**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**Лабораторная работа № 1**

на тему «Управление пользователями и группами в операционных системах семейства Windows, локальная политика безопасности»

|  |
| --- |
| Выполнил: студент группы ВКБ41 |
| Якушевский Сергей Сергеевич |
| (Фамилия, имя, отчество) |
| Проверил: |
| Скляров Алексей Викторович |
| (Фамилия, имя, отчество) |

Оглавление

[Цель: 3](#_Toc176738785)

[Задания 3](#_Toc176738786)

[1. «Управление пользователями и группами» 3](#_Toc176738787)

[2. Изменение пароля пользователя 9](#_Toc176738788)

[3. Отключение и активизация учетной записи пользователя 10](#_Toc176738789)

[4. Удаление учетной записи пользователя 11](#_Toc176738790)

[5. Задание «Локальная политика безопасности» 15](#_Toc176738791)

[6. Блокировка учётных записей 16](#_Toc176738792)

[7. Аудит 19](#_Toc176738793)

[8. Политики прав пользователей и безопасности 20](#_Toc176738794)

[9. Запрет запуска программ 21](#_Toc176738795)

[Контрольные вопросы: 23](#_Toc176738796)

## **Цель**:

- изучить способы создания локальных учетных записей пользователей и групп и настройки их свойств;

- изучить возможности настройки локальных политик безопасности для установки требований к паролям и учётным записям, блокировки нежелательных программ и сетевых соединений.

# Задания

## «Управление пользователями и группами»

Для управления учетными записями используется компонент «Управление компьютером». Чтобы его открыть выберите Пуск → Настройка → Панель управления. Дважды щелкните значок «Администрирование» затем дважды щелкните значок «Управление компьютером». Второй способ открыть «Управление компьютером» нажать правой кнопкой на значке «Мой компьютер» и в появившемся контекстном меню выбрать «Управление».

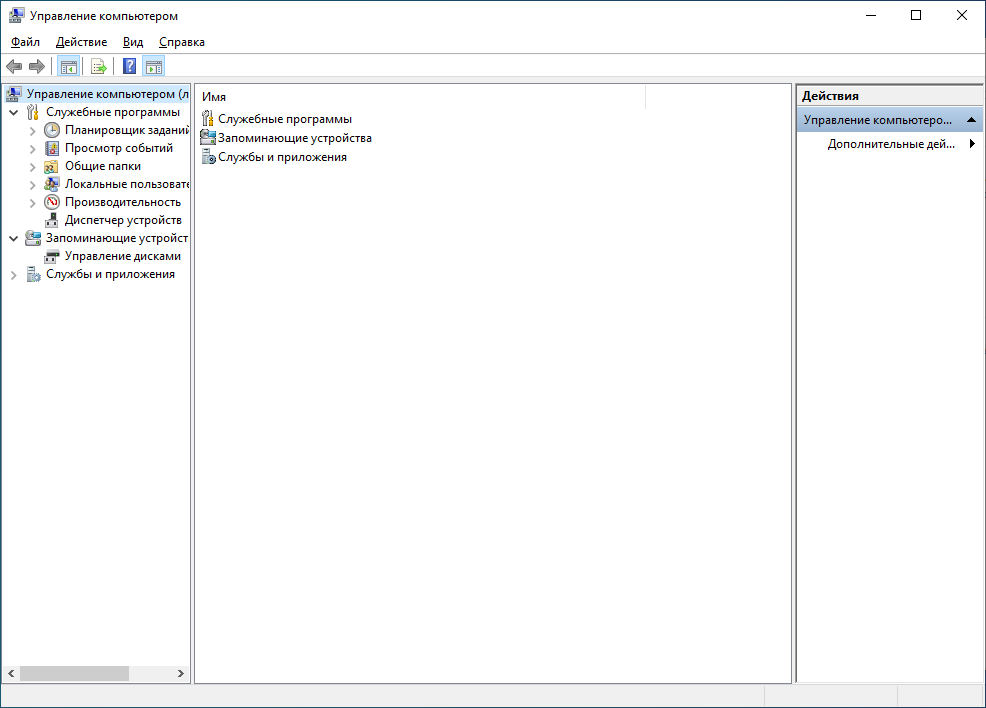


Рисунок1Управление

Откройте компонент «Управление компьютером» одним из описанных выше способов. В дереве консоли (слева) выберите компонент «Локальные пользователи и группы» и щелкните в нем узел «Пользователи». Нажмите правой кнопкой мыши в окне со списком пользователей и в появившемся меню выберите команду «Новый пользователь»

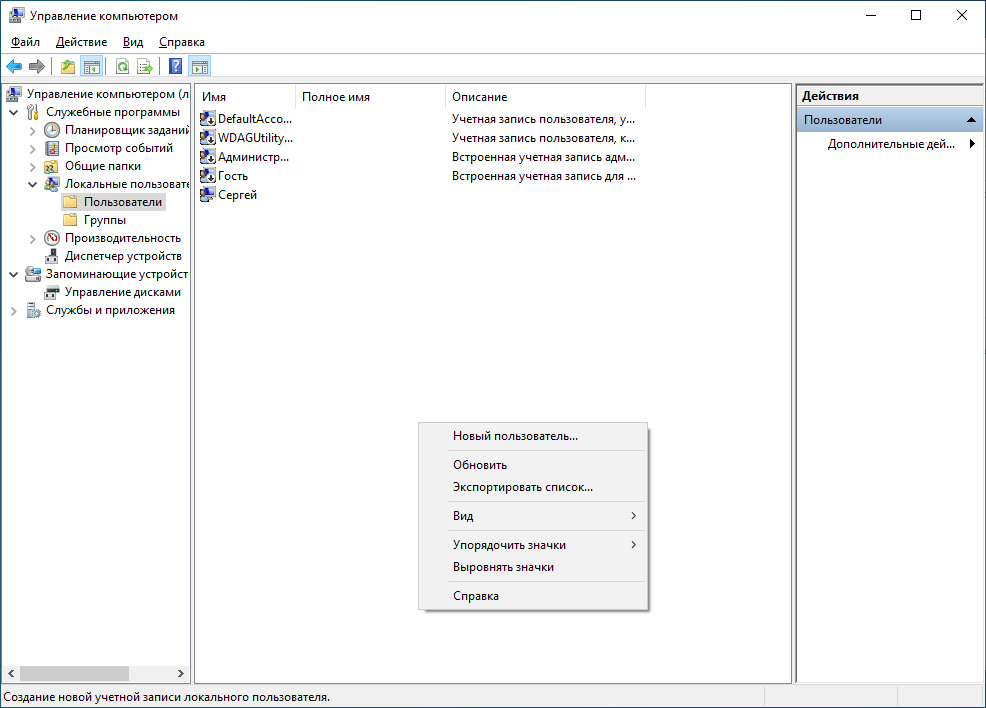


Рисунок 2 Создание нового пользователя

В появившемся окне заполните поля «Пользователь», содержащее имя, под которым пользователь будет входить в систему, а также «Пароль» и «Подтверждение».

Создайте пользователей User 1 (создается через оснастку «Управление компьютером») и User 2 (создается с использованием командной строки). После создания пользователи должны появится в списке выбора пользователей на начальном экране загрузки. Сделайте скриншот полученного результата.

