Лабораторная работа 1. Администрирование Windows

Цель лабораторной работы: освоение средств администрирования учётных записей пользователей и групп пользователей в ОС Windows 10, изучение основных параметров, определяющих взаимодействие пользователей с операционной системой, консолью управления и групповой политикой.

Задачи лабораторной работы:
1. Краткие теоретические сведения
2. Управление учётными записями локальных пользователей
3. Настройка политики учётной записи
4. Групповые политики
5. Контрольные вопросы
6. Задание на лабораторную работу

Содержание лабораторной работы:

1. Краткие теоретические сведения

В операционной системе Windows 10 существует 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.*

Консоль управления Microsoft Management Console (MMC) – это компонент операционных систем семейства Windows, 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. Управление учётными записями локальных пользователей

Рассмотрите механизм работы с учетными записями пользователей, предлагаемых Windows 10. Для этого через меню «Пуск» перейдите к параметрам системы (рис. 1).

Рис. 1. Параметры Windows

Перейдите в раздел «Учётные записи». В данном разделе будет представлена информация о том, под какой учетной записью был осуществлен вход, представлены функции по изменению параметров входа, представлены учетные записи на данном компьютере (если таковые имеются) и предложено создать новых пользователей (рис. 2).

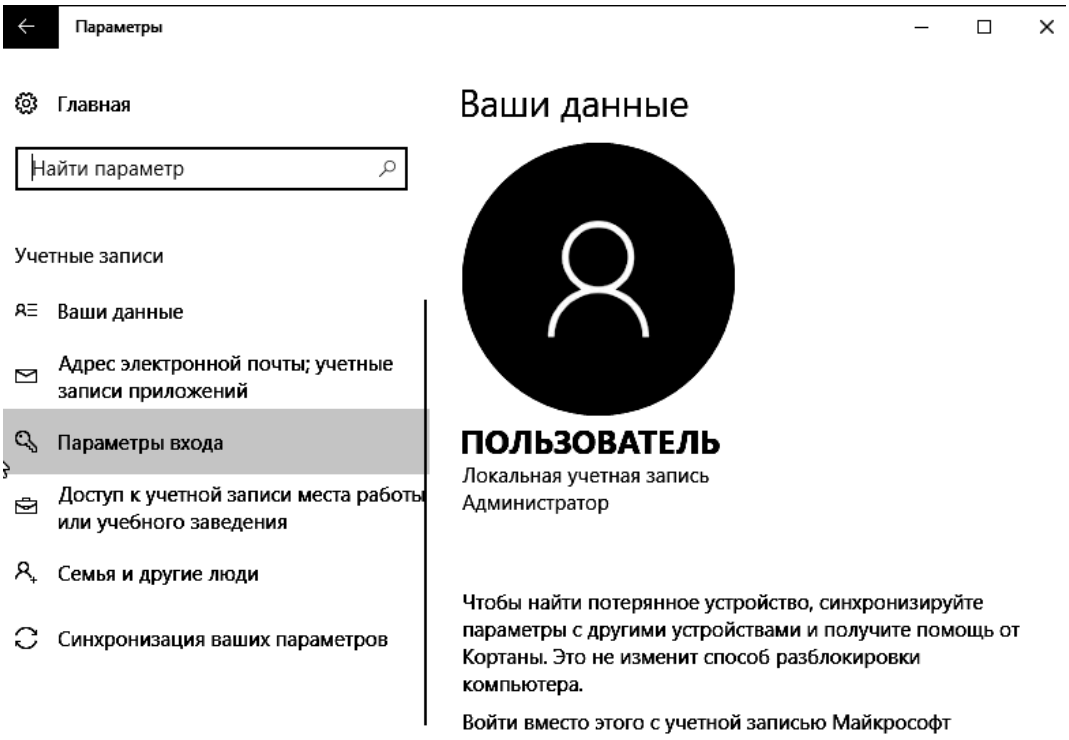

Рис. 2. Вкладка управления пользователями

Перейдите во вкладку «Семья и другие люди», нажмите на «Добавить нового пользователя для этого компьютера». В результате поступит предложение ввести электронный адрес или номер телефона для авторизации. Чтобы добавить локального пользователя нажмите на «У меня нет данных для данного человека» (рис. 3).

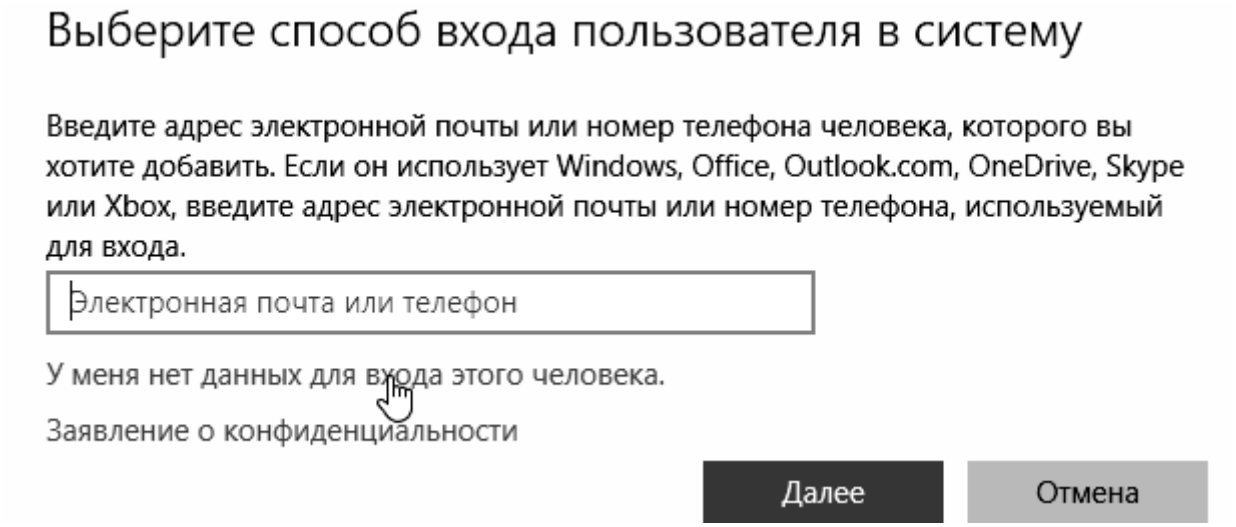

Рис. 3. Выбор способа входа в систему

Потом кликните по надписи: «Добавить пользователя без учётной записи» (рис. 4).

