройте свойства файла. При повторном входе в свойства файла у пользователя появляется возможность устанавливать права доступа (рис. 3.29). Пользователи и группы, имеющие право менять владельца, не обладая полным доступом к нему, перечисляются в групповых политиках («Панель управления\Система и безопасность\Администрирование\Локальная политика безопасности») в параметре «Смена владельцев файлов и других объектов» в «Назначение прав пользователей» (рис. 3.30).

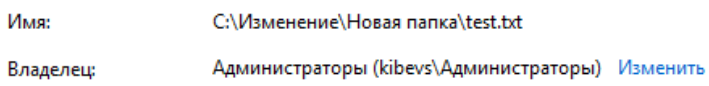

Рис. 3.29 – Установка группы «Администраторы»
в качестве владельца файла

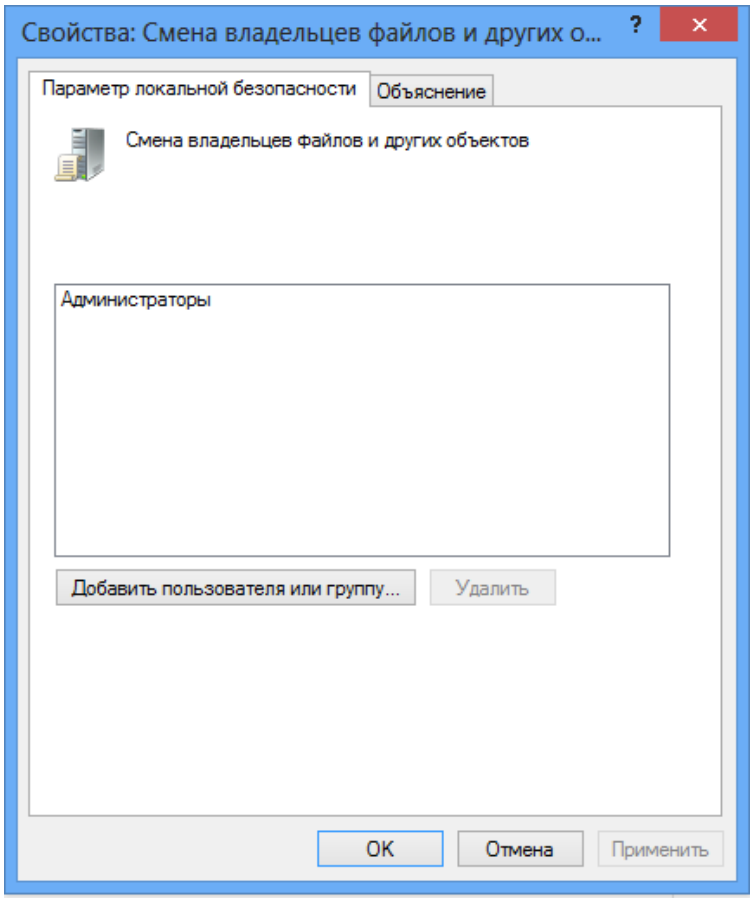

Рис. 3.30 – Параметр «Овладение файлами и другими объектами»

3.1.4 Наследование прав доступа

NTFS поддерживает наследование разрешений, которое означает, что по умолчанию разрешения каталога распространяются на все его файлы и подкаталоги. Любые изменения разрешений на доступ к родительскому каталогу будут отражаться на его вложенных объектах.

Изменить унаследованные разрешения можно и со стороны вложенного объекта. Откройте вкладку «Разрешения» в дополнительных параметрах безопасности каталога «D:\Чтение\Чтение1» и отключите наследование (параметр «Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне»). При отключении наследования скопируйте текущие разрешения (рис. 3.31).

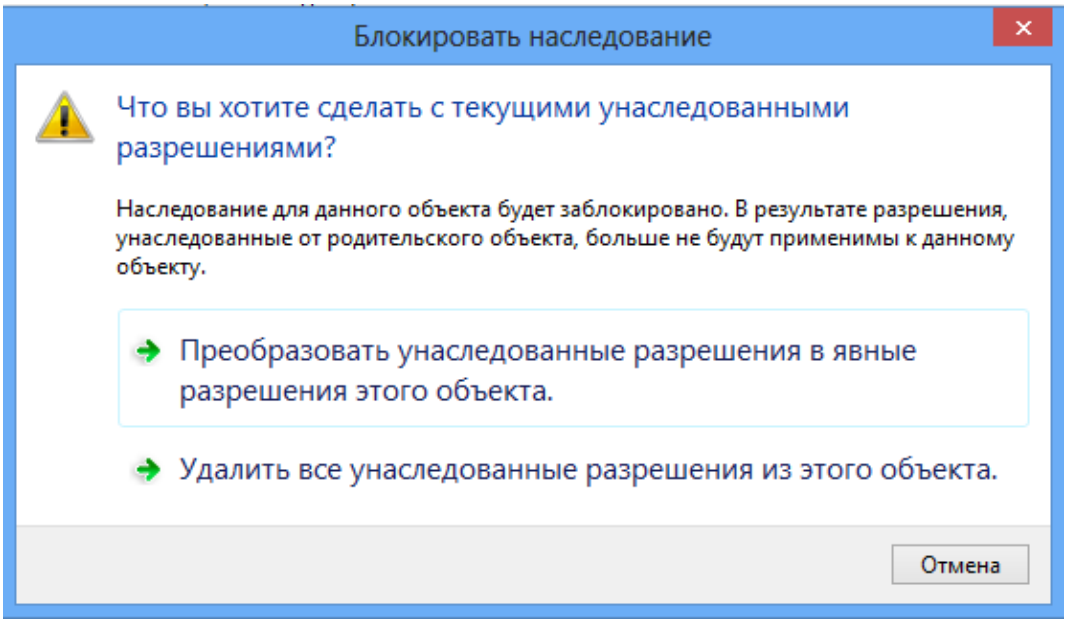

Рис. 3.31 – Выбор действия при отключении наследования

После отключения наследования в родительском каталоге разрешений в разделе «Унаследовано» у каждого элемента устанавливается значение «не унаследовано» (рис. 3.32).

Тип	Субъект	Доступ	Унаследовано от	Применяется к
Разр...	user (kibevs\user)	Полный доступ	Нет	Для этой папки, ее подпапок ...
Разр...	user1 (kibevs\user1)	Полный доступ	Нет	Для этой папки, ее подпапок ...
Разр...	Администраторы (kibevs\Ад...	Полный доступ	Нет	Для этой папки, ее подпапок ...
Разр...	СИСТЕМА	Полный доступ	Нет	Для этой папки, ее подпапок ...
Разр...	Пользователи (kibevs\Польз...	Чтение и выполнение	Нет	Для этой папки, ее подпапок ...
Разр...	Прошедшие проверку	Изменение	Нет	Для этой папки, ее подпапок ...

Рис. 3.32 – Элементы разрешений при отключенном наследовании

Изменить действующие разрешения у вложенных объектов можно при помощи параметра «Заменить разрешения для всех дочерних объектов заданными здесь разрешениями, применимыми к дочерним объектам». Удалите учётную запись user из числа санкционированных пользователей каталога «Чтение1». В родительском для него каталоге «Чтение» установите изменение прав дочерних объектов (рис. 3.33). Проверьте восстановление учётной записи user в перечне санкционированных пользователей каталога «Чтение1».

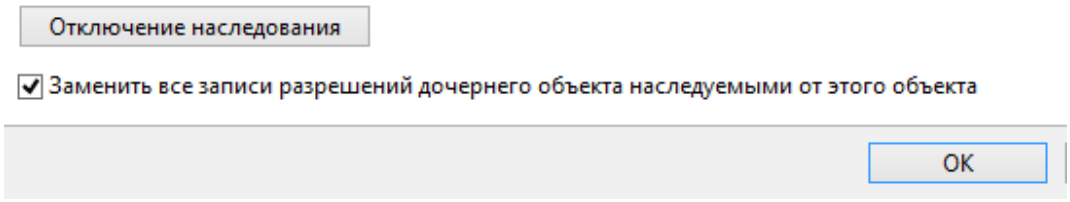

Рис. 3.33 – Включение принудительного наследования

При установке прав доступа на элементы можно выставлять не только разрешения, но и запреты. Запретите группе «Пользователи», членом которой является user (учётной записи user чтение разрешено) чтение файла «Чтение» (рис. 3.34). Войдите под учётной записью user. Попытайтесь открыть файл «Чтение». Невозможность открыть файл обусловлена тем, что запреты приоритетнее разрешений.