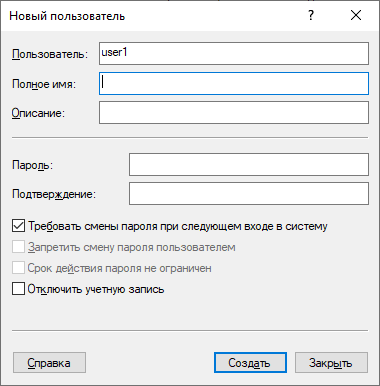


Рисунок 3 Окно создания нового пользователя

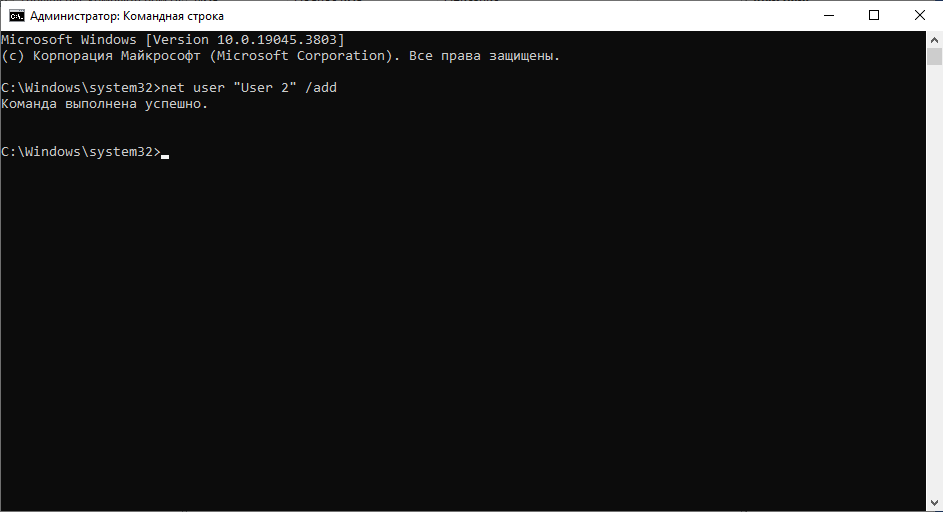


Рисунок 4 Создание пользователя User2 с помощью командной строки

Войдите от имени созданного пользователя User 2.

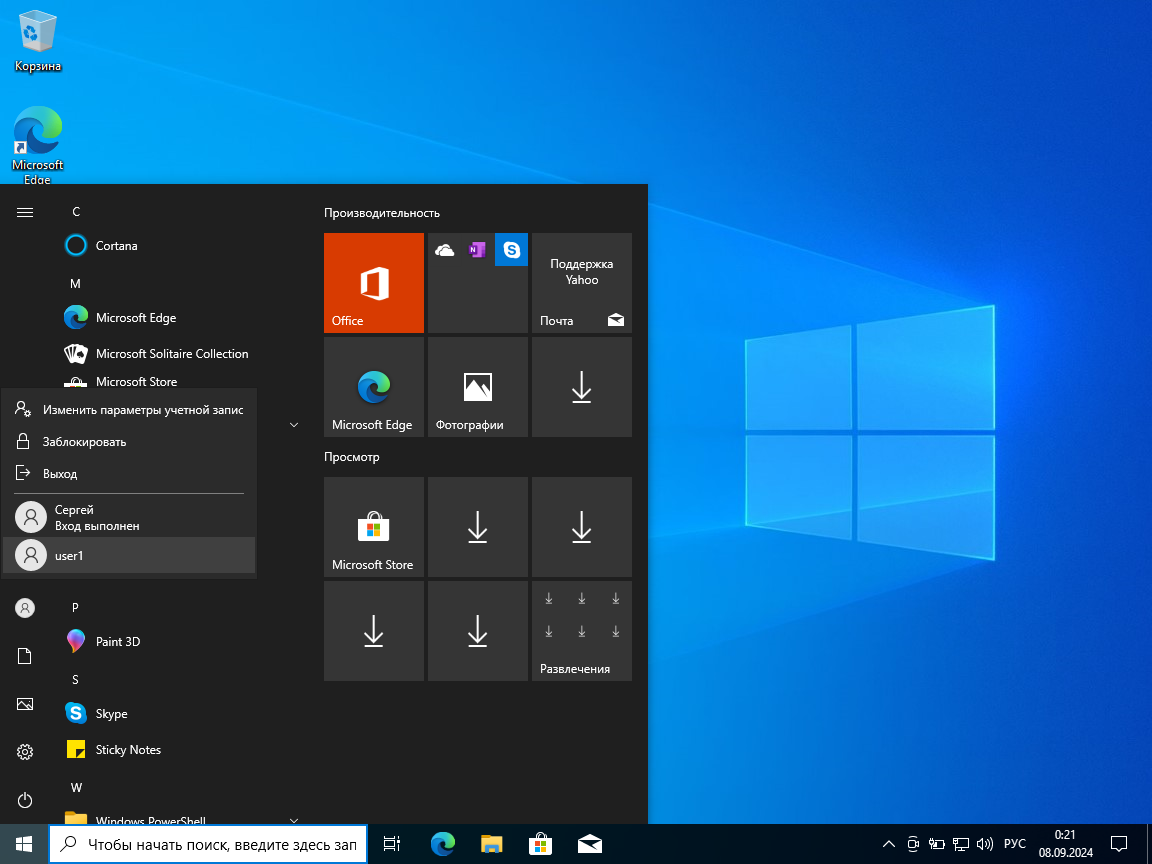


Рисунок 5 Вход под учётной записью User2

Далее смените пользователя на пользователя User 1. Для этого нажмите «Пуск» → «Выход из системы» → «Смена пользователя». На появившемся экране выберите созданного пользователя «User 1» и введите заданный для него при создании пароль. Появится окно с сообщением о необходимости изменения пароля. Задайте новый пароль и сделайте скриншот окна в котором проводились изменения.

