**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 ВКБ43 |
| Ковалев Данил Петрович |
| (Фамилия, имя, отчество) |
| Проверил: доцент |
| Скляров Алексей Викторович |
| (Фамилия, имя, отчество) |

## **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.

**Ход выполнения работы:**

**Задание № 2.1.** Открыть окно с данными, где есть параметр “Управление пользователями и группами”.

Для выполнения данного задания нужно, нажать с помощью ПКМ “Этот компьютер”, и выбрать “Управление”. Если нет данного приложения на рабочем столе, то можно в “Поиск приложений, параметров и документов” найти сразу “Управление компьютером”. Должно появиться такое вот окно, как на рисунке 1.

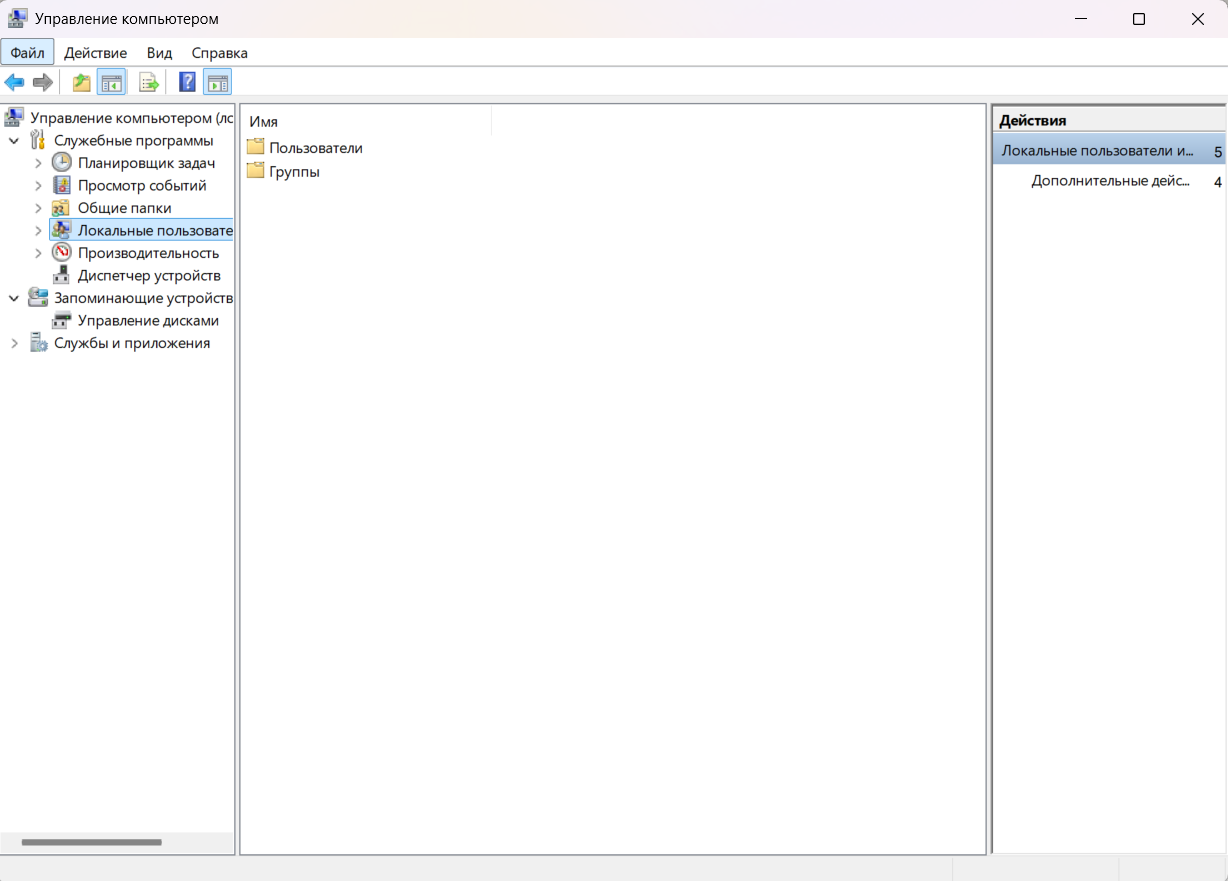


Рисунок 1 – окно “Управление компьютером”

**Задание 2.1.1.** Создать новые учетные записи “user1” и “user2”, используя различные подходы.

В начале рассмотрим, как добавить пользователя через “GUI”. В нашем случае создадим пользователя “user1”. Для этого в приложении “управление компьютером” выбираем пункт “пользователи”, как на рисунке 2.