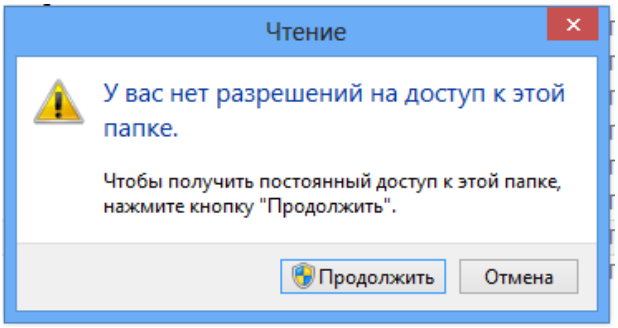

Рис. 3.34 – Результат запрета на чтение

Действующие разрешения можно просмотреть в одноимённой вкладке дополнительных параметров безопасности, выбрав интересующего пользователя или группу. Войдите под учётной записью «Администратор». Просмотрите действующие разрешения на файл «Чтение» для пользователя user (рис. 3.35). Удалите группу «Пользователи» из перечня разрешений. Повторно просмотрите действующие разрешения пользователя user (рис. 3.36). Таким образом, разрешения, предоставленные пользователю и группе, в которую он входит, суммируются. И после удаления элемента, запрещающего группе «Пользователи» чтение, у пользователя user остались только свои права.

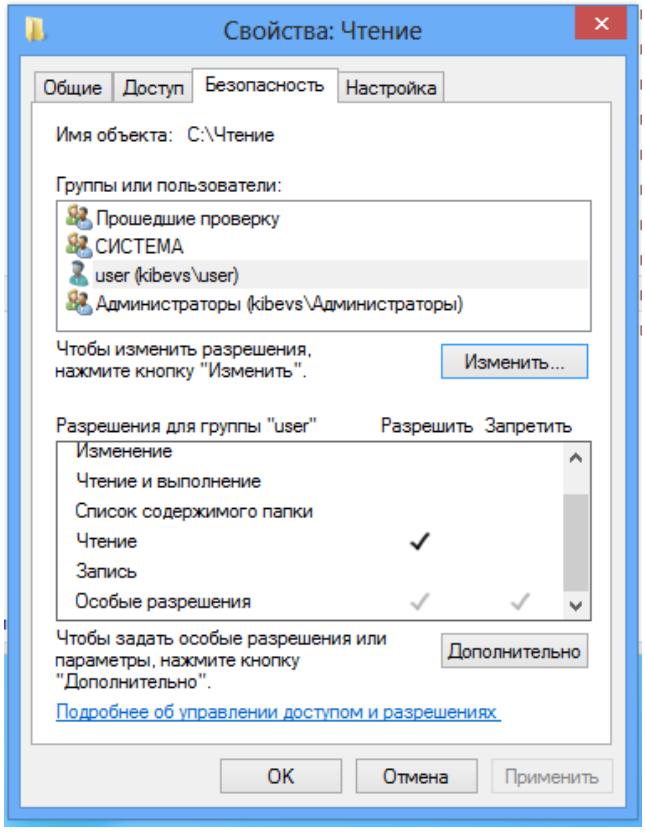

Рис. 3.35 –Действующие разрешения пользователя до изменений

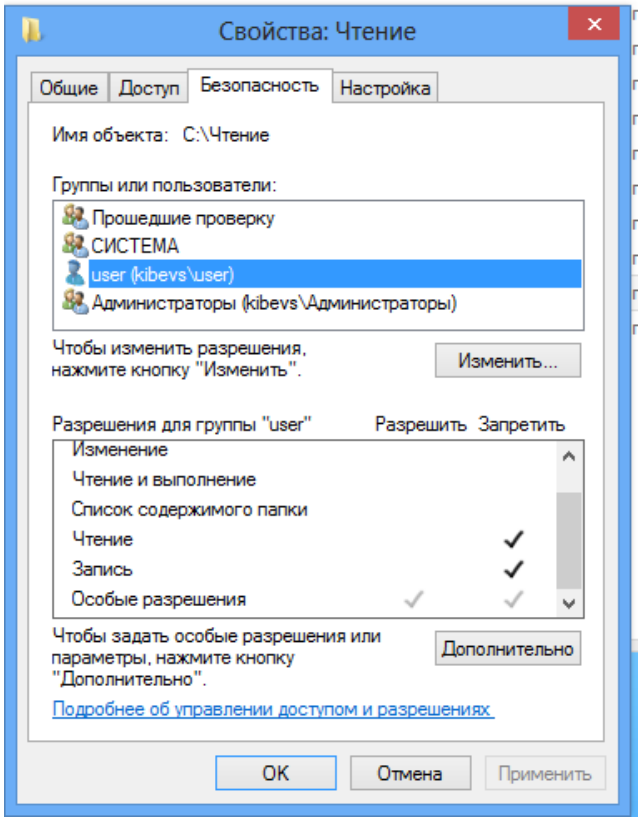

Рис. 3.36 –Действующие разрешения пользователя после изменений

При выставлении разрешений существует возможность указывать глубину наследования и типы объектов. Можно распространить установленные разрешения на данный каталог, только на вложенные объекты или на каталог и все его вложенные объекты, а также можно указать, на какие вложенные каталоги или файлы будут распространяться разрешения.

Разрешите пользователю user создание папок в каталоге «Чтение» только для подпапок, вложенных в этот каталог (рис. 3.37), т. е. в каталогах «Чтение» и «Чтение2» подпапки создавать будет запрещено, а в каталоге «Чтение1» (непосредственно вложенном в «Чтение») – разрешено. Войдите под учётной записью user. Проверьте возможность создания папок во всех указанных каталогах.

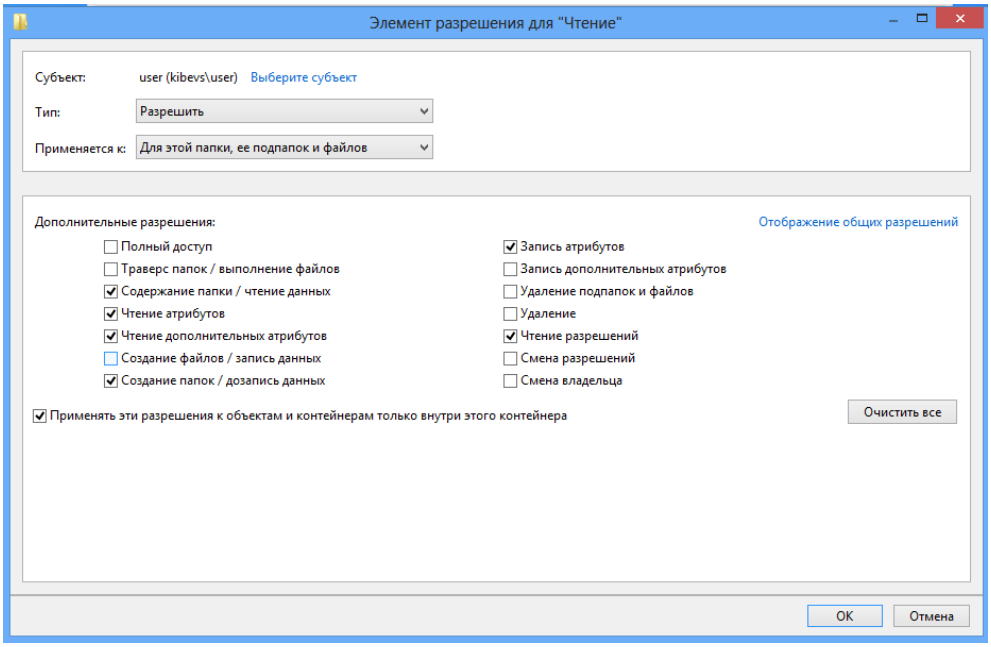

Рис. 3.37 – Выбор глубины и типа объектов наследования

3.1.5 Разграничение доступа к принтерам

Под учётной записью user отправьте текстовый файл на печать при помощи принтера doPDF.