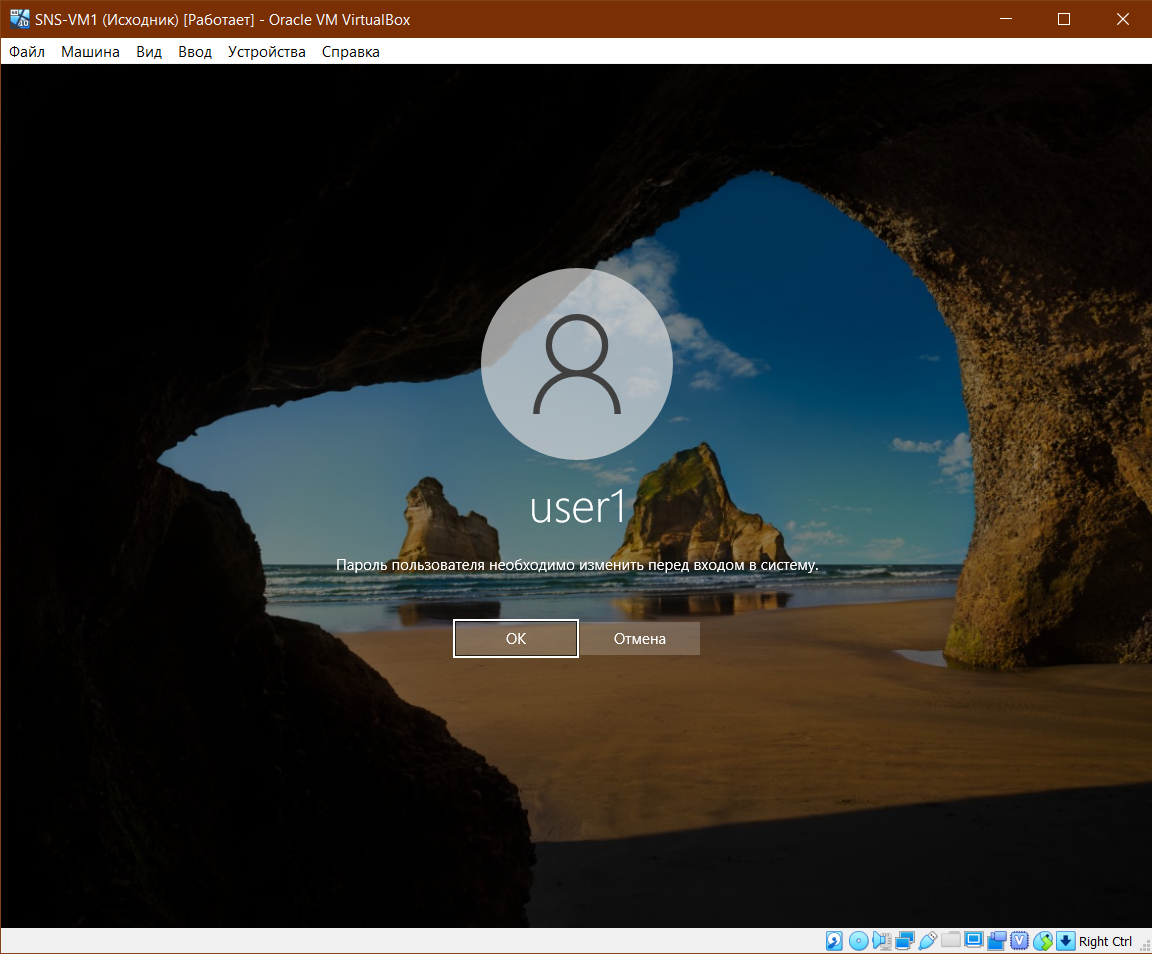


Рисунок 6 Задание нового пароля для учётной записи User1

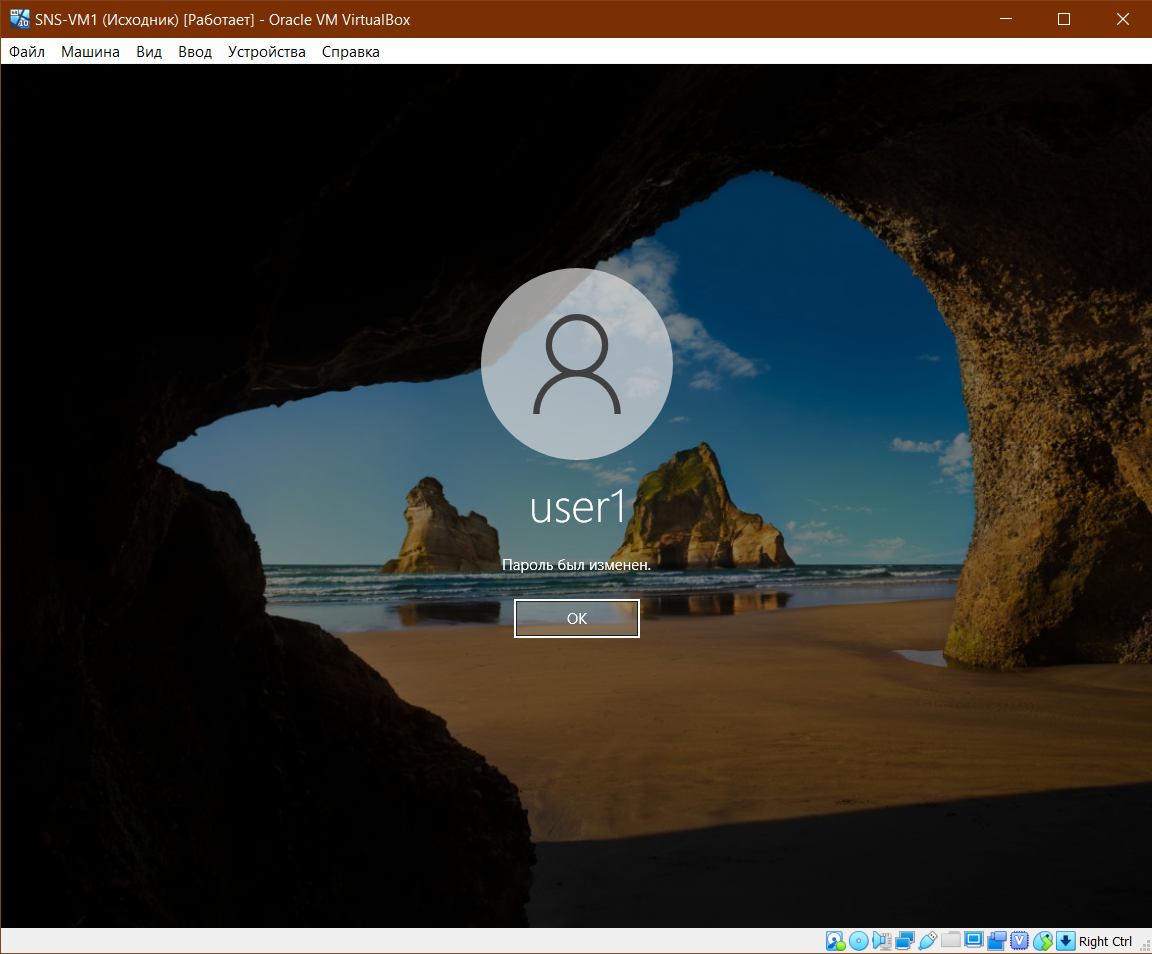


Рисунок 7 Успешное изменение пароля

Вернитесь обратно к пользователю «User 2». Для этого нажмите «Пуск» → «Выход из системы» → «Выход».

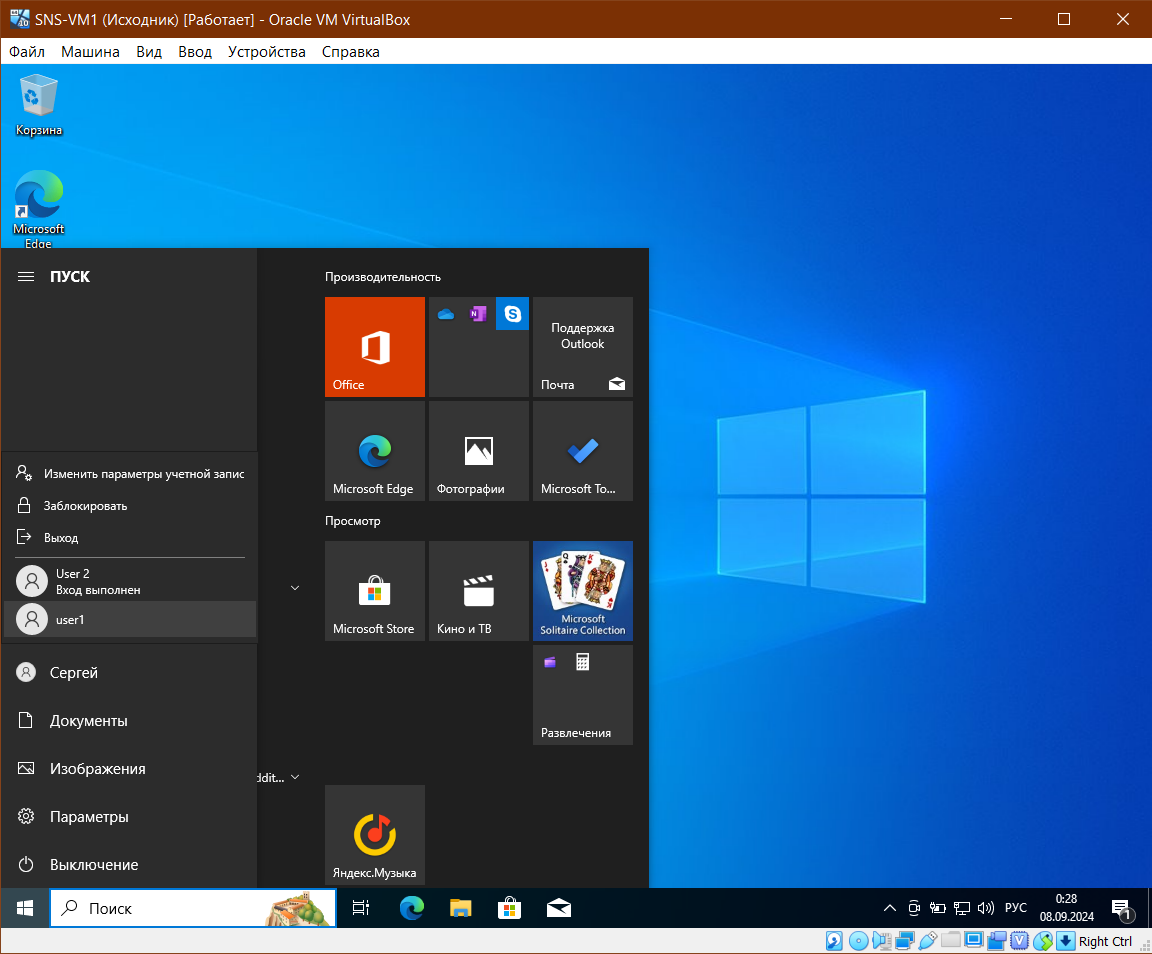


Рисунок 8 Выход из учётной записи User1 и смена пользователя User2 на Сергей

Разница между вариантами выхода из системы «Смена пользователя» и «Выход» заключается в том, что при смене пользователя все процессы, запущенные им, продолжают выполняться, а при выходе завершаются. Если завершить работу, используя учётную запись одного пользователя, пока второй остаётся в системе, это может привести к потере несохраненных данных приложений второго пользователя.