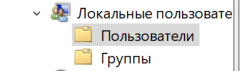


Рисунок 2 – пункт “Пользователи”

Правой кнопкой мыши нажимаем на “Пользователи” и выбираем “Новый пользователь”, как на рисунке 3.

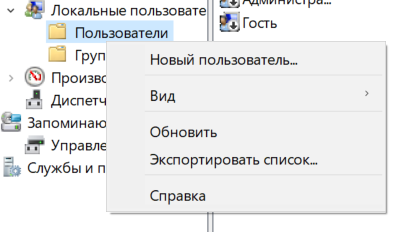


Рисунок 3 – выбор пункта для создания нового пользователя

У нас появится окно, как на рисунке 4, в котором мы можем ввести данные для создания нового пользователя. В моем случае будут использованы следующие данные:

* Пользователь: User1
* Полное имя: User1
* Описание: Пользователь, который создан с помощью GUI
* Пароль: 123
* Подтверждение: 123

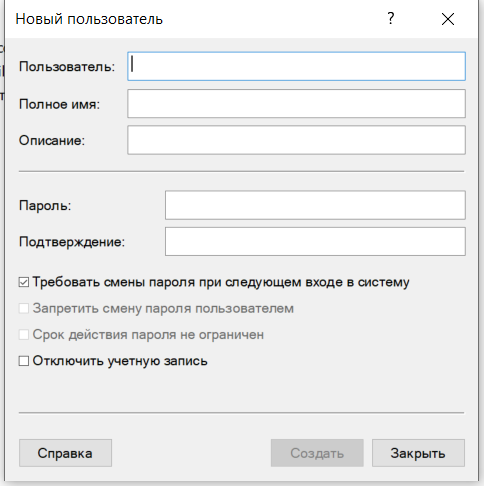


Рисунок 4 – диалоговое окно для создания пользователя

Перейдем теперь к 2 способу создания пользователя, то есть через консоль. Для этого открываем командную строку “CMD” от имени администратора. Через PowerShell данные команды не будут работать.

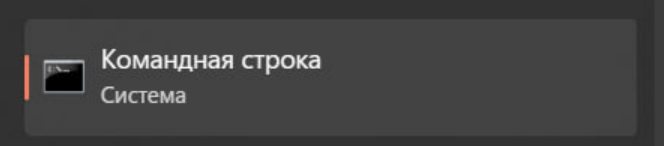


Рисунок 5 – приложение командная строка

Теперь нужно ввести команду для создания пользователя: ‘*net user "User 2" /add*’. Результат представлен на рисунке 6.

Рассмотрим более подробно данную команду и возможные аргументы:

*/add* – этот параметр указывает, что необходимо создать новую учетную запись;

*/times* – Время для входа в систему. Параметр время указывается в формате день[-день][,день[-день]],час [-час][,час [-час]], причем приращение равняется 1 часу. Название дней недели могут указываться полностью или в сокращенном виде. Часы могут указываться в 12- или 24-часовом представлении. Для 12- часового представления используются обозначения am, pm, a.m. или p.m. Значение all соответствует отсутствию ограничений на время входа в систему, а пустое значение обозначает полный запрет на вход в систему. Значения дней недели и времени разделяются запятой; несколько записей для значений дней недели и времени разделяются точкой с запятой;

*/fullname* – этот параметр идентичен полю «Полное имя» при создании пользователя предыдущими способами.

*/active:{yes|no*} - Активирует или деактивирует учетную запись. Если учетная запись не активирована, пользователь не может получить доступ к серверу. По умолчанию учетная запись активирована.

*/delete* - Удаление учетной записи пользователя.

*/expires:{дата|never}* - Дата истечения срока действия учетной записи. Значение never соответствует неограниченному сроку действия. Дата указывается в формате мм/дд/гг или дд/мм/гг в зависимости от кода страны. Месяц может указываться цифрами, полностью или в сокращенном виде (тремя буквами). Год может указываться двумя ли четырьмя цифрами. Элементы даты разделяются слэшем (/) без пробелов.

*/passwordchg:{yes|no}* - Указывает, может ли пользователь изменять свой пароль (по умолчанию может).

Вот ещё один пример команды для создания пользователя: ‘*net user User2 /add /times:monday-friday,9am-6pm /fullname:"New user"*’.