В разделе «Принтеры и факсы» меню «Пуск» попытайтесь изменить настройки принтера (рис. 3.38). Невозможность изменения настроек объясняется наличием у группы «Все» только права на «Печать» (отсутствием права на «Управление принтерами») (рис. 3.39).

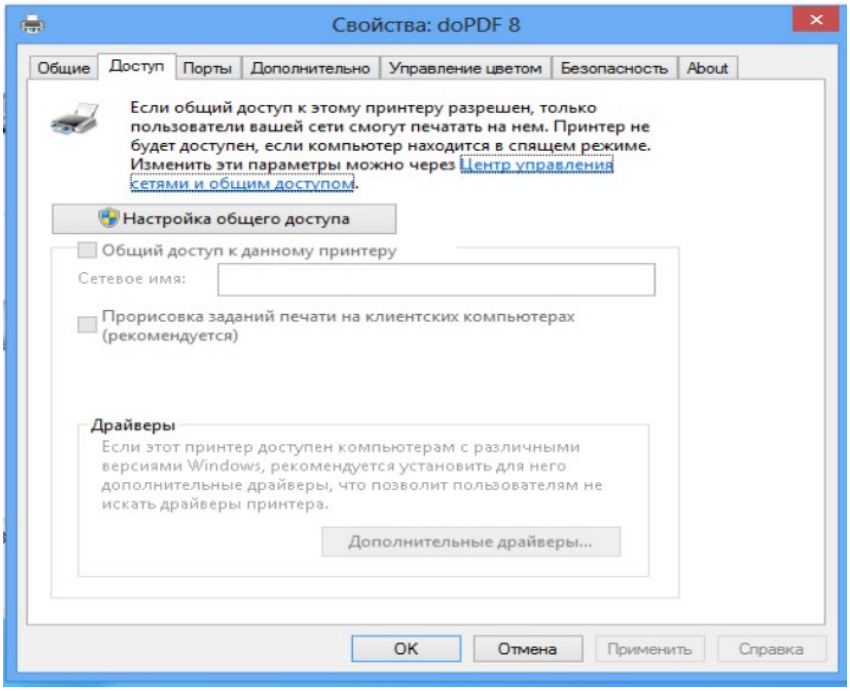

Рис. 3.38 – Свойства принтера

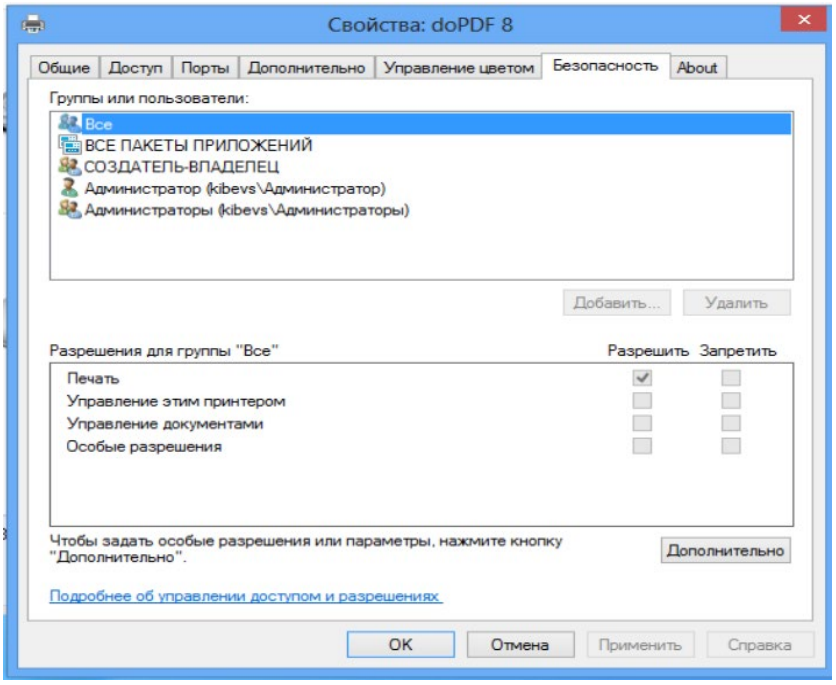

Рис. 3.39 – Разграничение доступа к принтеру

Войдите под учётной записью «Администратор». Удалите из списка доступа к принтеру doPDF группу «Все». Войдите под учётной записью user.

Попытайтесь напечатать текстовый файл. Откройте раздел «Принтеры и факсы», в котором doPDF отсутствует, т. к. user не входит в список пользователей, имеющих право на работу с принтером.

3.2 Задание

Создайте каталоги «Общедоступно» и «Конфиденциально». В каждый из этих каталогов скопируйте исполняемый и текстовый файлы. Разграничьте доступ к принтеру, а также созданным каталогам и файлам в соответствии со своим вариантом.

Вариант 1

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Принтер
Администратор	Полный доступ	Чтение	Полный доступ
user	Чтение	Изменить, кроме удаления	Печать, управление документами
user1	Изменить	Нет доступа	Печать

Вариант 2

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Принтер
Администратор	Полный доступ	Чтение и выполнение	Полный доступ
user	Изменить	Чтение	Печать
user1	Чтение и выполнение	Изменить	Печать, управление документами

Вариант 3

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Текстовый файл в «Конфиденциально»
Администратор	Полный доступ	Список содержимого	Нет доступа
user	Чтение	Изменить, кроме удаления	Изменить
user1	Изменить	Нет доступа	Нет доступа

Вариант 4

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Текстовый файл в «Конфиденциально»
Администратор	Изменить	Чтение и выполнение	Нет доступа
user	Чтение	Изменить	Запрет удаления
user1	Полный доступ, кроме смены владельца	Запись	Нет доступа

Вариант 5

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Исполняемый файл в «Конфиденциально»
Администратор	Полный доступ	Список содержимого	Выполнение
user	Чтение	Чтение и удаление	Выполнение, запрет удаления
user1	Изменить, кроме удаления	Запись	Нет доступа

Вариант 6

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Исполняемый файл в «Конфиденциально»
Администратор	Полный доступ	Чтение	Изменить
user	Чтение и удаление	Список содержимого	Выполнение
user1	Изменить	Нет доступа	Нет доступа

Вариант 7

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Текстовый файл в «Общедоступно»
Администратор	Список содержимого	Полный доступ	Нет доступа
user	Изменить, кроме удаления	Чтение	Изменить
user1	Нет доступа	Изменить	Нет доступа

Вариант 8

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Текстовый файл в «Конфиденциально»
Администратор	Чтение и выполнение	Изменить	Нет доступа
user	Изменить	Чтение	Изменить, запрет изменения дополнит. атрибутов
user1	Запись	Изменить, кроме удаления	Нет доступа

Вариант 9

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Исполняемый файл в «Конфиденциально»
Администратор	Список содержимого	Полный доступ	Выполнение
user	Чтение и удаление	Чтение	Выполнение, запрет удаления
user1	Запись	Полный доступ	Нет доступа

Вариант 10

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Исполняемый файл в «Конфиденциально»
Администратор	Чтение	Полный доступ	Изменить
user	Список содержимого	Чтение и удаление	Выполнение
user1	Нет доступа	Изменить	Нет доступа

Контрольные вопросы

1. Охарактеризуйте дискреционную модель управления доступом.

2. Перечислите стандартные права доступа к файловым объектам, существующие в файловой системе NTFS.