## Изменение пароля пользователя

Выберите учетную запись, которую требуется изменить (например, учетная запись пользователя «User1»). В контекстном меню выберите пункт «Задать пароль». В появившемся окне введите новый пароль и сделайте скриншот результата. Войдите в систему от имени пользователя «User1» используя новый пароль. Аналогичным образом задайте пароль учётной записи «User 2».

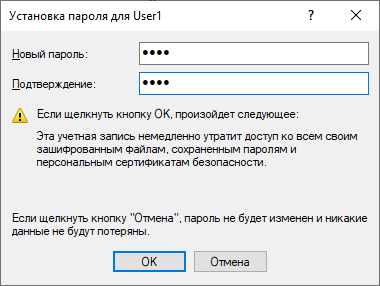


Рисунок 9 Задание нового пароля 2222 для пользователя User1

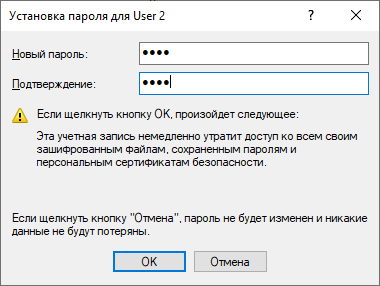


Рисунок 10 Задание пароля 2222 для пользователя User2

## Отключение и активизация учетной записи пользователя

Выберите учетную запись «User1». В контекстном меню выберите Свойства. Чтобы отключить выбранную учетную запись пользователя, установите флажок «Отключить учетную запись». Отключение учетной записи также возможно с использованием команды net user с параметрами net user имя пользователя /active:no Отключите учетную запись пользователя User 1 любым из приведенных способов, попробуйте войти от имени «User1». Сделайте скриншот результата.

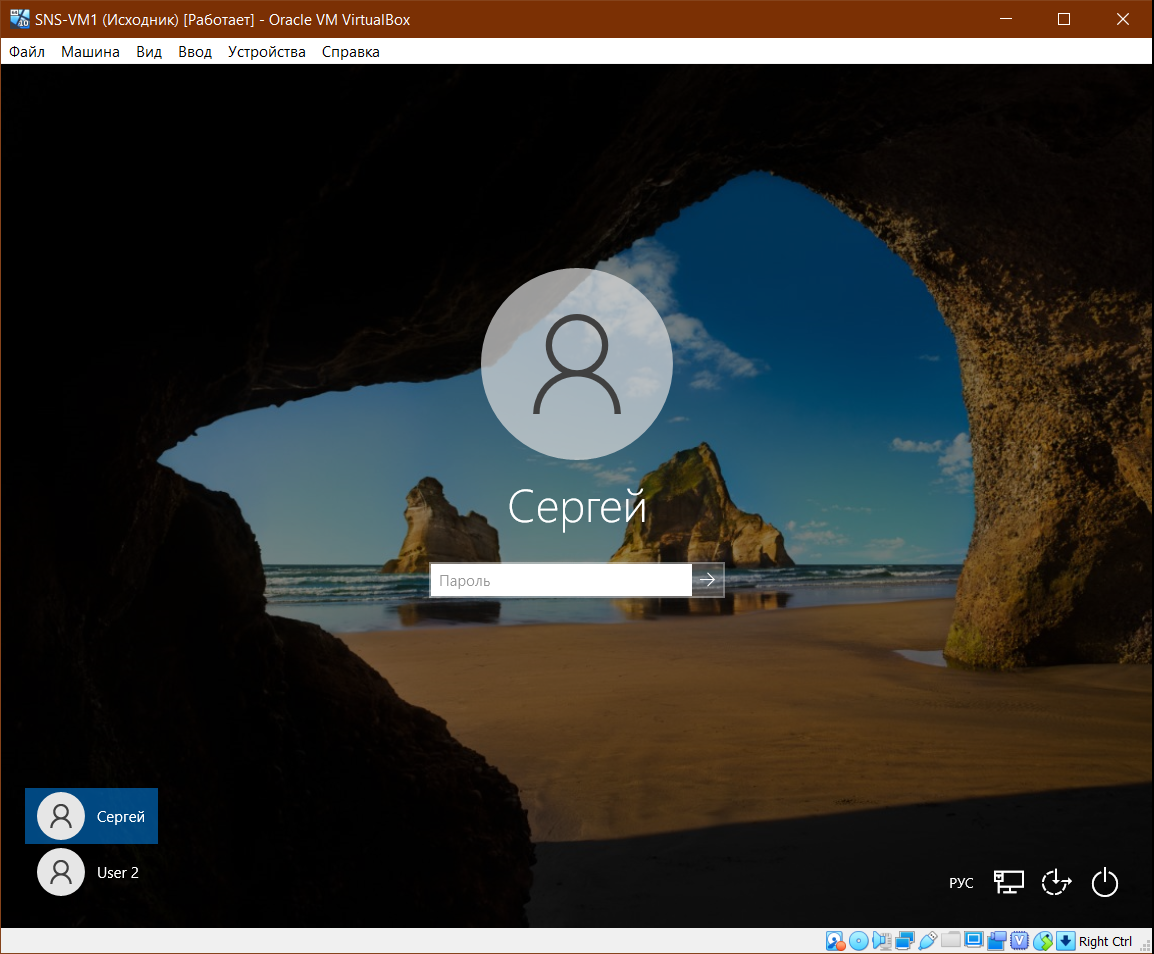


Рисунок 11 Попытка входа через учётную запись User1 неудачна. Пользователь пропал из списка предложеных

## Удаление учетной записи пользователя

Выберите учетную запись «user1». В контекстном меню учетном записи выберите Удалить. Появится окно, предупреждающее о последствиях удаления пользователя. Выберите ДА. Сделайте скриншот полученного результата. Удаление учетной записи также возможно с использованием команды net user с параметрами net user имя пользователя /delete

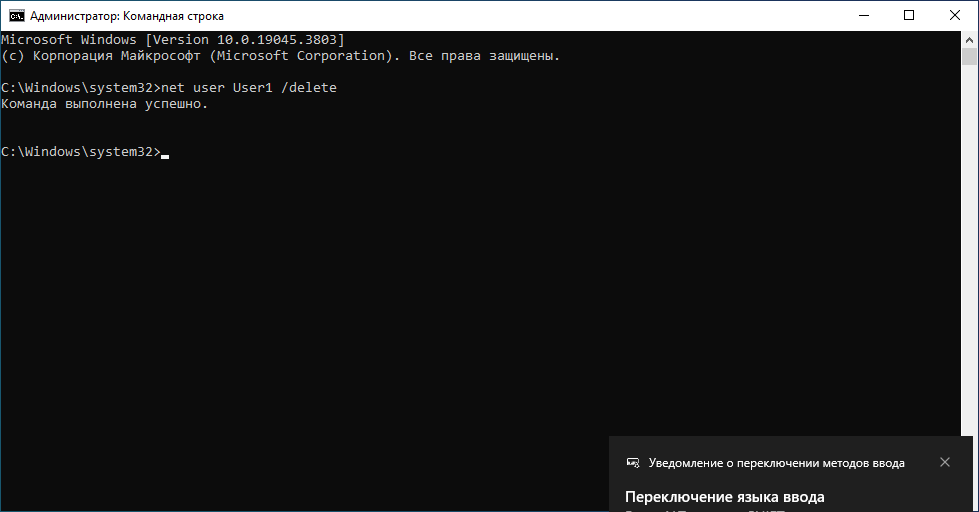


Рисунок 12 Успешное удаление учётной записи User1

Нажмите дважды на группу «Пользователи» и посмотрите, какие учётные записи входят в эту группу. Сделайте скриншот данного окна.