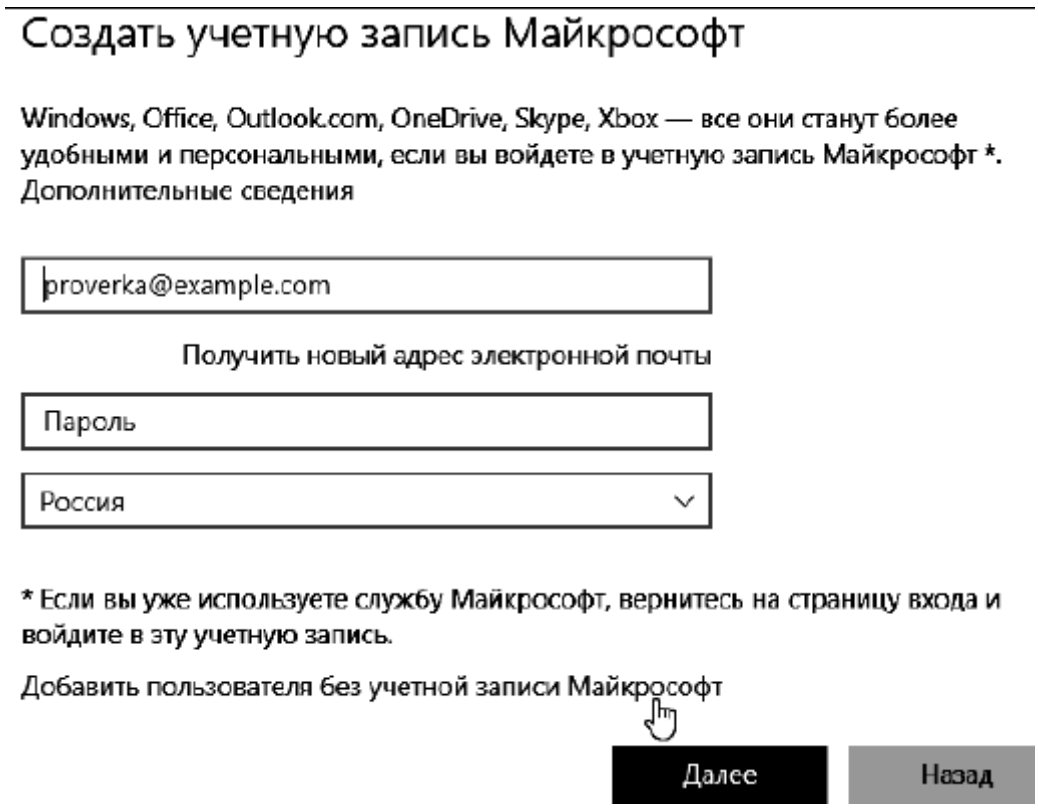

Рис. 4. Добавление локального пользователя

После этого потребуется задать имя пользователя и пароль для него, а также подсказку для пароля. 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 → Добавить или удалить оснастку». В результате будет предложен перечень, из которого пользователь может выбрать одну или несколько оснасток.

Нажмите «Файл» и перейдите в пункт «Параметры». Здесь можно выбрать режим работы пользователя с этой консолью: авторский режим, предоставляющий пользователю полный доступ ко всем функциям MMC, и пользовательский режим.

Существует три вида пользовательского режима:

- *полный доступ (full access) даёт пользователю доступ ко всем командам MMC, но не позволяет добавлять или 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 (рис. 5). Выявите отличия работы консоли в различных режимах.

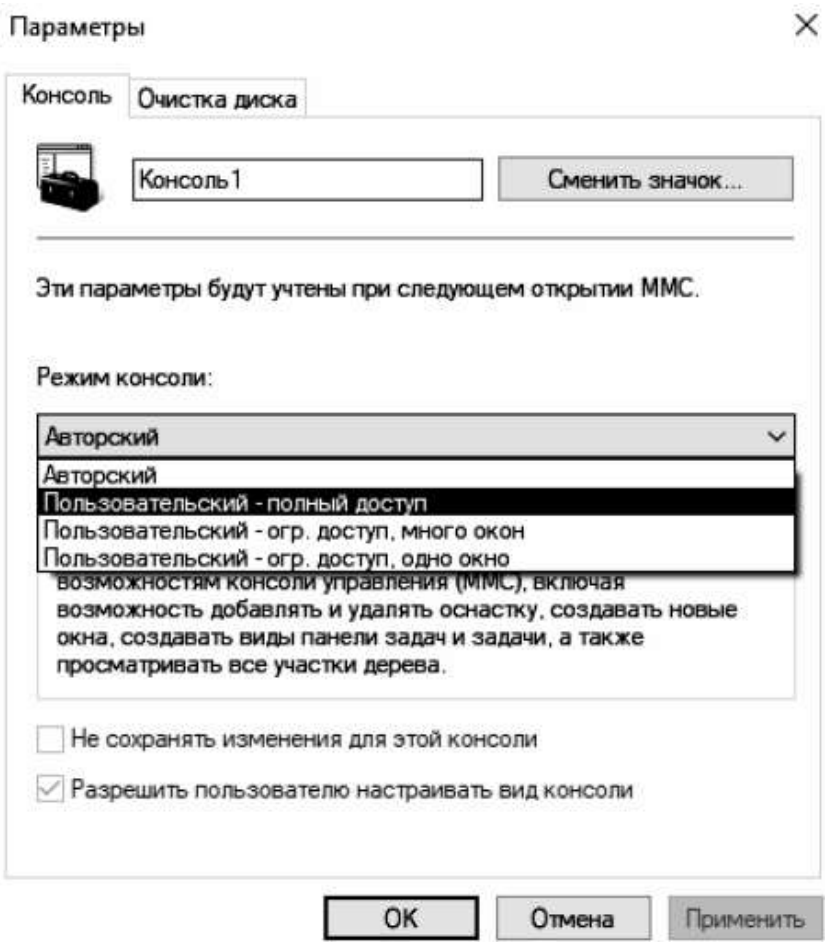

Рис. 5. Параметры режима консоли

Через пункт «Добавить или удалить оснастку» добавьте «Локальные пользователи и группы» (рис. 6).

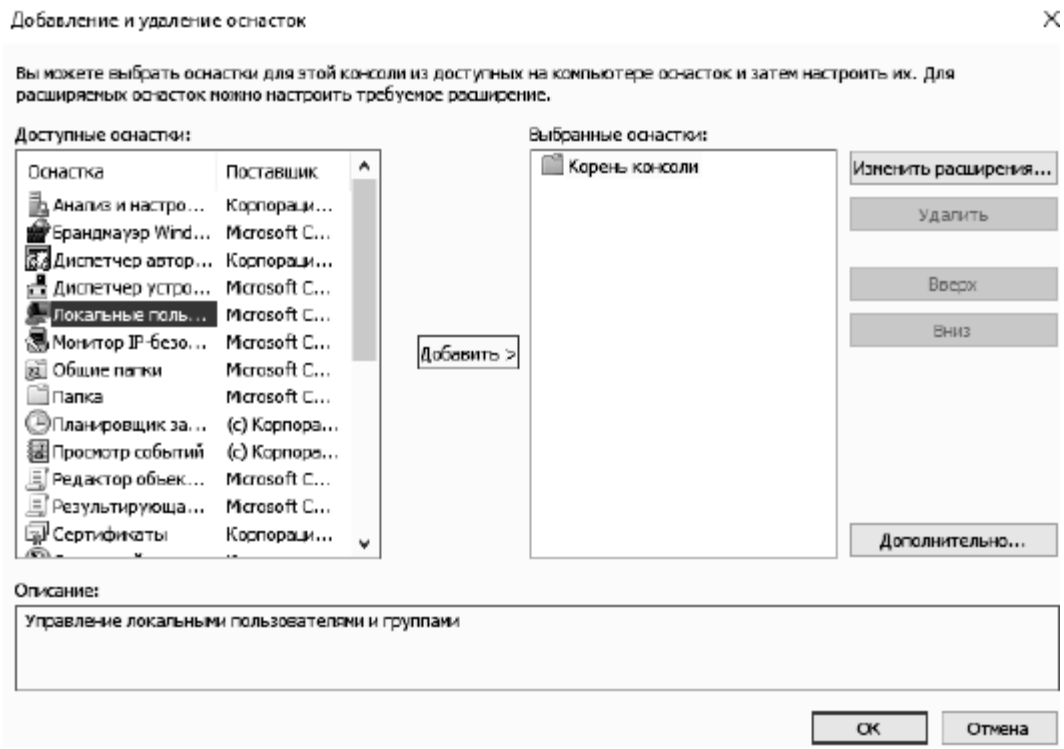

Рис. 6. Добавление оснастки

Через данную оснастку также возможно добавить нового пользователя (рис. 7).