3. Объясните принцип работы разрешения «Запись».

4. Перечислите элементы разрешений.

5. Кто может стать владельцем объекта?

6. Раскройте понятие наследования разрешений.

7. Как отключить наследование разрешений?

8. Как реализовать принудительное наследование вложенными объектами установленных разрешений?

9. Перечислите приоритеты применения разрешений при определении действующих разрешений на доступ к файловым объектам.

10. Перечислите стандартные права доступа к принтерам, существующие в файловой системе NTFS.

4 ЛАБОРАТОРНАЯ РАБОТА № 4 «ПОЛИТИКА ОГРАНИЧЕННОГО ИСПОЛЬЗОВАНИЯ ПРОГРАММ»

Целью лабораторной работы является ознакомление и практическое применение встроенных средств ограничения использования программ в ОС Windows 8.

4.1 Руководство по созданию замкнутой программной среды

Политики ограниченного использования программ позволяют осуществлять идентификацию программ, запускаемых в ОС семейства Windows, и управлять возможностью их выполнения на локальном компьютере.

Политики ограниченного использования программ (ПОИП) – это вид политик безопасности, который позволяет администраторам разрешить или запретить использовать программные приложения. Применение основано на использовании алгоритма хеширования файла, связи путей файлов с программным обеспечением, сертификата издателя программного обеспечения или зоны Интернета, в которой работает программное обеспечение.

Войдите в ОС под учетной записью администратора и перейдите по следующему пути: «Панель управления – Администрирование – Локальная политика безопасности», далее в дереве консоли раскройте узел «Политики ограниченного использования программ» (рис. 4.1). Также доступ к политикам ограниченного использования программ (далее ПОИП) можно получить через добавление оснастки «Локальные параметры безопасности» в консоль управления. Через контекстное меню создайте новую политику (рис. 4.2).

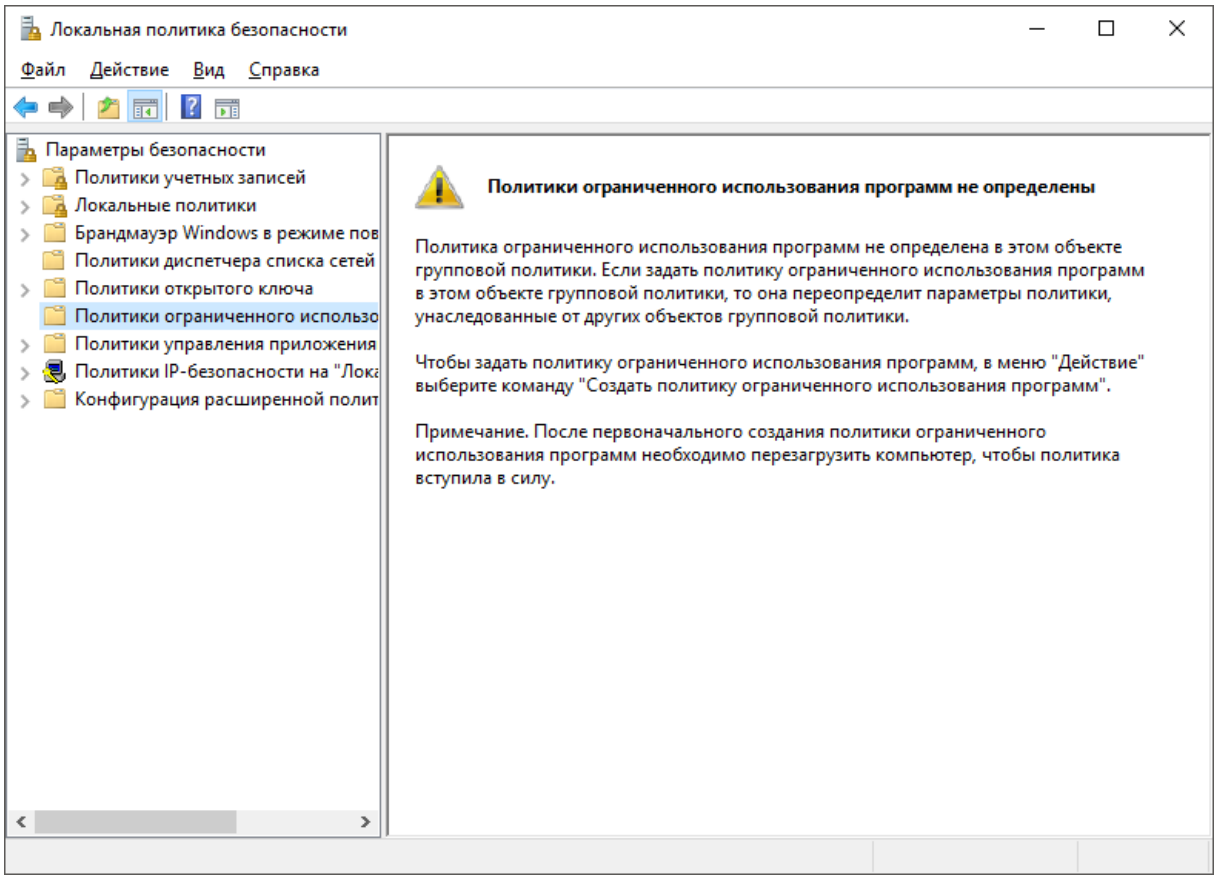

Рис. 4.1 – Локальная политика безопасности

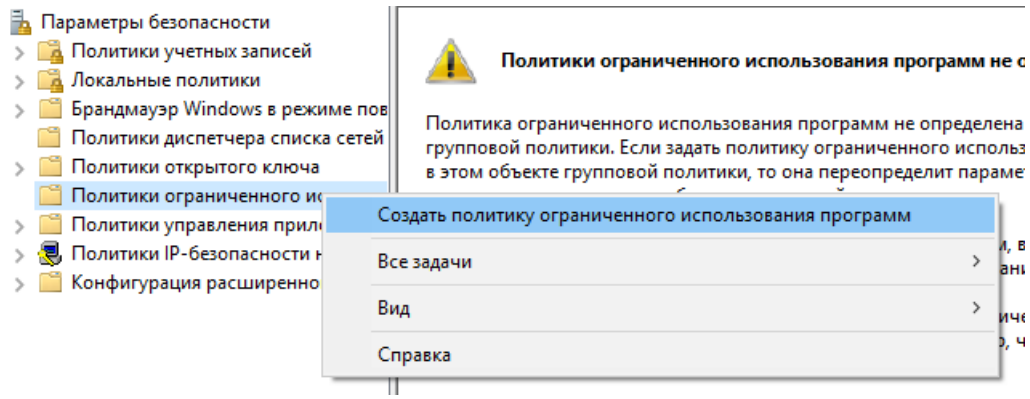

Рис. 4.2 – Создание новой политики

Раскройте объект «Уровни безопасности» (рис. 4.3), в который включены три уровня: 1) «Не разрешено», где запрещен запуск любого ПО, кроме разрешённого в ПОИП; 2) «Обычный пользовательский», где разрешается запускать программы без прав администратора; 3) «Неограниченный», означающий возможность работы с ПО в соответствии с правами пользователя.

Уровень, используемый по умолчанию, обозначается «галочкой», чтобы его изменить, дважды кликните на уровень безопасности и выберите пункт «По умолчанию».

Установите уровень «Неограниченный» в качестве уровня безопасности по умолчанию.