Рисунок 6 – команда для создания User2

Теперь проверим удачно ли были созданы пользователи. Для этого в “Пуск” просмотрим какие пользователи доступны. Результат на рисунке 7.

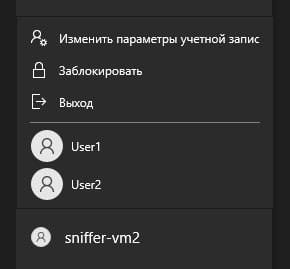


Рисунок 7 – созданные пользователи в системе

Теперь переходим в каждого юзера. Если вы переходите на пользователя сменив его, то пользователь, который был изначальным, остаётся активным. Если же мы переходим на пользователя, предварительно выходя из него, то предыдущий пользователь становится полностью не активным.

Переходим в user1. Windows сразу же предложит установить новый пароль. Ставим новый пароль.

В случае с User 2, Windows не будет предлагать поставить новый пароль, так как мы не добавляли такой параметр в консоли.

**Задание 2.1.2.** Сменить пароли пользователей.

Данное задание буду выполнять, оставаясь за администратора. Переходим в “Управление компьютером”, как было в задании 2.1. Правой кнопкой мыши нажимаем на пользователя, пароль которого хотим изменить. В моём случае я выберу пользователя “User1”. Результат представлен на рисунке 8.

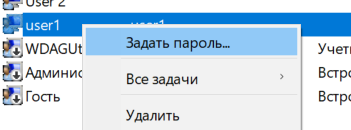


Рисунок 8 – выбор смены пароля для пользователя

У нас откроется диалоговое окно, как на рисунке 9. Здесь вводим новый пароль. В моем случае будет просто пароль – 123.

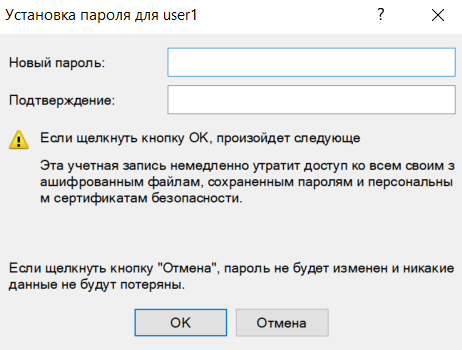


Рисунок 9 – смена пароля для “user1”

Теперь выставим пароль также для пользователя “user2”. В моем случае пароль будет – 123.

**Задание 2.1.3.** Отключение и активизация пользователей.

Для выполнения данного задания в приложении “Управление компьютером” выбираем интересующего нас пользователя. В моем случае будет “User1”. Нажимаем ПКМ, а потом выбираем пункт свойства, как на рисунке 10.

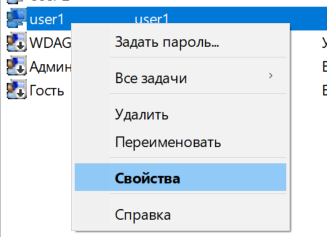


Рисунок 10 – свойства для выбора пользователя

У нас после этого появится окно, которое представлено на рисунке 11.