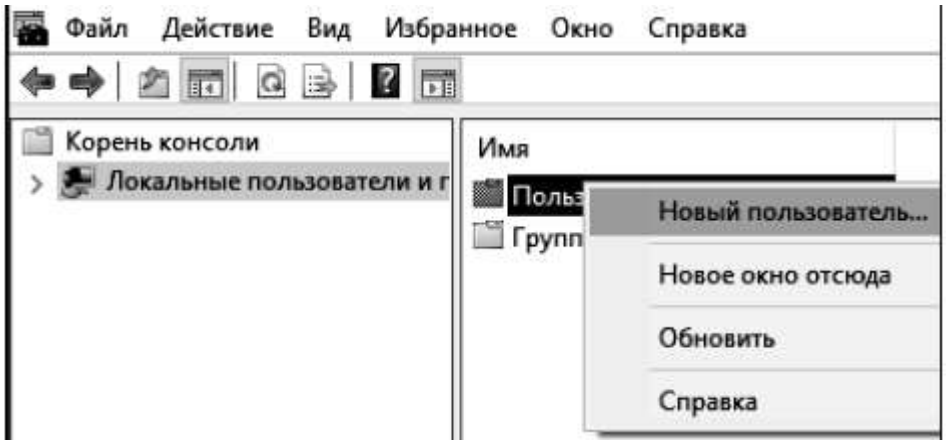

Рис. 7. Добавление пользователя через оснастку

В появившемся окне (рис. 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.

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. 8). Смените пароль у созданной учётной записи.

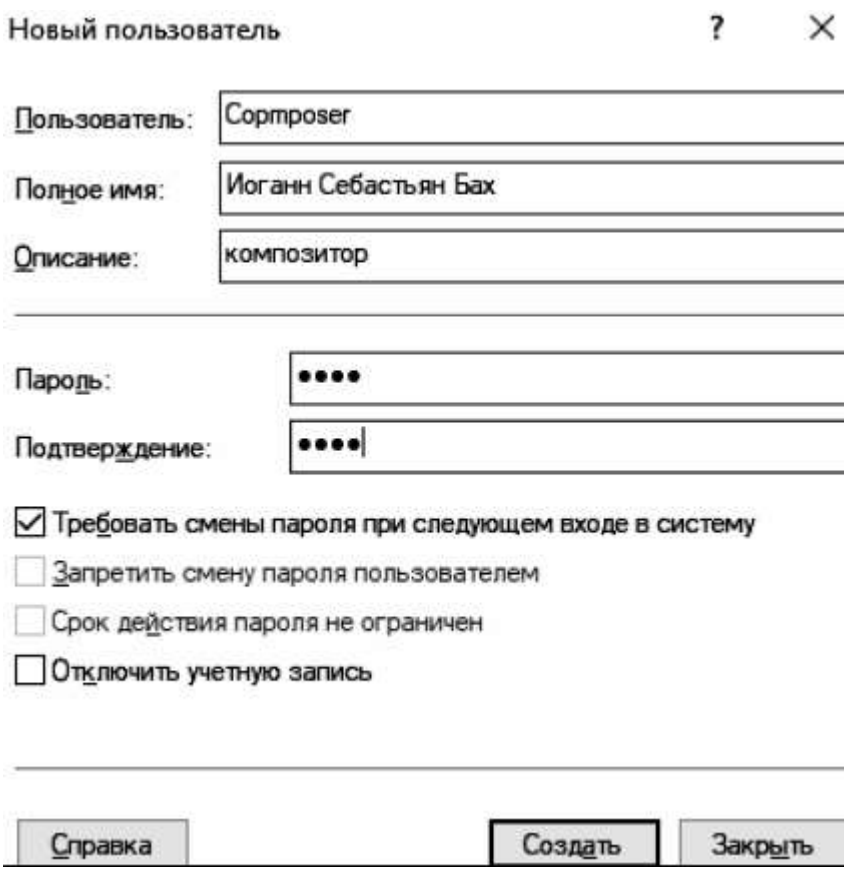

Рис. 8. Настройка параметров учётной записи при её создании

В данный момент времени учетная запись «Администратор» является заблокированной (рис. 10). Разблокируйте её, выбрав соответствующий пункт в свойствах учетной записи. Посмотрите какие еще параметры можно настроить через свойства.

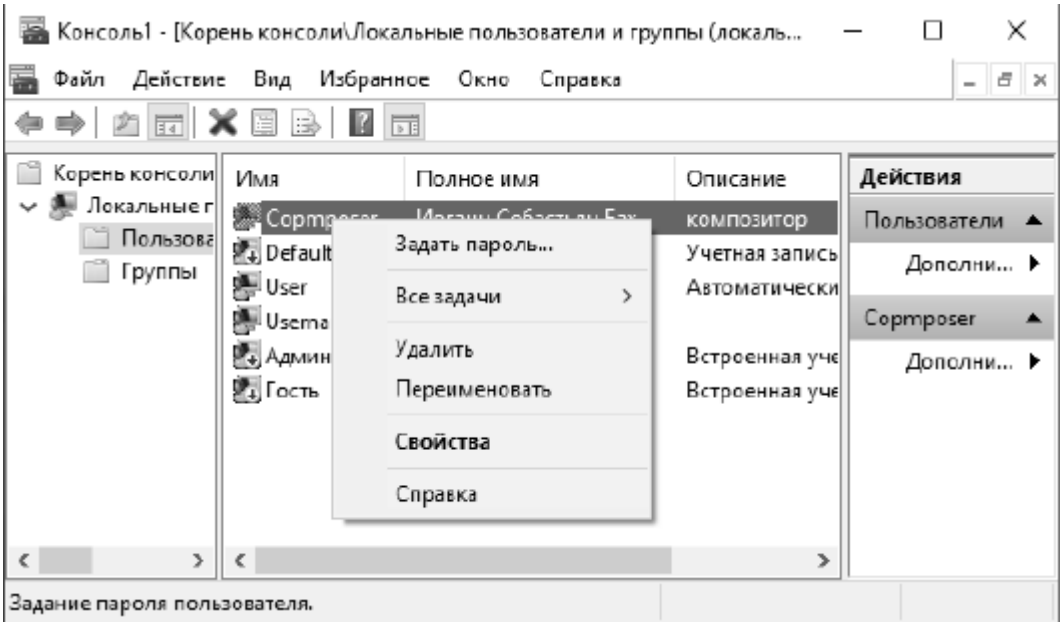

Рис. 9. Задание пароля пользователя администратором

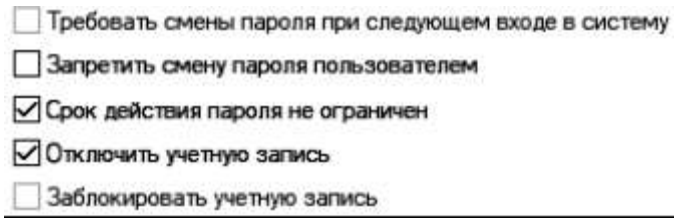

Рис. 10. Изменение свойств администратора

Войдите в систему под созданной учётной записью. При первом входе пользователю будет выдано сообщение о необходимости ввести пароль (рис. 11) и окно смены пароля (рис. 12). Смените пароль созданной учётной записи. Здесь подтверждение действий осуществляется клавишей «Enter».