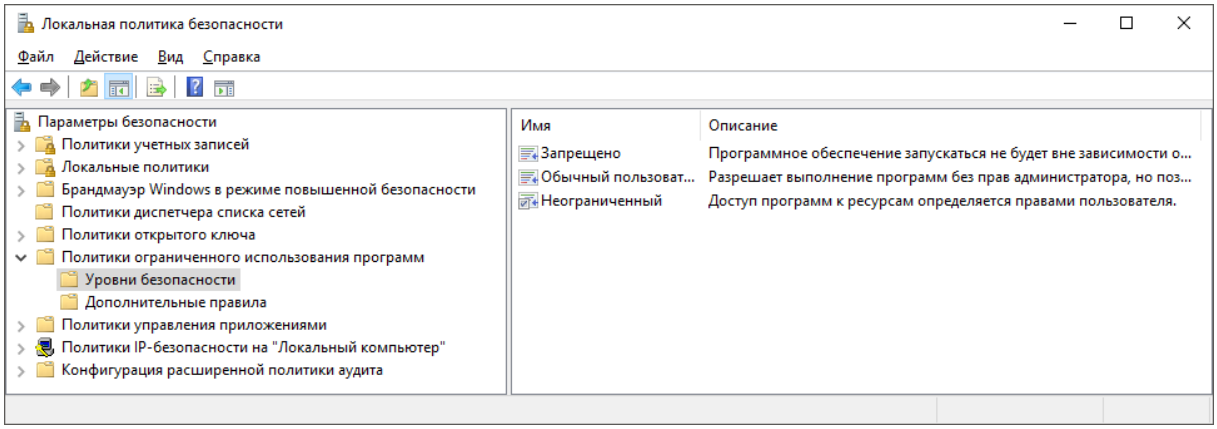

Рис. 4.3 – Выбор уровня безопасности

Чтобы применить ПОИП к локальным администраторам, дважды кликните тип объекта «Применение» и выберите «Для всех пользователей» (рис. 4.4). Здесь же настраивается возможность исключать применение ПОИП к библиотекам программ, таких как DLL, которые могут использоваться другими разрешенными программами. Установите применение ПОИП ко всем пользователям и файлам.

В пункте «Назначенные типы файлов» раздела «Политики ограниченного использования программ» уже имеется список назначенных типов файлов, используемый для всех правил. Для того чтобы определить, с какими типами файлов будет работать ПОИП, выберите пункт «Назначенные типы файлов», в появившемся окне (рис. 4.5) в поле «Расширение:» введите требуемое расширение, например exe. Таким образом, добавляются новые типы файлов, которые учитываются в правиле для пути.

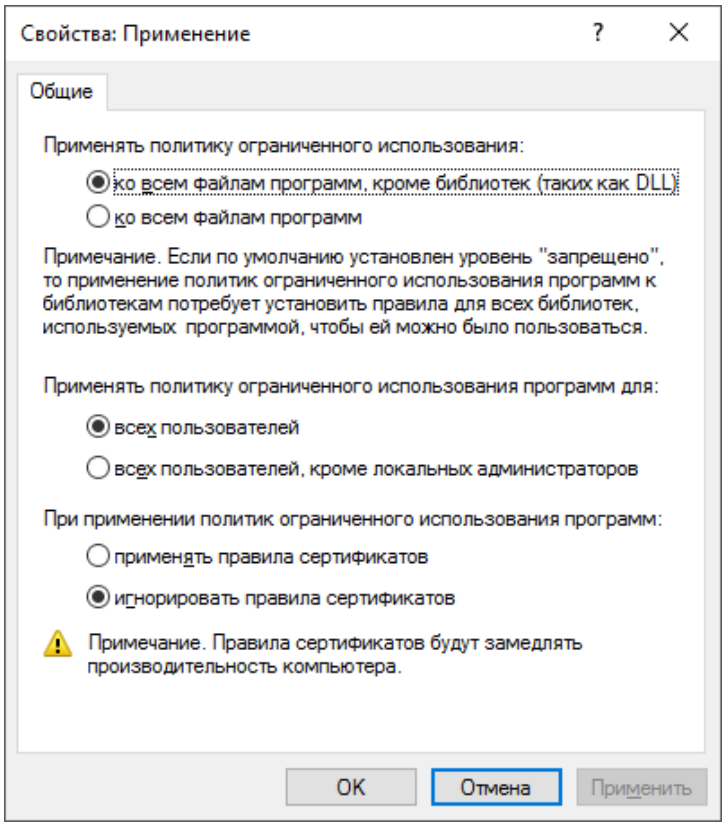

Рис. 4.4 – Настройка дополнительных параметров

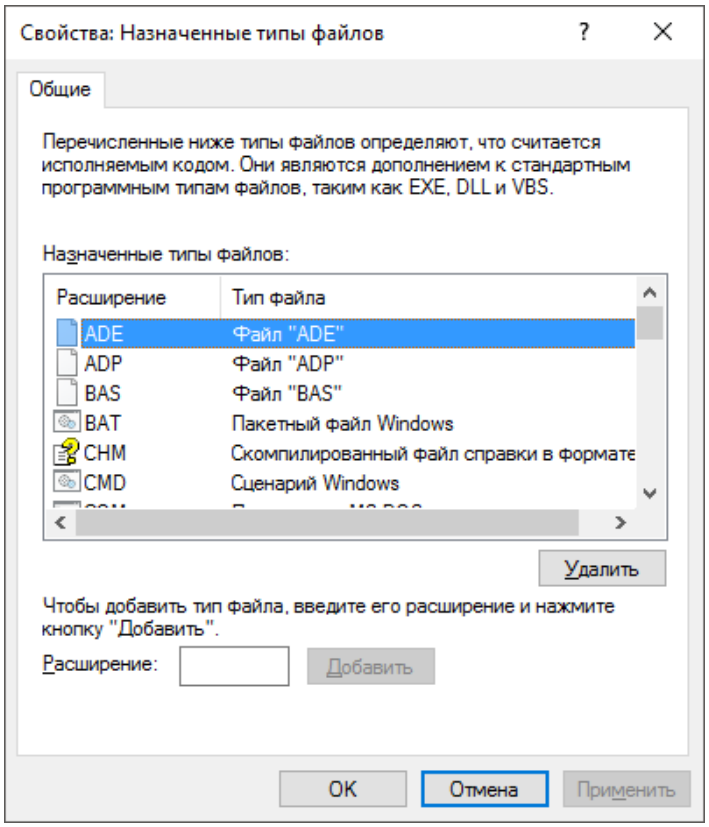

Рис. 4.5 – Список файловых типов политики

Перейдите в пункт «Дополнительные правила» (рис.4.6) в нем уже имеются два правила пути. Они обеспечивают запуск ОС при выбранном по умолчанию уровне безопасности «Не разрешено». В меню выберите «Действие», далее «Создать правило для хэша…», в появившемся окне (рис. 4.7) при помощи кнопки «Обзор» укажите файл, работу с которым вы хотите запретить, например utorrent.exe, информация о нем заполнится автоматически. Также можно вносить само значение хэша, рассчитанное другим пользователем, например хэш вируса.

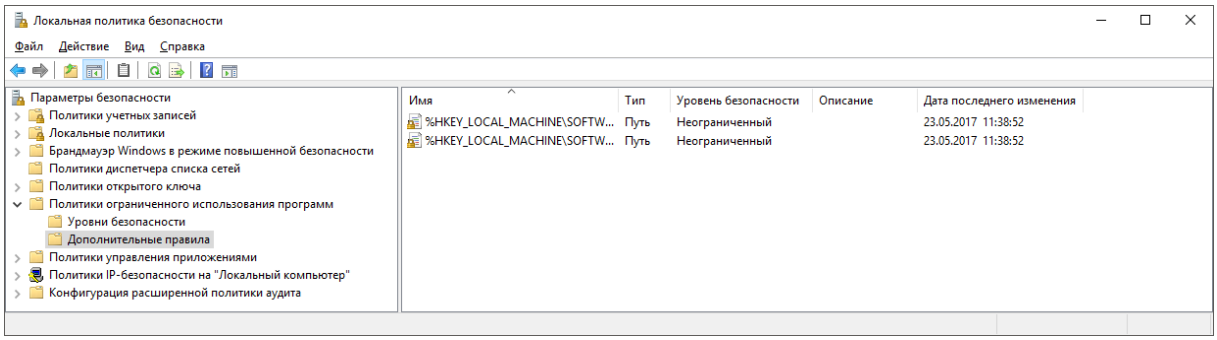

Рис. 4.6 – Вкладка «Дополнительные правила»