Рисунок 13 Список учётных записей группы "Пользователи"

Добавьте пользователя «User 1» в группу «Опытные пользователи» с помощью командной строки, сделайте скиншот результата.

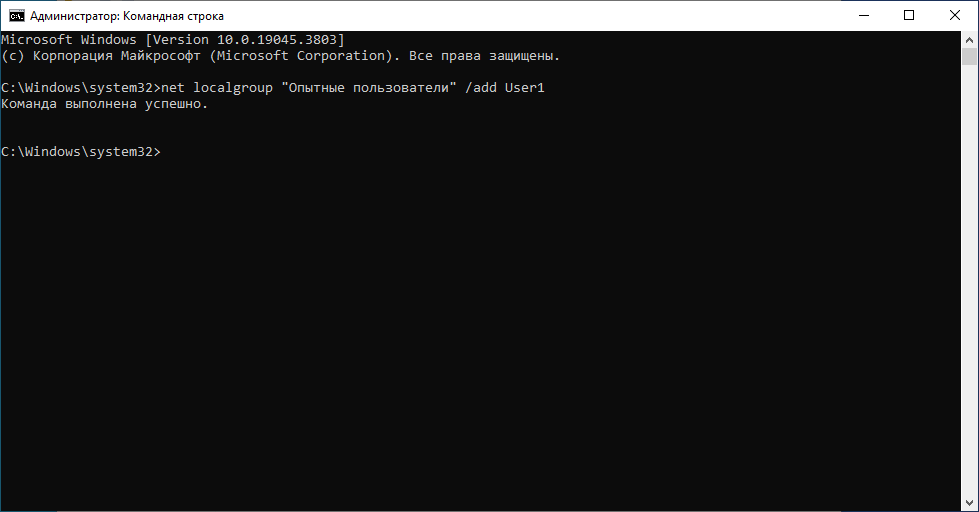


Рисунок 14 Добавление пользователя User1 в группу "Опытные пользователи"

Попробуйте от имени пользователя «User 2» создать файл на диске C:. Пользователи группы «Пользователи» не имеют данного права, поэтому будет выдано сообщение о невозможности выполнения данной операции. Сделайте его скриншот.

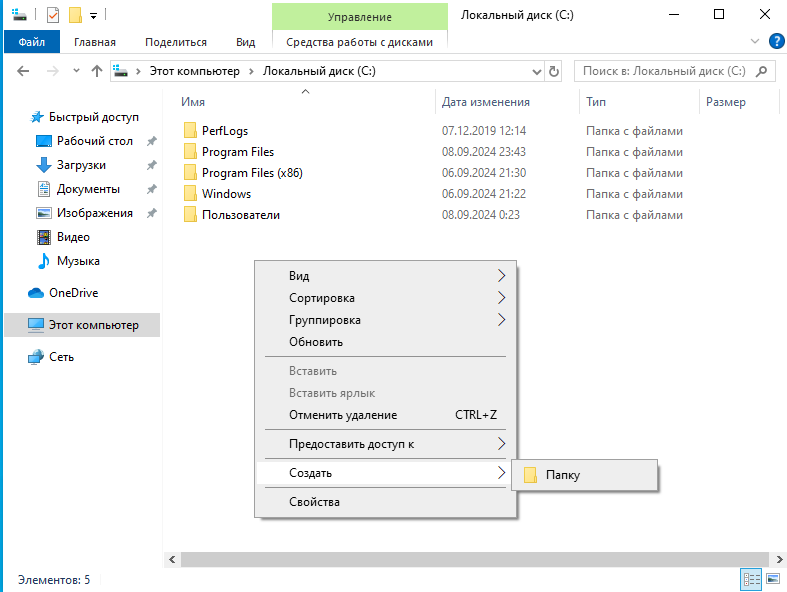


Рисунок 15 Отсутствие права на создание файла на диске С: у пользователя User2

Выйдите из системы и зайдите от имени пользователя «Администратор». Добавьте пользователя «User2» в группу «Администраторы», используя графический интерфейс. Для этого нажмите правой кнопкой на имени группы и выберите пункт меню «Добавить в группу…»

Появится окно выбора пользователя. Введите имя «User 2» и нажмите «OK».

Зайдите снова от имени «User 2» и создайте на диске C: любой файл. Сделайте скриншот результата.

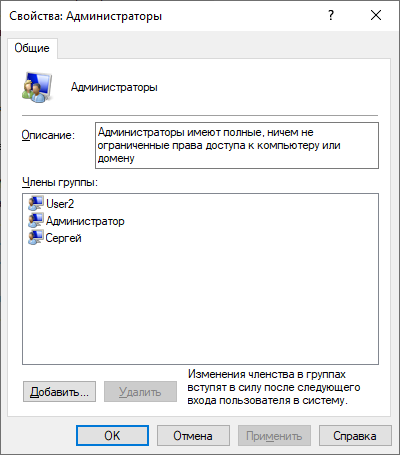


Рисунок 16 Учётная запись User2 успешно добавлена в группу "Администраторы"

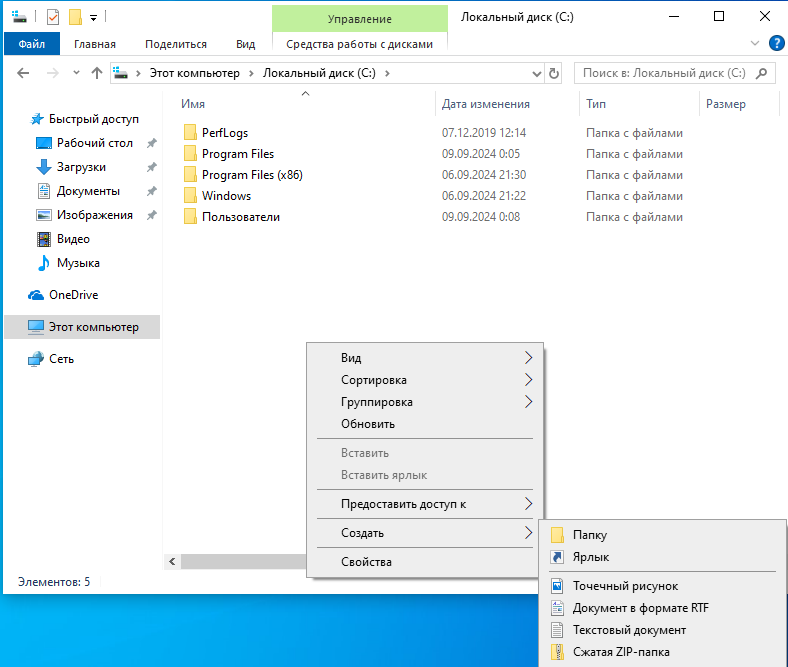


Рисунок 17 Наличие права на создание файлов у пользователя User2 после добавления учётной записи в группу "Администраторы"

## Задание «Локальная политика безопасности»

Для выполнения задания 2.2 лабораторной работы используется консоль «Локальная политики безопасности». Чтобы открыть её нажмите Пуск → Панель управления → Администрирование → Локальная политики безопасности.

**Политика паролей**

Откройте вкладку «Политики учётных записей» → «Политика паролей». Установите минимальную длину пароля — 8 символов. Смените пароль любому из существующих пользователей и проверьте невозможность задания пароля длиной меньше 8 символов. Сделайте скриншот соответствующего сообщения.

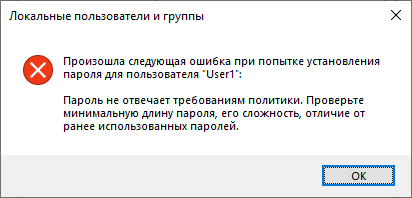


Рисунок 18 Неудачная попытка изменения пароля учётной записи User1 длиной меньше 8 символов

Включите требование «Пароль должен отвечать требованиям сложности». Смените пароль любому пользователю. Приведите примеры паролей отвечающих требованиям сложности и не отвечающих данным требованиям.