Рис. 11. Сообщение пользователю о необходимости смены пароля

Рис. 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.

Рис. 13. Добавление группы

Войдите в систему под учётной записью «Администратор». Откройте «Свойства» созданной учётной записи. На вкладке «Членство в группах» добавьте пользователя в группу «Опытные пользователи» (рис. 13). Имя группы можно ввести самостоятельно или

выбрать из списка, предоставляемого после последовательного нажатия кнопок «Дополнительно» и «Поиск».

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. 14)

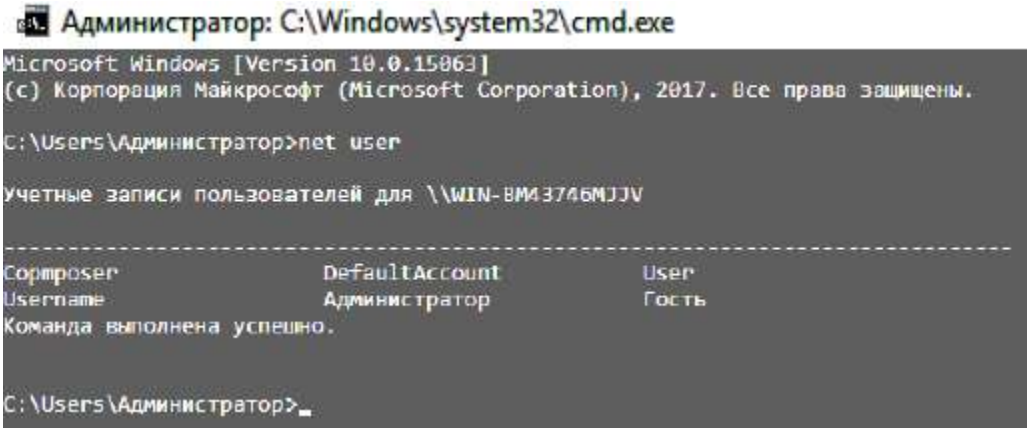

Рис. 14. Список пользователей в командной строке

Создание и изменение учётных записей осуществляется при помощи команды «net user». Подробную информацию о команде можно получить, введя «net user /help» (рис. 15). Изучите предлагаемые функции команды.

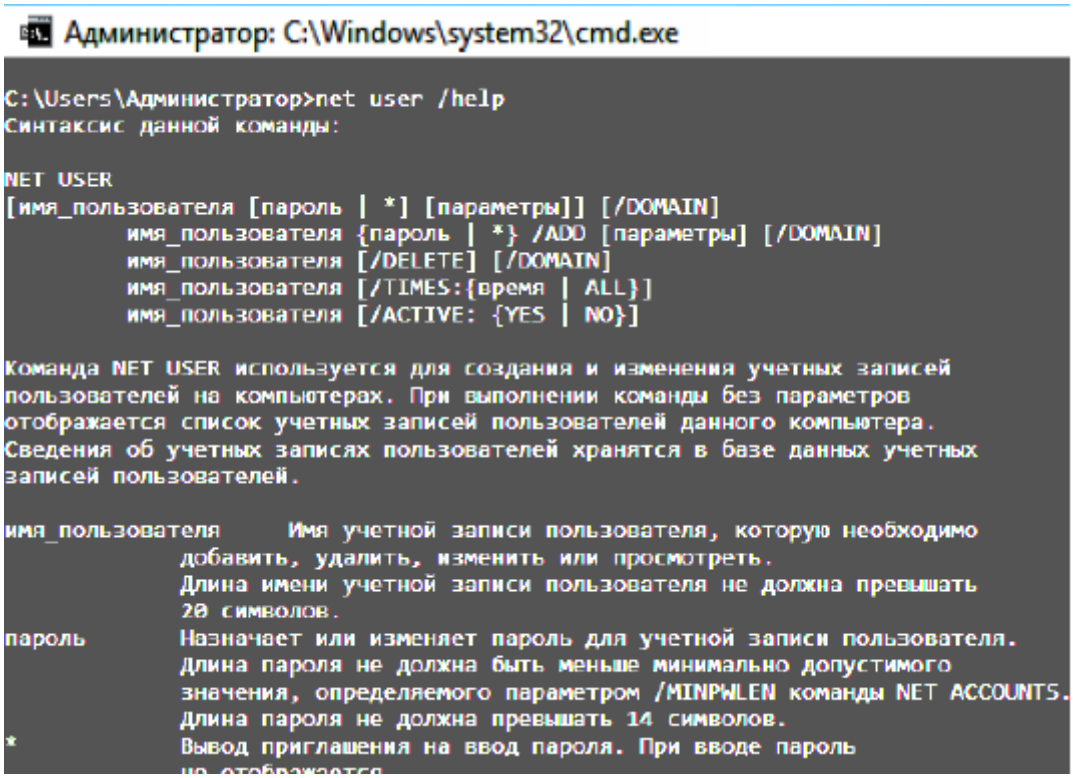

Рис. 15. Справка по команде Net user

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. 16).

Синтаксис команды Net user при создании учётной записи пользователя:

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

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

```
C:\Users\Администратор>net user XXX 12345 /add /fullname:"XXX YYY"
Команда выполнена успешно.
```

Рис. 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. 17).

```
C:\Users\ Администратор >net user sdv *
Введите пароль для пользователя:
Повторите ввод пароля для подтверждения:
Команда выполнена успешно.
```

Рис. 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. 18). Переведите часы на время, не входящее в интервал рабочего, и протестируйте возможность входа пользователя в операционную систему.

```
C:\Users\Администратор>net user XXX /times:Пн-Пт,09:00-18:00
Команда выполнена успешно.
```

Рис. 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. 19).

```
C:\Users\Администратор>net user XXX /active:no
Команда выполнена успешно.
```

Рис. 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. 20). Установите системное время на срок более поздний, чем

установленное ограничение. Попытайтесь войти в систему под данной учётной записью – операционная система выдаст ошибку (рис. 21).

```
C:\Users\Администратор >net user XXX /expires:07.09.2021
Команда выполнена успешно.
```

Рис. 20. Ограничение времени действия учётной записи

Рис. 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. 22). Выведите список всех существующих групп.

Синтаксис команды Net net при создании локальной группы: Net localgroup имя_группы {/ADD }. Создайте локальную группу Students (рис. 23).

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. 24).

```
C:\Users\Администратор>net localgroup

Псевдонимы для \\WIN-BM43746MJJV

-------------------------------------------------------------------------------
*IIS_IUSRS
*Администраторы
*Администраторы Hyper-V
*Гости
*Криптографические операторы
*Операторы архива
*Операторы настройки сети
*Операторы помощи по контролю учетных записей
*Опытные пользователи
*Пользователи
*Пользователи DCOM
*Пользователи журналов производительности
*Пользователи системного монитора
*Пользователи удаленного рабочего стола
*Пользователи удаленного управления
*Репликатор
*Управляемая системой группа учетных записей
*Читатели журнала событий
Команда выполнена успешно.
```

Рис. 22. Список групп

```
C:\Users\Администратор>net localgroup students /add
Команда выполнена успешно.
```

Рис. 23. Создание группы

```
C:\Users\Администратор>net localgroup Students
Имя псевдонима     Students
Комментарий

Члены

-------------------------------------------------------------------------------
XXX
Команда выполнена успешно.
```

Рис. 24. Просмотр списка пользователей заданной группы

Для удаления пользователя из группы используется команда Net localgroup имя_группы имя_пользователя {/DELETE}. Удалите группу Students (рис. 25).

```
C:\Users\Администратор>net localgroup students XXX /delete
Команда выполнена успешно.
```

Рис. 25. Исключение пользователя из группы

Для удаления группы используется команда Net localgroup имя_группы {/DELETE}. Удалите группу Students (рис. 26).

```
C:\Users\Администратор>net localgroup students /delete
Команда выполнена успешно.
```

Рис. 26. Удаление группы пользователей

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

3. Настройка политики учётной записи

Откройте «Локальную политику безопасности», вызвав её запросом secpol.msc в меню «Пуск». Основное окно «Локальной политики безопасности» представлено на рисунке 27. Значения параметров, заданные при настройке политики, будут применяться ко всем пользователям локального компьютера.