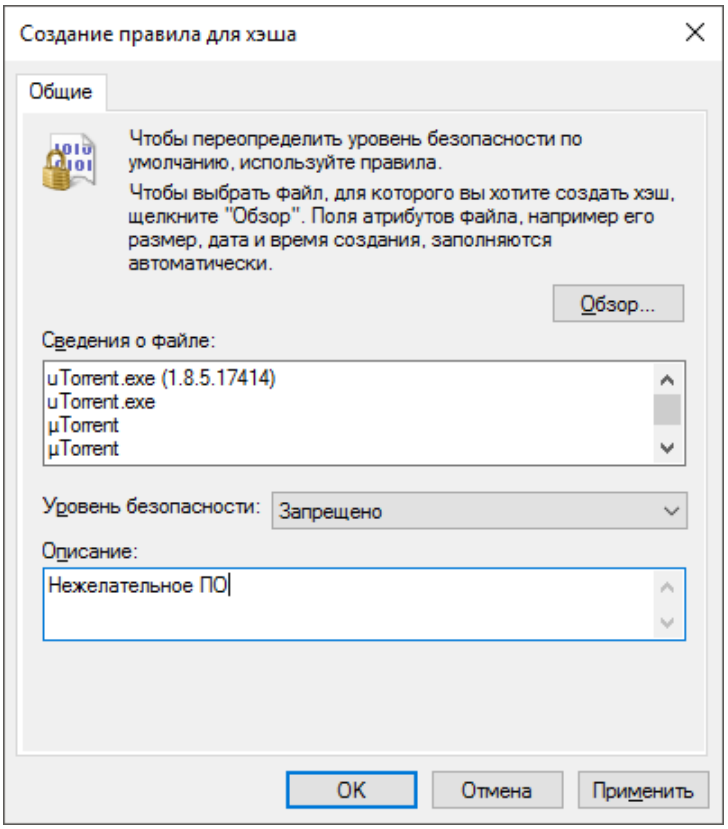

Рис. 4.7 – Создание правила для хэша

Запустите файл utorrent.exe, после чего отобразится сообщение, информирующее пользователя о запрете запуска файла. Необходимо помнить, что любые изменения в файле приводят к изменению хэша.

По аналогии с правилом хэша создайте правило пути. В появившемся окне (рис. 4.8) в поле «Путь:» введите путь к файлам, работу с которыми нужно ограничивать, например %programfiles%\Messenger, и выберите уровень безопасности «Не разрешено». Путь можно указывать и к конкретному файлу, а также использовать подстановочные знаки «*» и «?», например: c:\downloads*.*. Попробуйте запустить программу обмена сообщений Windows Messenger. Убедитесь в запрете запуска.

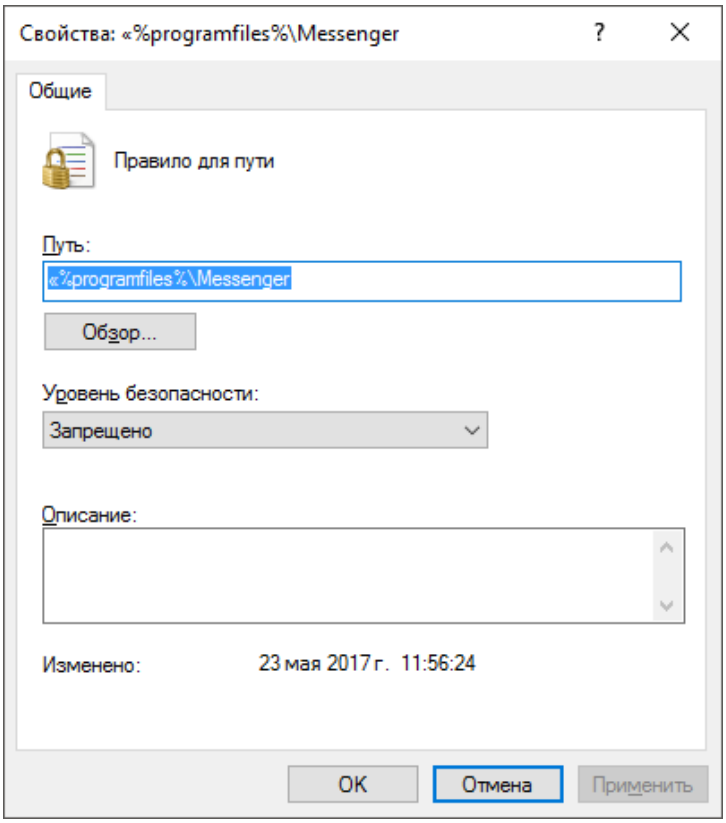

Рис. 4.8 – Создание правила пути

В правиле для пути имеется возможность использовать системные переменные, такие как %programfiles%, %systemroot%, %userprofile%, %windir%, %appdata% и %temp%, а также переменные окружения.

Переменные окружения создаются следующим образом: в свойствах системы по пути «Пуск – Панель управления – Свойства системы» во вкладке «Дополнительно», нажмите на кнопку «Переменные среды». Далее в появившемся окне (рис. 4.9) нажмите кнопку «Создать». Введите имя переменной, например Share и значение переменной C:\Documents and Settings\All Users\Документы. Создайте и проверьте правило пути, применив переменную %Share%.

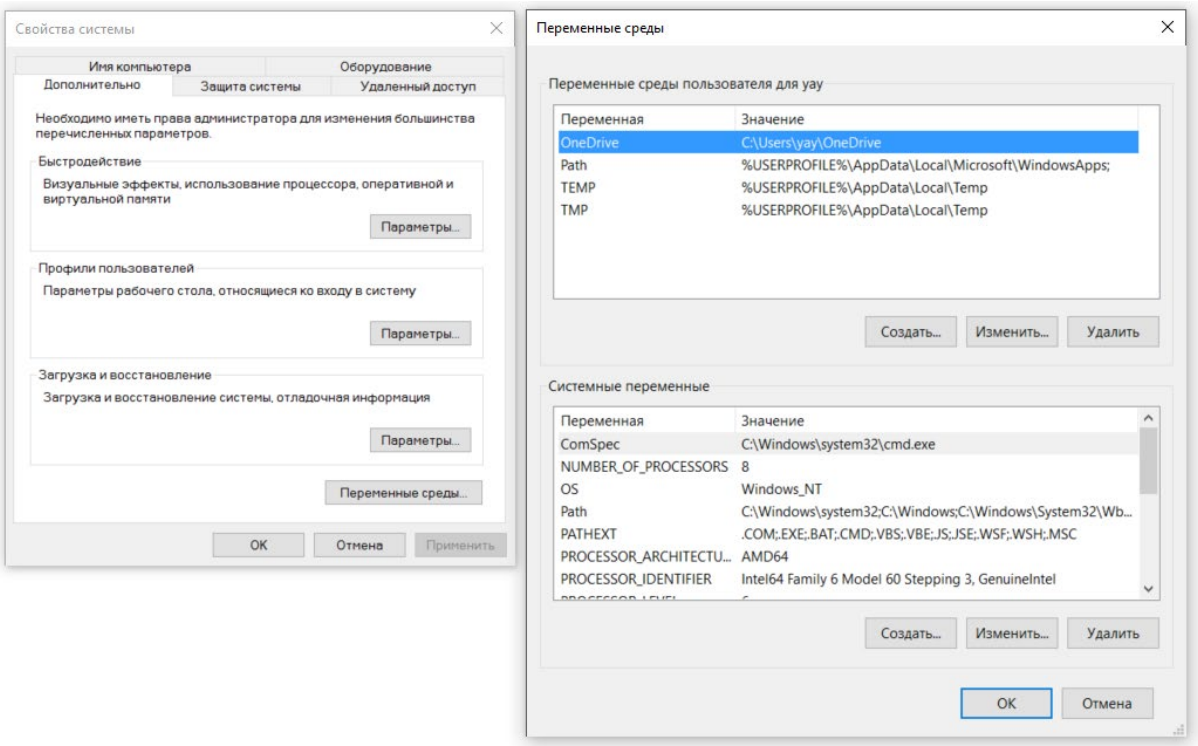

Рис. 4.9 – Создание переменных окружения

Создаваемые «Правила для зоны сети» применяются только к пакетам установщика программ Windows, добавление зон происходит с помощью свойств обозревателя Internet Explorer во вкладке «Безопасность».