## Блокировка учётных записей

Откройте вкладку «Политики учётных записей» → «Политика блокировки учётной записи». Измените параметр «Ошибок входа в систему» политики «Пороговое значение блокировки» на 3.

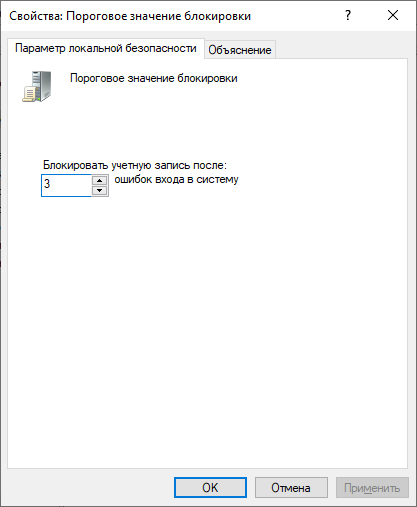


Рисунок 19 Изменение количества ошибочных попыток входа на 3

Попытайтесь войти от имени любого пользователя, например: User 1, имеющего пароль, введя неправильный пароль 3 раза. Затем введите правильный пароль и снова попытайтесь выполнить вход.

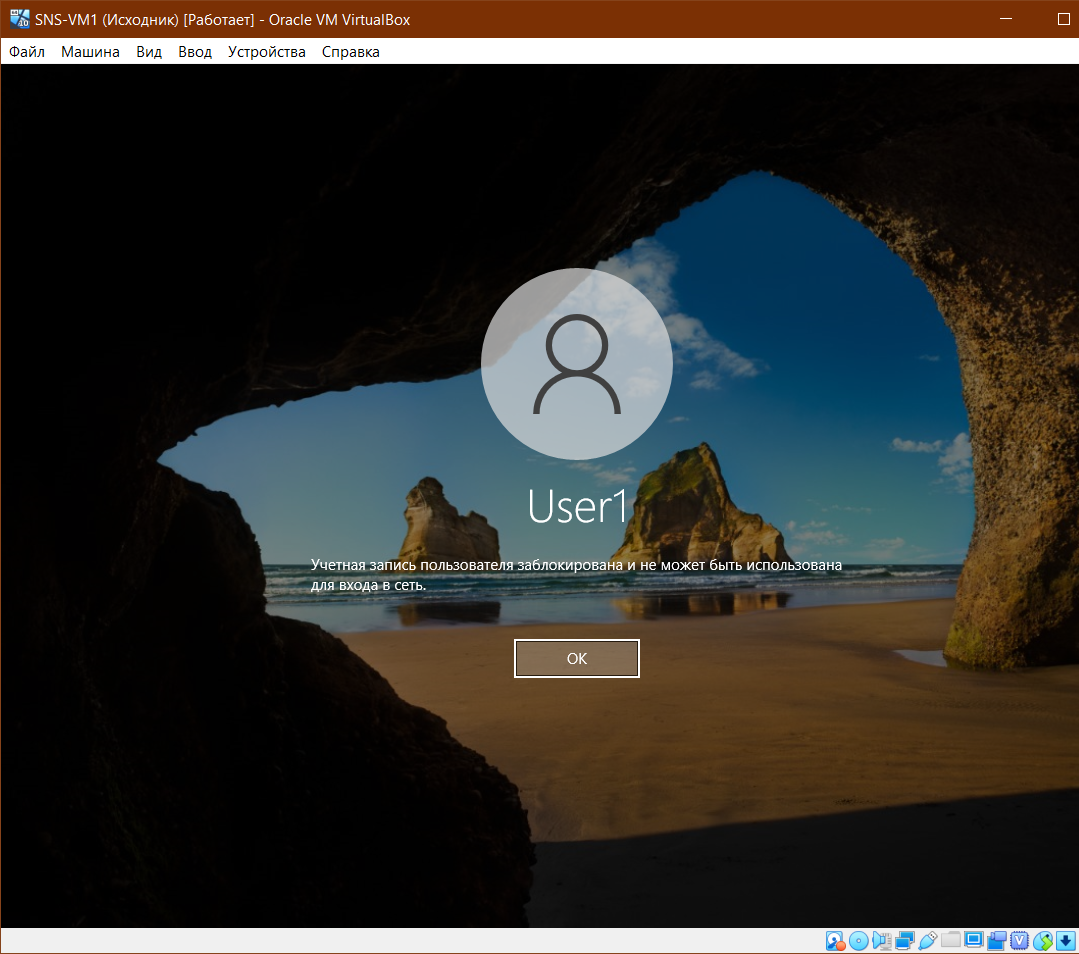


Рисунок 20 Блокировка учётной записи User1 после 3 неудачных попыток входа

Откройте консоль управления компьютером. Для этого нажмите на значке «Мой компьютер» правой кнопкой мыши и выберите пункт меню «Управление». Откройте папку «Локальные пользователи и группы» → «Пользователи» и дважды щелкните на пользователя от имени которого Вы пытались выполнить вход. Обратите внимание на установленный флажок «Заблокировать учётную запись», объясните причину блокировки пользователя, сделайте скриншот окна свойств пользователя.

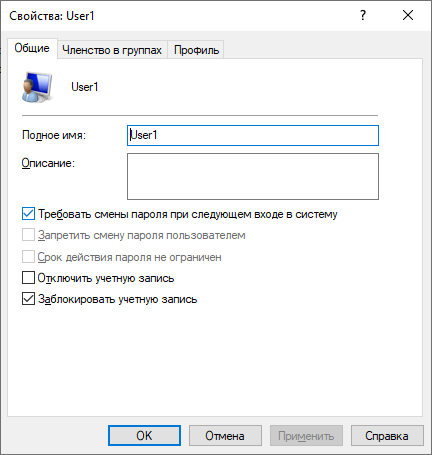


Рисунок 21 Результат блокировки учётной записи User1

Данные параметры обусловлены задаными параметрами локальной политики паролей. После 3 неудачных попыток учётная запись пользователя блокируется, другой пользователь, чья учётная запись состоит в группе «Администраторы», не разблокирует её.

## Аудит

В консоли «Локальная политика безопасности» откройте папку «Локальные политики» → «Политики Аудита» и в окне свойств каждого параметра установите флажки «Вести аудит следующих попыток доступа» в пунктах «Успех» и «Отказ».

Откройте консоль «Управление компьютером», выберите раздел «Служебные программы» → «Просмотр событий» → «Безопасность». Найдите последнюю по времени запись, относящуюся к категории «Изменение политики» откройте её и посмотрите описание события, в котором должны быть указаны новые настройки политик аудита, а ниже — пользователь, изменивший их. Текст описания события необходимо поместить в отчёт.

Описание:

Платформа фильтрации Windows заблокировала пакет.

Сведения о приложении:

Идентификатор процесса: 0

Имя приложения: -

Сведения о сети:

Направление: Входящие

Адрес источника: 20.54.37.64

Порт источника: 443

Адрес назначения: 10.0.2.15

Порт назначения: 49728

Протокол: 6

Сведения о фильтре:

Код выполнения фильтра: 68331

Имя уровня: Транспорт

## Политики прав пользователей и безопасности

В консоли «Локальная политика безопасности» откройте папку «Локальные политики» → «Назначение прав пользователя». Найдите параметр «Завершение работы системы» дважды щелкните на нём, чтобы открыть окно свойств и из перечисленных в нём групп удалите группу «Пользователи». Зайдите от имени пользователя, входящего в эту группу, и попытайтесь завершить работу, сделайте скриншот результата.