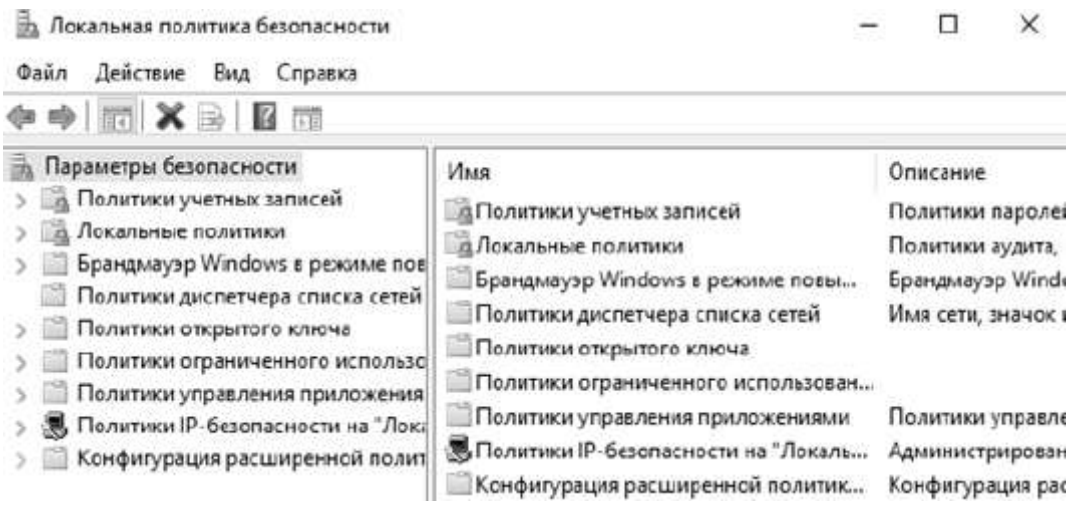

Рис. 27. Локальная политика безопасности

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 рис. 28.

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».*

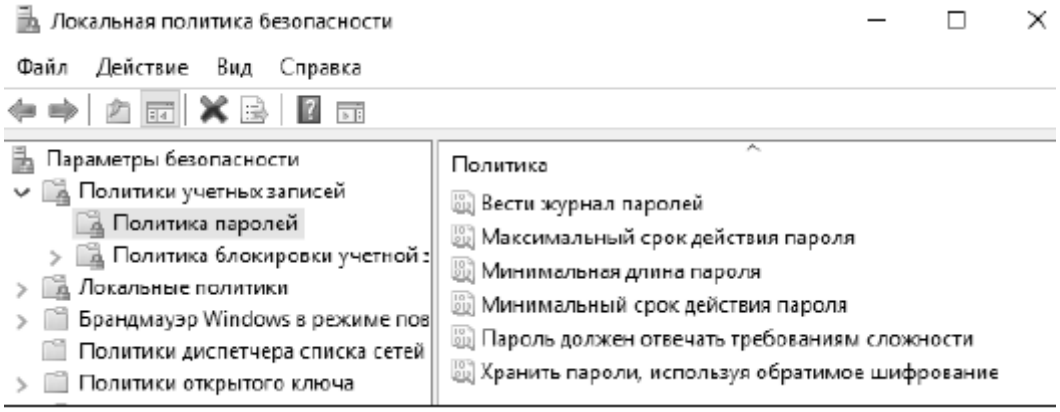

Рис. 28. Политика паролей

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. 29). При смене пароля попытайтесь заменить пароль на более простой (например, abc12345 или включающий имя учётной записи).

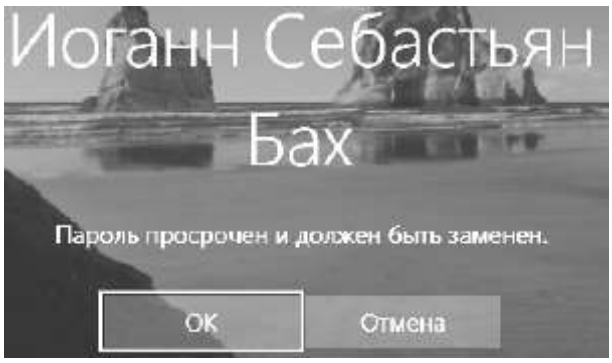

Рис. 29. Сообщение об истечении срока действия пароля

В этом случае пользователю будет выдано сообщение об ошибке при смене пароля (рис. 30). Введите пароль, удовлетворяющий требованиям.

Рис. 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 31.

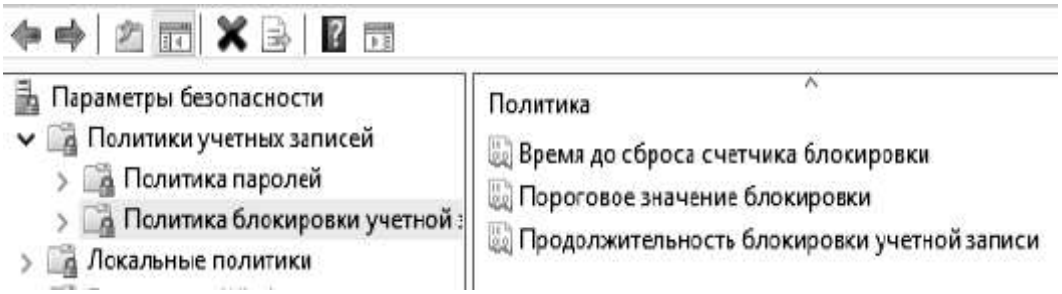

Рис. 31. Политика блокировки учетной записи

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 мин. 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. 32).

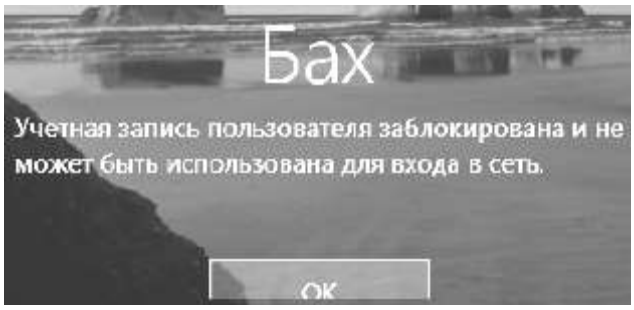

Рис. 32. Сообщение о блокировке учетной записи

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. 33).