Перед созданием правила для сертификата получите сертификат следующим образом: выберите, например, в свойствах файла программы visio.exe вкладку «Цифровые подписи» (рис. 4.10).

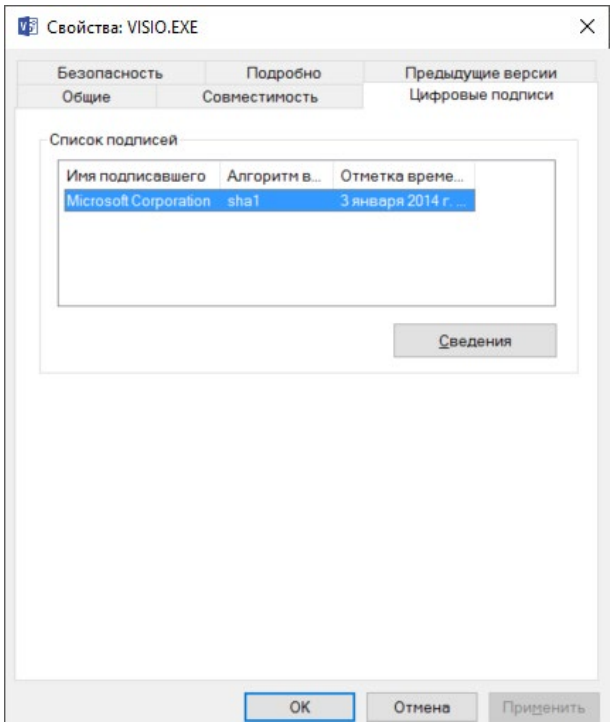

Рис. 4.10 – Цифровые подписи файла

Далее нажмите кнопку «Сведения», в появившемся окне (рис. 4.11) нажмите кнопку «Просмотр сертификата». Сертификат должен быть действителен.

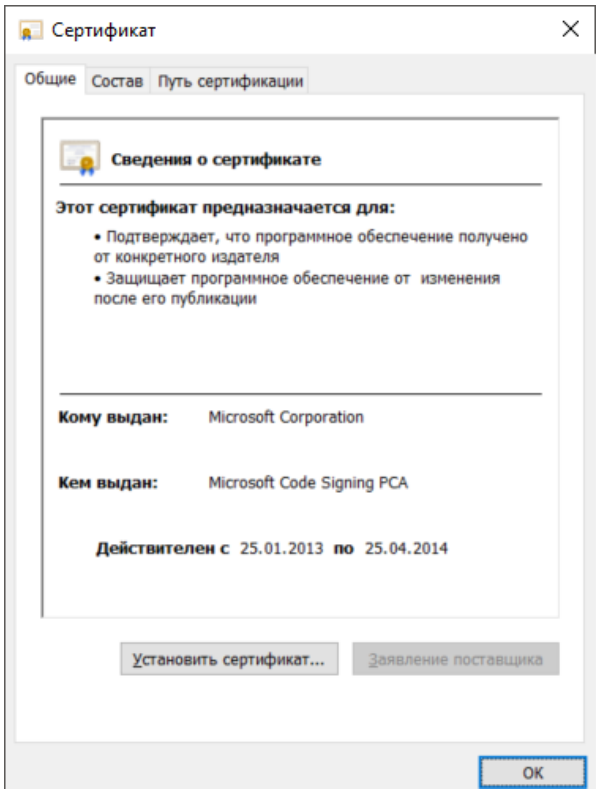

Рис. 4.11 – Сведения о сертификате

В появившемся окне (рис. 4.11) выберите вкладку «Состав» и нажмите кнопку «Копировать в файл…», при помощи мастера экспорта сертификатов сохраните сертификат, например под именем Microsoft.cer (формат сохранения – X.509).

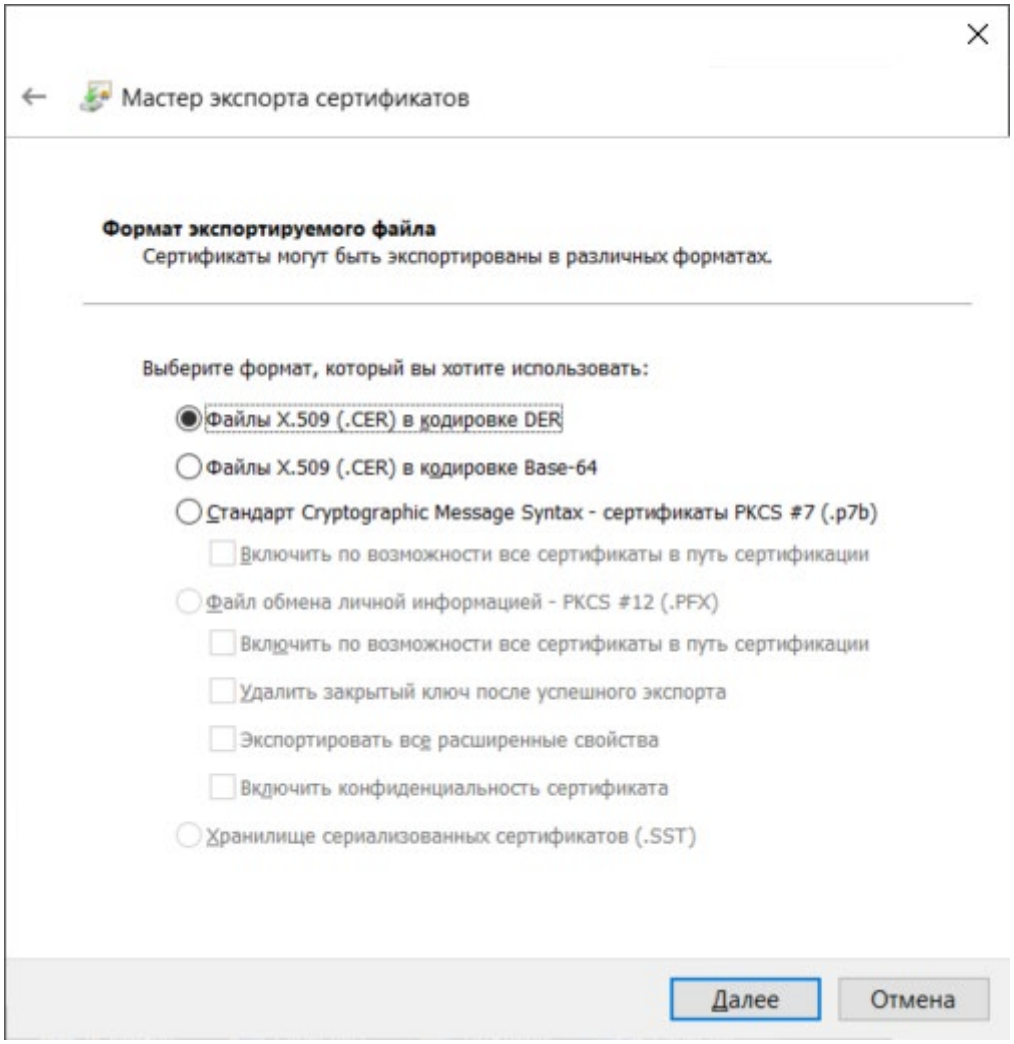

Рис. 4.12 – Мастер экспорта сертификатов

Назначьте по умолчанию уровень безопасности «Не разрешено». Далее в дополнительных правилах создайте «Правило для сертификата…», в появившемся окне (рис. 4.13) укажите путь к сохраненному файлу сертификата «Microsoft.cer» и выставите уровень безопасности «Неограниченный».