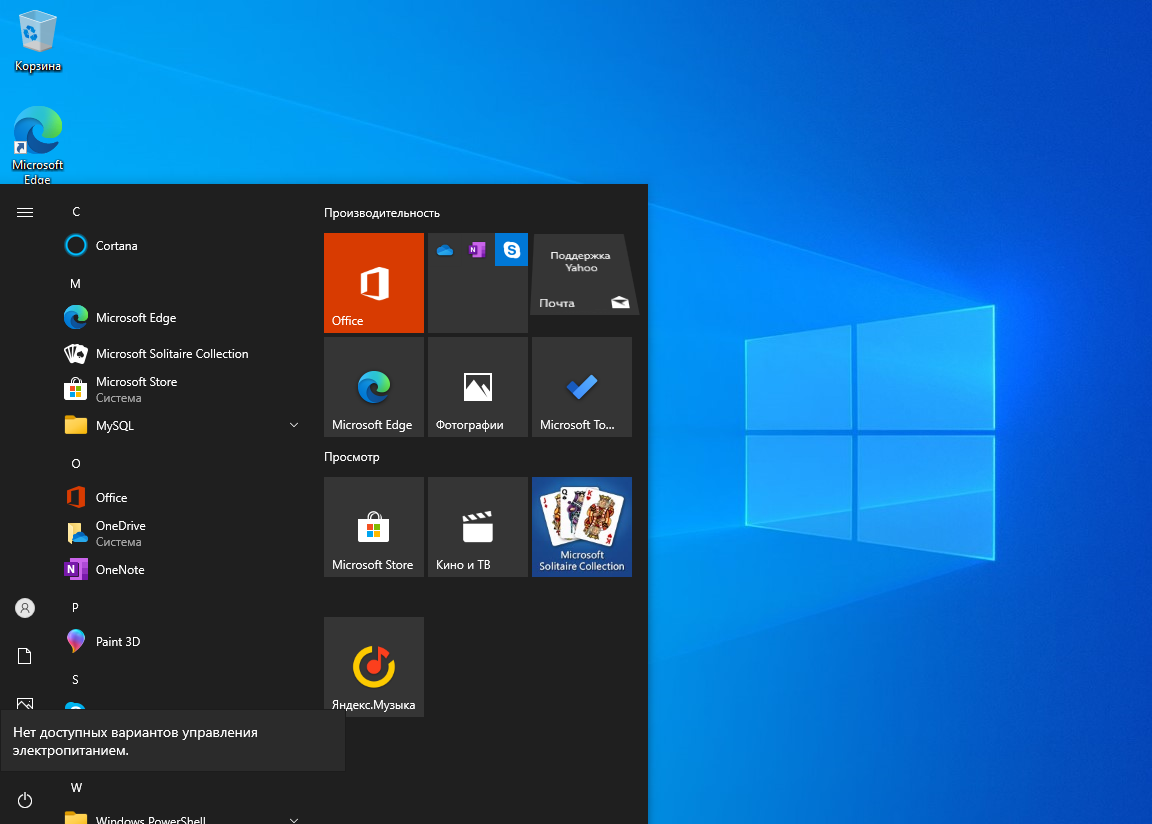


Рисунок 22 отсутствие пункта "завершение работы"

Откройте «Локальные политики» → «Параметры безопасности». Найдите параметр «Интерактивный вход в систему: Заголовок сообщения для пользователей при входе в систему» и в окне его свойств: - в поле для ввода впишите любой заголовок сообщения (например: «Сообщение»); - в поле для ввода впишите любой текст сообщения (например: «Привет»). Зайдите от имени любого пользователя и сделайте скриншот с окном сообщения, появляющимся при входе.

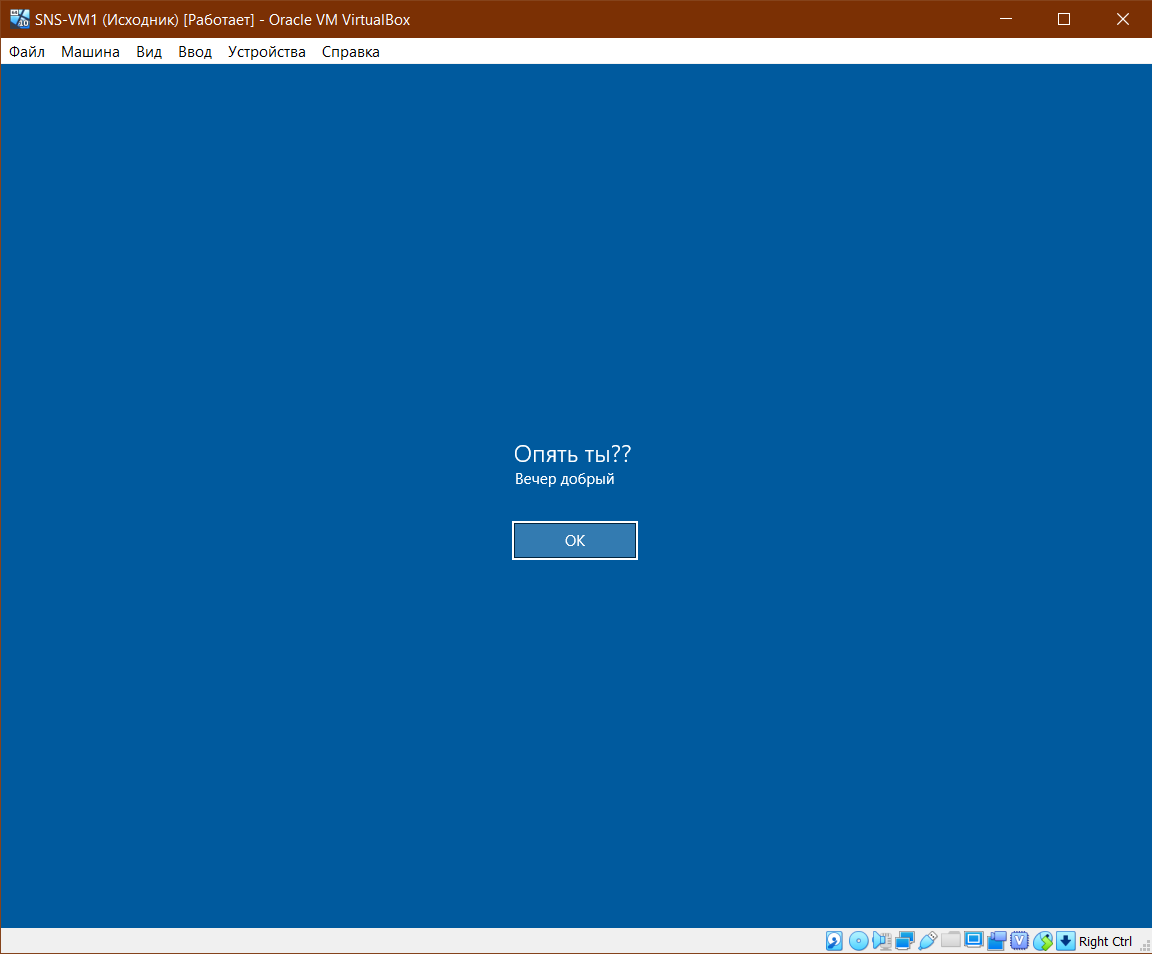


Рисунок 23 Изменение параметров интерактивного входа

## Запрет запуска программ

В консоли «Локальная политика безопасности» выделите папку «Политики ограниченного использования программ». В основном окне появится надпись «Политики ограниченного использования программ не определены».

Нажмите правой кнопкой мыши на папке «Политики ограниченного использования программ» и выберите пункт контекстного меню «Создать политику ограниченного использования программ».

Зайдите в папку «Дополнительные правила». Нажмите правой кнопкой мыши и выберите пункт контекстного меню «Создать правило для хеша…». В появившемся окне нажмите кнопку «Обзор…» и выберите хешируемый файл. Это может быть любой исполняемый файл какого-либо приложения (например калькулятор Windows — C:\Windows\system32\calc.exe).

В выпадающем меню «Безопасность» оставьте значение «Запрещено» и нажмите «OK». Попытайтесь запустить калькулятор и сделайте скриншот результата. Правило, созданное для хеша применяется к файлу независимо от того где он находится. Можно переместить файл calc.exe в любую другую папку, и он попрежнему не будет запускаться.