Задайте следующие требования к паролю:

- *минимальную длину – 6 символов;*
- *максимальный срок действия пароля – 40 дней;*
- *запрет использования 3 последних паролей пользователя.*

```
C:\Users\Администратор>net accounts
Принудительный выход по истечении времени через:        Никогда
Минимальный срок действия пароля (дней):                0
Максимальный срок действия пароля (дней):               10
Минимальная длина пароля:                               10
Хранение неповторяющихся паролей:                       3
Блокировка после ошибок ввода пароля:                   3
Длительность блокировки (минут):                        30
Сброс счетчика блокировок через (минут):                15
Роль компьютера:                                        РАБОЧАЯ СТАНЦИЯ
Команда выполнена успешно.
```

Рис. 33. Просмотр информации о требованиях к качеству паролей

Применение этих требований (рис. 34) производится при помощи следующих параметров команды Net accounts:

/MINPWLEN: длина /MAXPWAGE: дни /UNIQUEPW: число

```
C:\UsGrs\Администратор>net accounts /minpwlen:6 /maxpwage:40 /uniquepw:3
Команда выполнена успешно.
```

Рис. 34. Изменение требований к качеству паролей

4. Групповые политики

Откройте оснастку «Групповая политика» («Пуск → Выполнить → gpedit.msc»). Оснастка «Групповая политика» состоит из двух основных частей: конфигурация компьютера и конфигурация пользователя (рис. 35).

«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. 36).

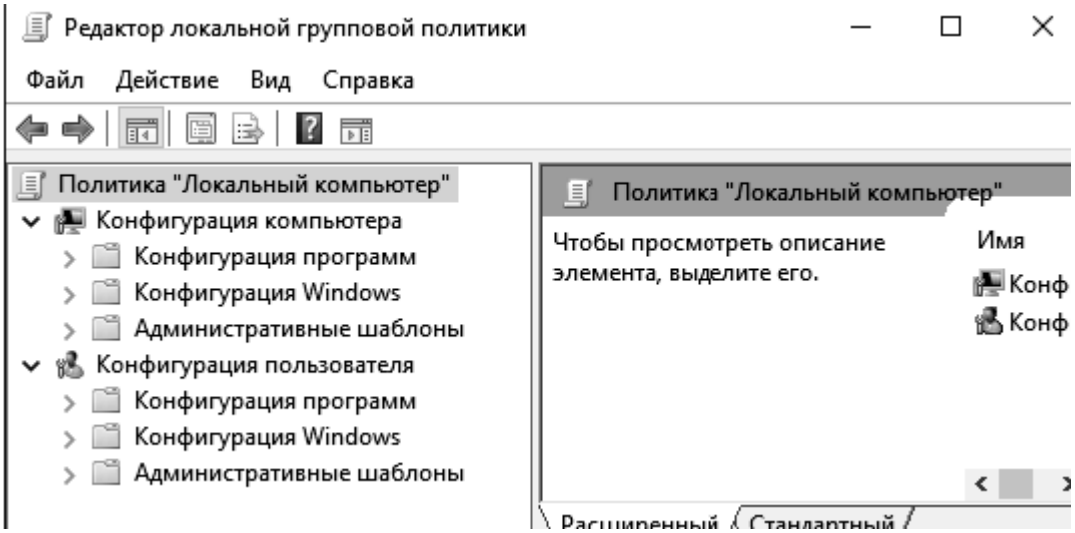

Рис. 35. Редактор групповых политик

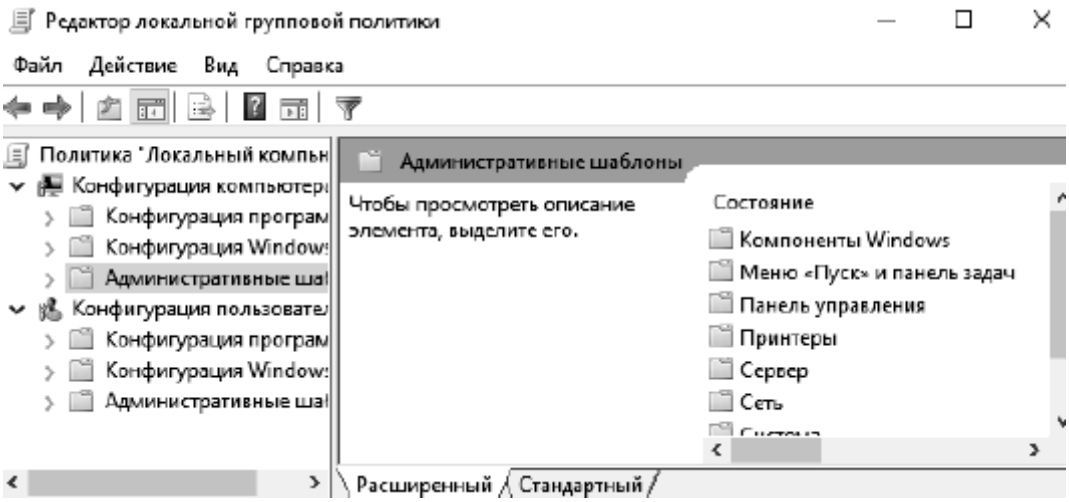

Рис. 36. Раздел «Административные шаблоны»

Средствами виртуальной машины подключите компакт-диск. В разделе «Административные шаблоны» выберите подраздел «Компоненты Windows» - «Политики автозапуска». Включите параметр «Выключение автозапуска» (рис. 37). Чтобы проверить выполнение данного параметра, необходимо повторно вставить диск в CD-привод. Система не будет производить его автозапуск, как это делалось раньше.

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. 38).