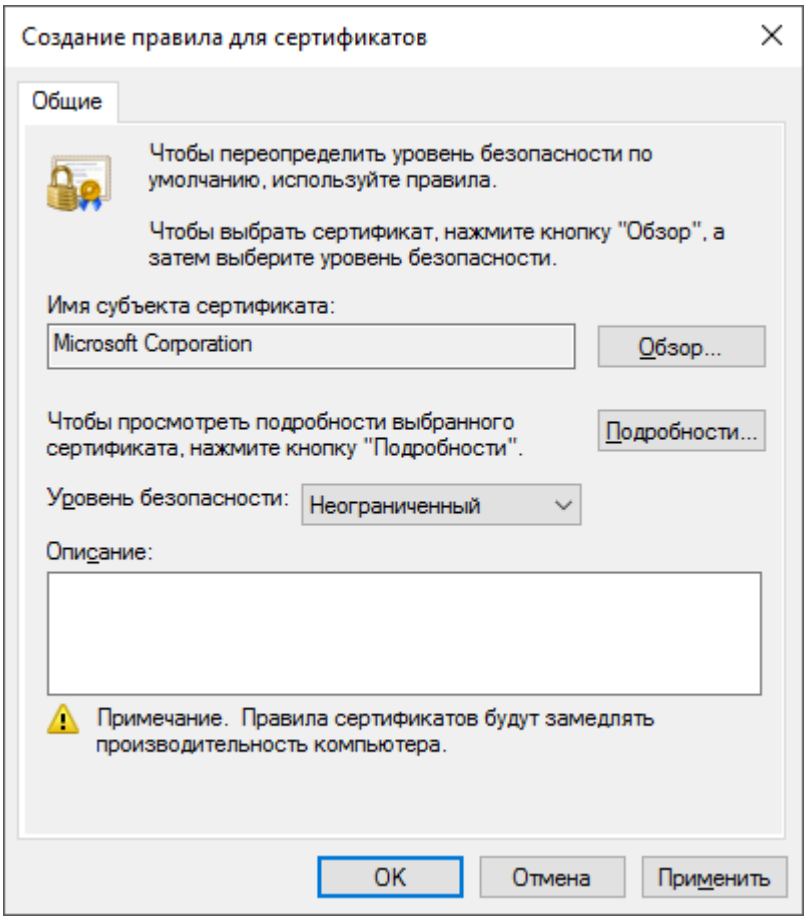

Рис. 4.13 – Создание правила для сертификата

Скопируйте файл visio.exe в папку «C:\Documents and Settings\All Users\Документы». При попытке запустить установочный пакет, подписанный данным сертификатом, выполнится приоритет правила сертификата над правилом пути. Проверьте возможность запуска. Правило сертификатов также может ограничить запуск подписанных программ с переносных носителей информации.

Для разрешения конфликтов, возникающих при использовании нескольких правил, используется приоритет. Ниже перечислены правила в порядке убывания приоритета:

1. Правило для хэша.
2. Правило для сертификата.
3. Правило для пути.

При конфликте правил для пути приоритет имеет правило с большим ограничением. Ниже приведен набор путей в порядке от высшего приоритета (наибольшее ограничение) к низшему приоритету:

– диск:\папка1\папка2\имя_файла.расширение;
– диск:\папка1\папка2*.расширение;
– *.расширение;
– диск:\папка1\папка2\;
– диск:\папка1\.

4. Правило для зоны Интернета.

При конфликте двух похожих правил для пути приоритет имеет правило с большим ограничением. Например, если имеется правило для пути C:\Windows\ с уровнем безопасности «Не разрешено» и правило для пути %windir% с уровнем «Неограниченный», будет применяться более строгое правило с уровнем безопасности «Не разрешено».

В качестве примера создайте разрешающее правило хэша для программы calc.exe, расположенного по запрещенному пути c:\downloads. Далее попытайтесь запустить эту программу из ранее запрещенного пути. Приоритет правила для хэша позволит запустить программу из этой папки.

Удалите все созданные правила перед выполнением задания.

4.2 Задание

Создайте политику ограничения использования программ, которая будет удовлетворять следующим требованиям, согласно вашему варианту (табл. 4.1):

а) разрешает запуск ПО, подписанного сертификатом от Microsoft;

б) применяется ко всем пользователям, включая локальных администраторов;

в) не ограничивает использование программных библиотек, таких как DLL;

г) право выбора доверенных издателей разрешено только локальным администраторам;

д) запрещает запуск любых программ в качестве уровня безопасности по умолчанию;

е) разрешает запуск любых программ из папок: C:\WINDOWS, C:\Program Files, C:\Documents and Settings\LocalService, C:\Documents and Settings\All Users;

ж) разрешает запуск любых программ пользователю из своей папки C:\Documents and Settings\user (где user – имя любого пользователя) при помощи переменной окружения;

з) при помощи приоритета правил пути пользователю запрещено запускать любые программы из папок других пользователей, как например, C:\Documents and Settings\Администратор;

и) разрешает установку ПО, подписанного сертификатом от Microsoft;

к) запрещает запуск программ «Паук», «Сапер» и utorrent.exe вне зависимости от их месторасположения;

л) запрещает запуск файла с именем AUTORUN.INF из любого места;

м) применяется ко всем пользователям, исключая локальных администраторов;

н) ограничивает использование программных библиотек, таких как DLL;

о) право выбора доверенных издателей разрешено любым пользователям;

п) запрещает установку ПО, подписанного сертификатом от Microsoft.

Таблица 4.1 – Распределение требований по вариантам

Вариант	Требования
1	Выполнить пункты: а – д
2	Выполнить пункты: б – е
3	Выполнить пункты: в – ж

Окончание табл. 4.1

Вариант	Требования
4	Выполнить пункты: г – з
5	Выполнить пункты: д – и
6	Выполнить пункты: е – к
7	Выполнить пункты: ж – л
8	Выполнить пункты: з – м
9	Выполнить пункты: к – о
10	Выполнить пункты: л – п

Контрольные вопросы

1. Как создать политику ограниченного использования программ?

2. Возможно ли исключение из ПОИП локальных администраторов?

3. Для чего служит пункт «Назначенные типы файлов»?

4. В чем основное преимущество правила хэша перед правилом пути?

5. Приведите пример, когда запрещенная правилом хэша программа может выполниться.

6. Для чего служит правило для сертификата?

7. Как можно получить сертификат из файла?

8. Приведите три примера использования приоритета правил.

9. Как запретить открытие любых файлов с расширением .swf из любого места на жестком диске?

10. Объясните различие между уровнями безопасности «Неограниченный» и «Не разрешено».

5 ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТОВ ПО ЛАБОРАТОРНЫМ РАБОТАМ

Отчеты по лабораторным работам должны быть оформлены в соответствии с требованиями образовательного стандарта вуза ОС ТУСУР 01–2013 «Работы студенческие по направлениям подготовки и специальностям технического профиля. Общие требования и правила оформления». Текст стандарта можно найти по ссылке: https://regulations.tusur.ru/documents/70

Пример оформления титульного листа отчета представлен в приложении А.

В отчете должны быть обязательно отображены в формате скриншотов действия по выполнению индивидуального задания и краткие ответы на контрольные вопросы. Действия, указанные в руководстве, включать в отчет не обязательно, их необходимо проделать для понимания принципов работы подсистем защиты информации в операционной системе.

ПРИЛОЖЕНИЕ А

Пример оформления титульного листа отчета

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

ТЕМА ЛАБОРАТОРНОЙ РАБОТЫ ПРОПИСНЫМИ БУКВАМИ
Отчет о выполнении лабораторной работы № X
по дисциплине «Защита информации»
Вариант № N

Студент гр. *(номер)*
_____ И. О. Фамилия
(дата)

М.н.с. каф. КИБЭВС
_____ А. Ю. Якимук
(дата)

Томск 2017