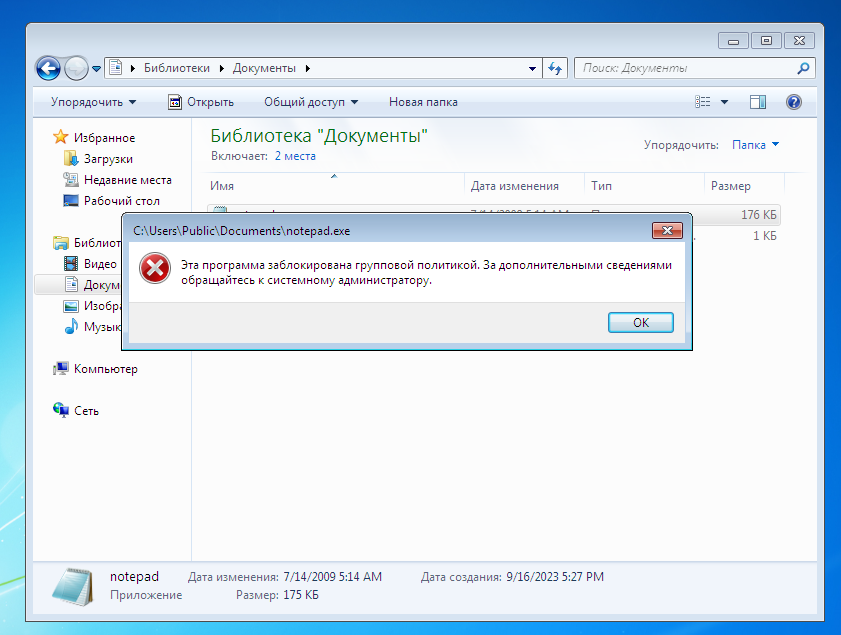


Рисунок 24 Запрет на использование программы calc.exe

# Контрольные вопросы:

1. Какой компонент используется для управления учётными записями пользователей и как получить к нему доступ?

Для управления учетными записями используется компонент «Управление компьютером». Чтобы его открыть выберите Пуск → Настройка → Панель управления. Дважды щелкните значок «Администрирование» затем дважды щелкните значок «Управление компьютером». Второй способ открыть

«Управление компьютером» нажать правой кнопкой на значке «Мой компьютер» и в появившемся контекстном меню выбрать «Управление».

1. Кто может осуществлять управление учётными записями?

Управление учётными записями могут обладать группы пользователей «Администраторы»

1. В чём разница между выходом из системы и сменой пользователя?

При выходе из системы все процессы, запущенные текущим пользователем, будут приостановлены. При смене пользователя, текущая сессия сохраняет своё состояние. При выходе из системы есть риск потери несохранённых данных

1. Как сменить пароль учётной записи?

Выберите учетную запись, которую требуется изменить (например, учетная запись пользователя «User1»).

В контекстном меню выберите пункт «Задать пароль».

В появившемся окне введите новый пароль и сделайте скриншот результата. Войдите в систему от имени пользователя «User1» используя новый пароль. Аналогичным образом задайте пароль учётной записи «User 2».

1. Что такое отключение учётной записи? Чем оно отличается от удаления? Как отключить учётную запись?

При отключении учётной записи все её данные и права хранятся в системе.

Чтобы отключить учётную запись:

* Выберите учетную запись «User1».
* В контекстном меню выберите Свойства.
* Чтобы отключить выбранную учетную запись пользователя, установите флажок «Отключить учетную запись».

Отключение учетной записи также возможно с использованием команды net user с параметрами net user имя пользователя /active:no

1. Для чего предназначены группы пользователей?

Пользователь, принадлежащий группе, имеет все права на разрешения, предоставленные этой Группе. Пользователь, являющийся членом нескольких групп, имеет все права и разрешения, предоставленные каждой из этих групп.

При удалении локальной группы удаляется учетная запись группы. Учетные записи пользователей, являющихся членами удаленной группы, при этом не удаляются.

1. Как добавить пользователя в группу?

Управление группами пользователей (добавление, отображение и изменение локальных групп) также осуществляется с использованием командной строки, по средсвам команды **net localgroup**. Ввод команды **net localgroup** без параметров выводит имя сервера и имена локальных групп компьютера.

Каким требованиям должен отвечать пароль при включении параметра

«Пароль должен отвечать требованиям сложности»?

араметр политики **Пароль должен соответствовать требованиям к сложности** определяет, должны ли пароли соответствовать ряду правил для надежных паролей. Если этот параметр включен, пароли должны удовлетворять следующим требованиям:

Пароли не могут содержать значение samAccountName пользователя (имя учетной записи) или полное значение displayName (полное имя). Ни один из этих проверок не учитывает регистр.

Параметр samAccountName проверяется в полном объеме только для того, чтобы определить, является ли параметр частью пароля. Если параметр samAccountName имеет длину менее трех символов, эта проверка пропускается. Параметр displayName анализируется на наличие разделителей: запятых, точек, тире или дефисов, подчеркиваний, пробелов, знаков фунта и табуляций. Если какой-либо из этих разделителей найден, параметр displayName разделяется, и подтверждается, что все проанализированные разделы (маркеры) не будут включены в пароль. Маркеры короче трех символов игнорируются, а подстроки маркеров не проверяются. Например, имя "Erin M. Hagens" разделяется на три маркера: "Erin", "M" и "Hagens". Так как второй маркер всего один символ в длину, он игнорируется. Таким образом, у этого пользователя не может быть пароля, который включает "erin" или "hagens" в качестве подстроки в любом месте пароля.

1. Пароль содержит символы из трех следующих категорий.
   * Прописные буквы европейских языков (от A до Z, с диакритической меткой, греческим и кириллицем).
   * Строчные буквы европейских языков (от a до z, sharp-s, с диакритических знаков, греческий и кириллица).
   * Базовые 10 цифр (от 0 до 9).
   * Небукенно-цифровые символы (специальные символы).Символы валюты, такие как евро или британский фунт, не учитываются в качестве специальных символов для этого параметра политики.
   * Любой символ Юникода, классифицируемый как цифра или буква, но не в верхнем или нижнем регистре. Эта группа включает символы Юникода из азиатских языков.

Требования к сложности применяются при смене или создании паролей.

1. Что такое пороговое значение блокировки в политике учётных записей?

Пороговое значение блокировки в политике учётных записей определяет количество неудачных попыток входа в систему, после которого учётная запись, под которым пытались зайти в систему, будет заблокирована.

1. Что такое «Политики аудита»?

Политика аудита предписывает заносить в журнал Безопасность те или иные события (удачные и/или неудачные). После указания событий, требующих регистрации, можно указать конкретные объекты, за которыми будет вестись слежение (например, после разрешения аудита доступа к объектам можно в

свойствах папки указать ведение аудита доступа для конкретных пользователей и/или групп).

1. Что такое политики ограниченного использования программ?

С помощью политик ограниченного использования программ имеется возможность защищать компьютерное оборудование от программ неизвестного происхождения путем определения программ, разрешенных для запуска. В данной политике приложения могут быть определены с помощью правила для

«hash», правила для сертификата, правила для пути и правила для зоны Интернета.

1. Какие уровни безопасности могут использоваться в правилах политик ограниченного использования программ?

В ОС Windows предусмотрено три уровня безопасности при реализации Политики ограниченного использования программ:

1. «Запрещено» - программное обеспечение запускаться не будет вне зависимости от прав доступа пользователя;
2. «Обычный пользователь» - разрешает выполнение программ без прав администратора, но позволяет обращаться к ресурсам, доступным обычным пользователям;«Неограниченный» - доступ программ к ресурсам определяется правами пользователя.
3. «Неограниченный» - доступ программ к ресурсам определяется правами пользователя.
4. Чем отличается правило для хеша и правило для пути в политиках ограниченного использования программ?

Правило для хеша применяется к конкретному файлу независимо от его расположения в файловой системе. Правило для пути применяется для конкретного пути к файлу или папке.