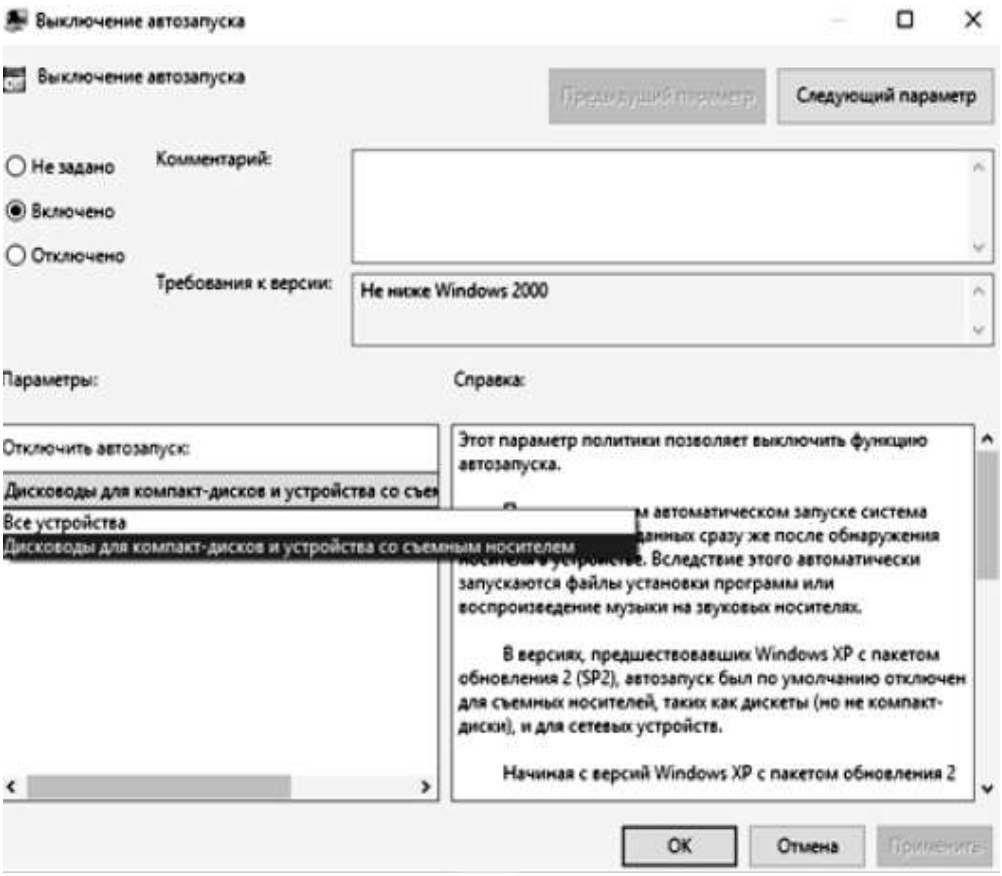

Рис. 37. Выключение автозапуска носителя

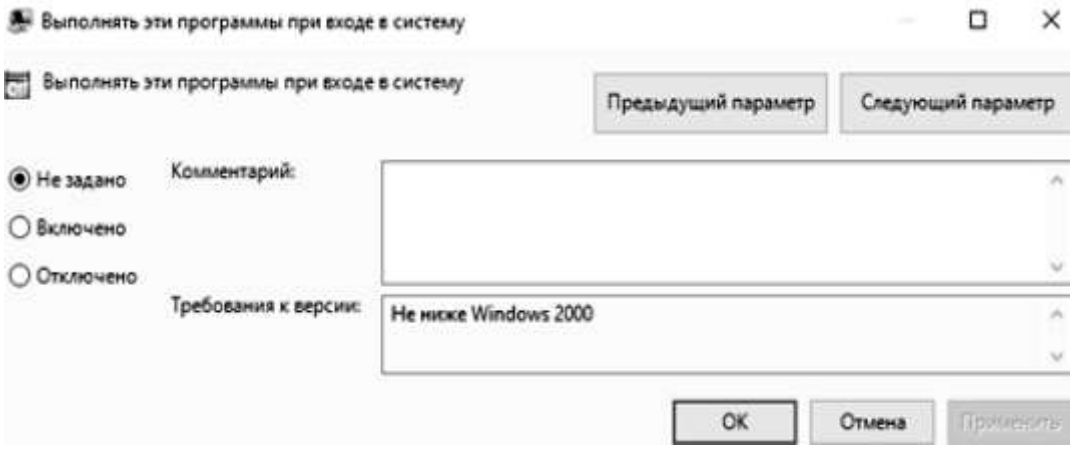

Рис. 38. Включение параметра

Добавленные программы (рис. 39) будут запускаться при каждом входе пользователя в систему. Для проверки повторно войдите в систему.

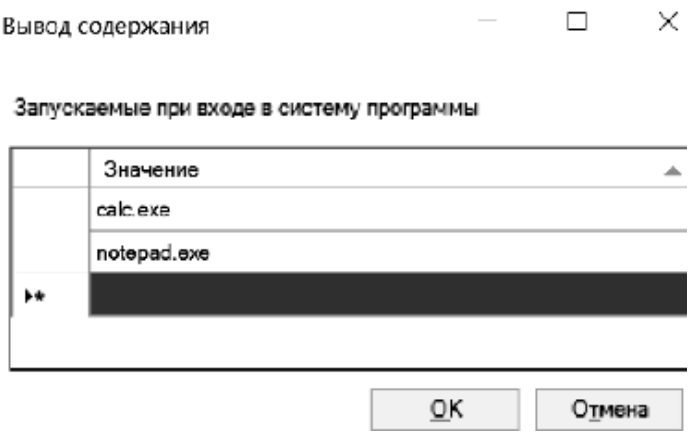

Рис. 39. Список запускаемых программ

«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 C:\ (рис. 40).

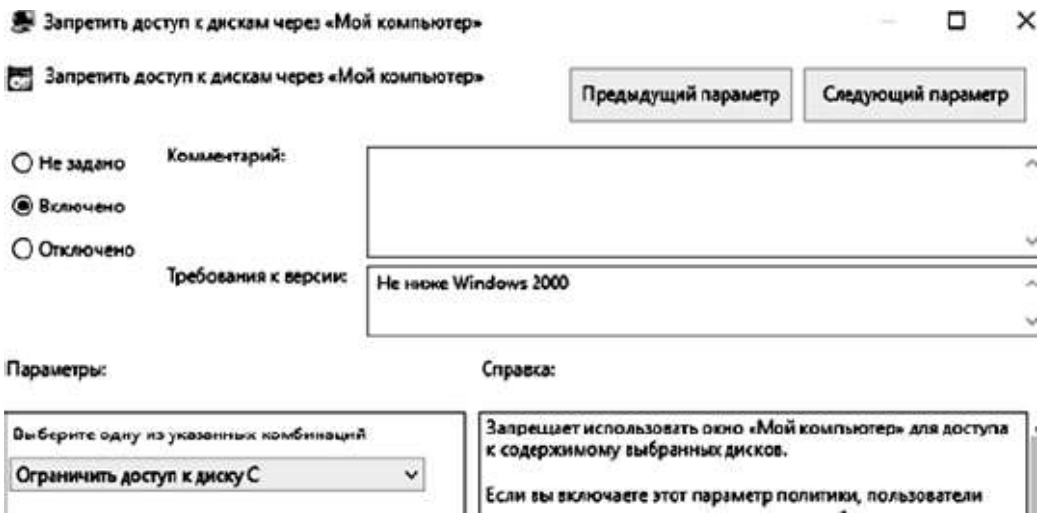

Рис. 40. Включение ограничения доступа к диску D

Попытайтесь открыть диск D:\ через «Мой компьютер» (рис. 41) и командную строку (рис. 42). В первом случае система откажет в доступе, а во втором – доступ будет предоставлен (т.к. доступ запрещён только через «Проводник»).

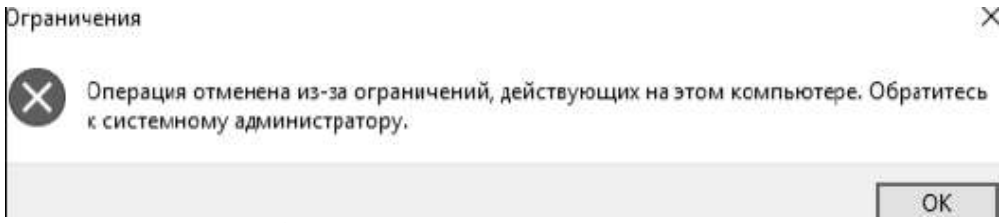

Рис. 41. Попытка доступа через проводник

```
C:\Users\Администратор>C:

C:\Users\Администратор>_
```

Рис. 42. 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» (рис. 43). Попытайтесь открыть «Панель управления».

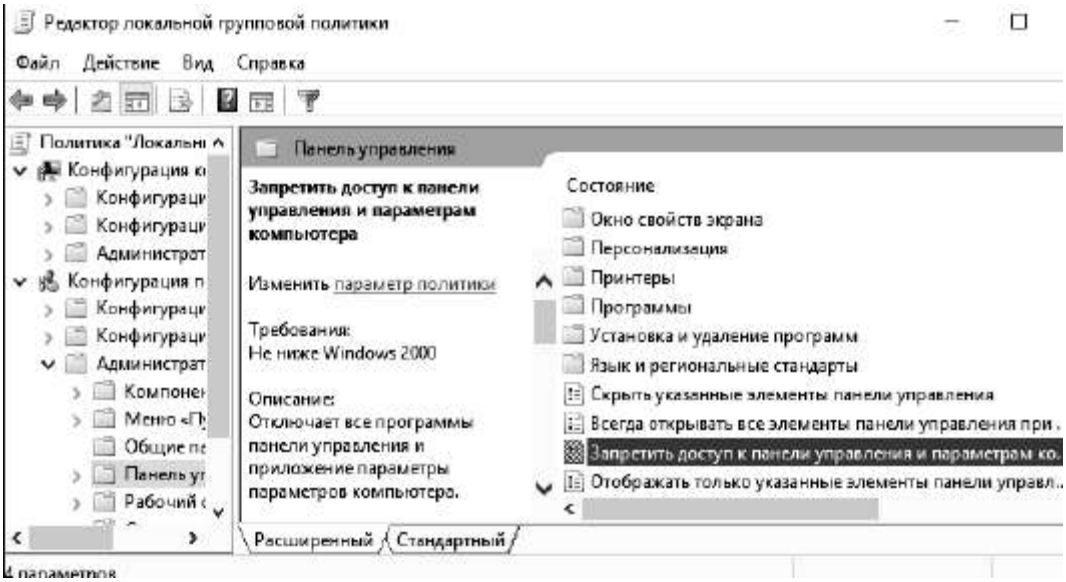

Рис. 43. Ошибка при открытии панели управления

Для полного запрета использования командной строки включите параметр «Запретить использование командной строки» в подразделе «Система». Попытайтесь запустить cmd.exe (рис. 44).

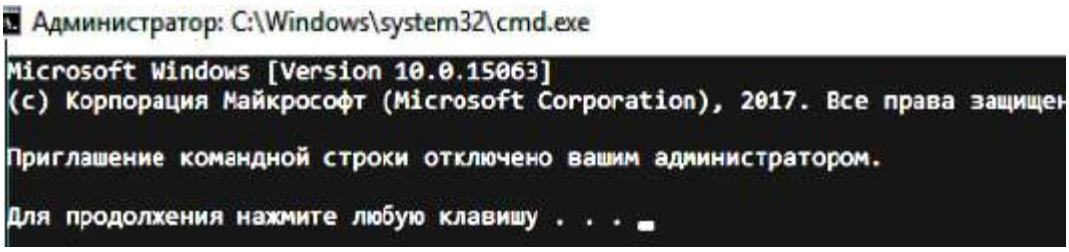

Рис. 44. Попытка запуска командной строки

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.

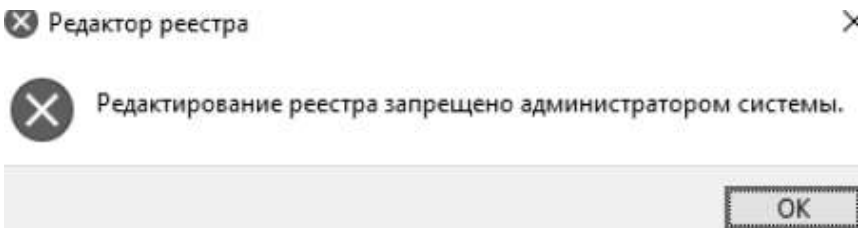

Рис. 45. Попытка запуска реестра

Добавление и удаление шаблонов может производиться через контекстное меню раздела «Административные шаблоны» (рис. 46). В появившемся контекстном меню

выберите «Добавление и удаление шаблонов». В появившемся окне можно удалить любой шаблон, а также добавить новый шаблон политики.

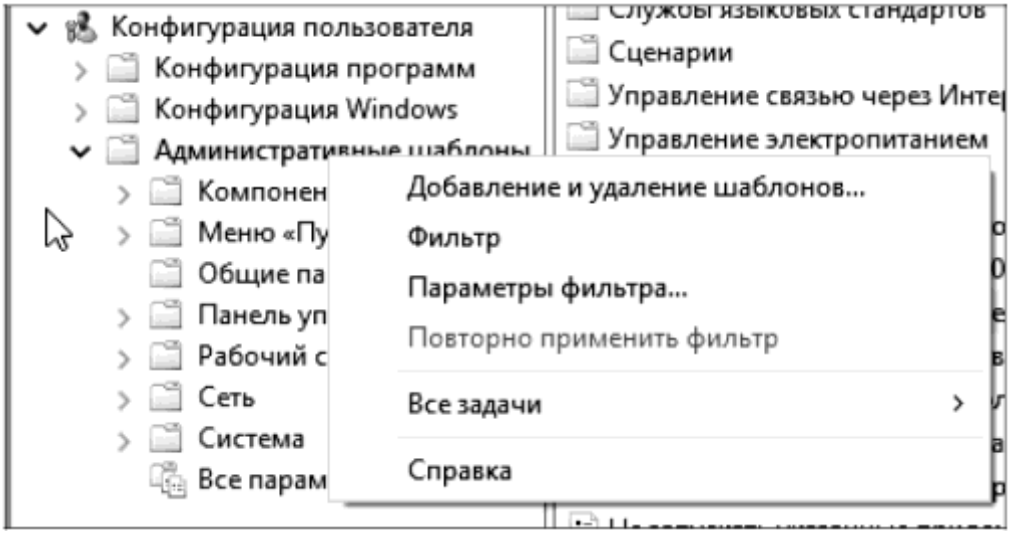

Рис. 46. Контекстное меню административных шаблонов

5. Контрольные вопросы

1. Поясните параметр «Пароль должен отвечать требованиям сложности» и перечислите минимальные требования, которым должны удовлетворять пароли, если параметр включен.
2. Какие параметры входят в политику блокировки учётной записи?
3. Возможно ли, что учётная запись не будет блокирована при количестве ошибок большем, чем установленное пороговое значение?
4. Что такое и для чего применяется MMC?
5. Что такое оснастка?
6. В чём состоит отличие конфигурации компьютера от конфигурации пользователя в групповой политике?
7. Каким образом можно включить автозапуск программ через групповую политику?
8. При помощи какой команды можно получить список пользователей операционной системы?
9. При помощи какой команды можно получить список групп пользователей операционной системы?
10. При помощи какой команды можно создать нового пользователя?

6. Задание на лабораторную работу

1. *Ознакомьтесь с теорией.*
2. *Выполните представленные задания и составьте по проделанной работе отчет.*
3. *В оснастке «Локальные пользователи и группы» создайте новую группу пользователей. В качестве имени группы пользователей используйте номер Вашей учебной группы.*
4. *Создайте учётную запись с именем Вашей учётной записи в кафедральной сети и включите её в созданную группу.*
5. *Примените к созданной учётной записи настройки, указанные в Вашем варианте (табл. 1).*
6. *Создайте новую консоль. Добавьте в корень консоли оснастки «Редактор объекта групповой политики» и «Результирующая политика». Сохраните консоль в режиме, указанном в Вашем варианте (табл. 2.).*

7. *Установите параметры групповой политики, указанные в Вашем варианте (табл. 2), и продемонстрируйте преподавателю результат применения параметров (например, невозможность запуска редактора реестра).*
8. *Продемонстрируйте преподавателю изменённые параметры при помощи «Результирующей политики» для пользователя «user».*

Таблица 1. Варианты заданий работы с пользователями

Вариант / Параметр	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
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	+		+		+		+		+	

Таблица 2. Варианты работы с групповыми политиками

Вар.	Режим работы с консолью	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 обязательный запрос пароля при выходе из экранной заставки. Удалить «Завершение сеанса» из меню «Пуск»
7	Пользовательский - многооконный	Скройте диск D: (CD-привод) из окна «Мой компьютер». Удалить значок «Мои документы» с «Рабочего стола»
8	Пользовательский - однооконный	Удалите «Общие документы» из окна «Мой компьютер». Скрыть общие группы программ из меню «Пуск»
9	Авторский	Запретите 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

Отчет по лабораторной работе выполняется по стандарту, описанному в методических указаниях