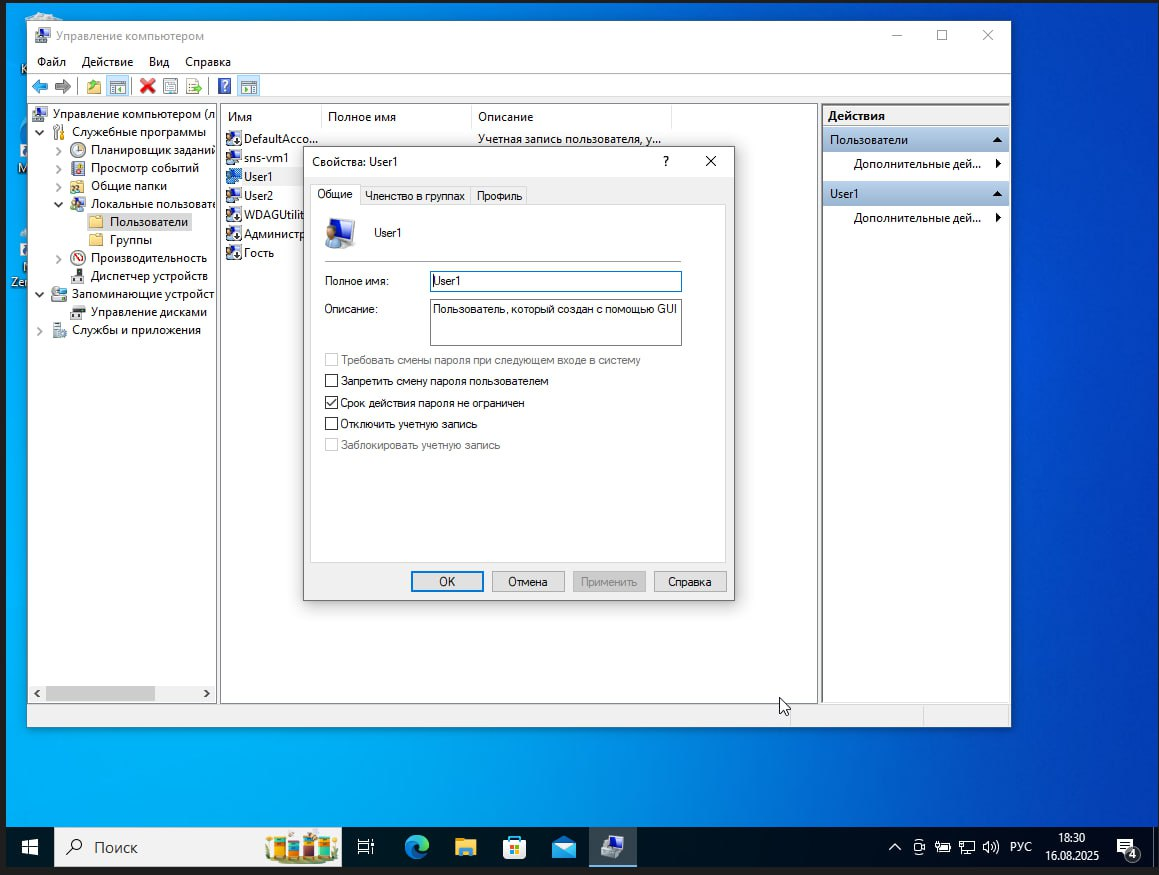


Рисунок 11- свойства для “User1”

Ставим галочку “Отключить учётную запись”. После этого пользователь “User1” должен пропасть из выбора в “Пуск”. Также можно деактивировать пользователя, используя консоль. Для этого нужно выполнить команду: “*net user имя пользователя /active:no*”. Выбор пользователей после блокировки представлен на рисунке 12.

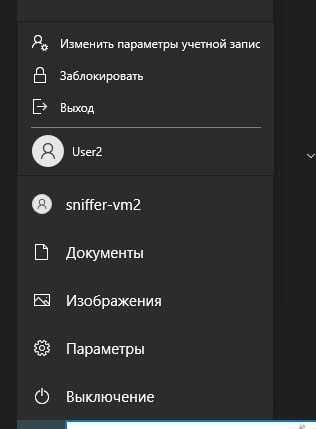


Рисунок 12 – выбор пользователей после блокировки

**Задание 2.1.4.** Удаление учётной записи пользователя.

В моем случае я буду удалять пользователя “User1”. Для выполнения данных действий в приложении “Управление компьютером” нажимаем c помощью ПКМ на “User1” и нажимаем с помощью ЛКМ “Удалить”. Операция представлена на рисунке 13.

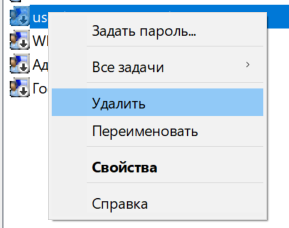


Рисунок 13 – удаление учетной записи пользователя

При удалении пользователя появляется такое предупреждение, которое представлено на рисунке 14. Здесь просто нажимаем на “Да”.

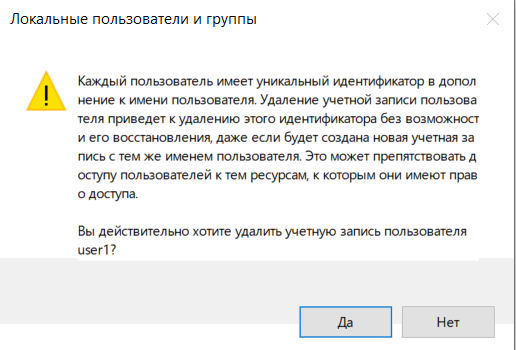


Рисунок 14 – предупреждение на удаление пользователя

Теперь видим, что в списке нет пользователя “User1”, как и ожидалось. Результат представлен на рисунке 15.

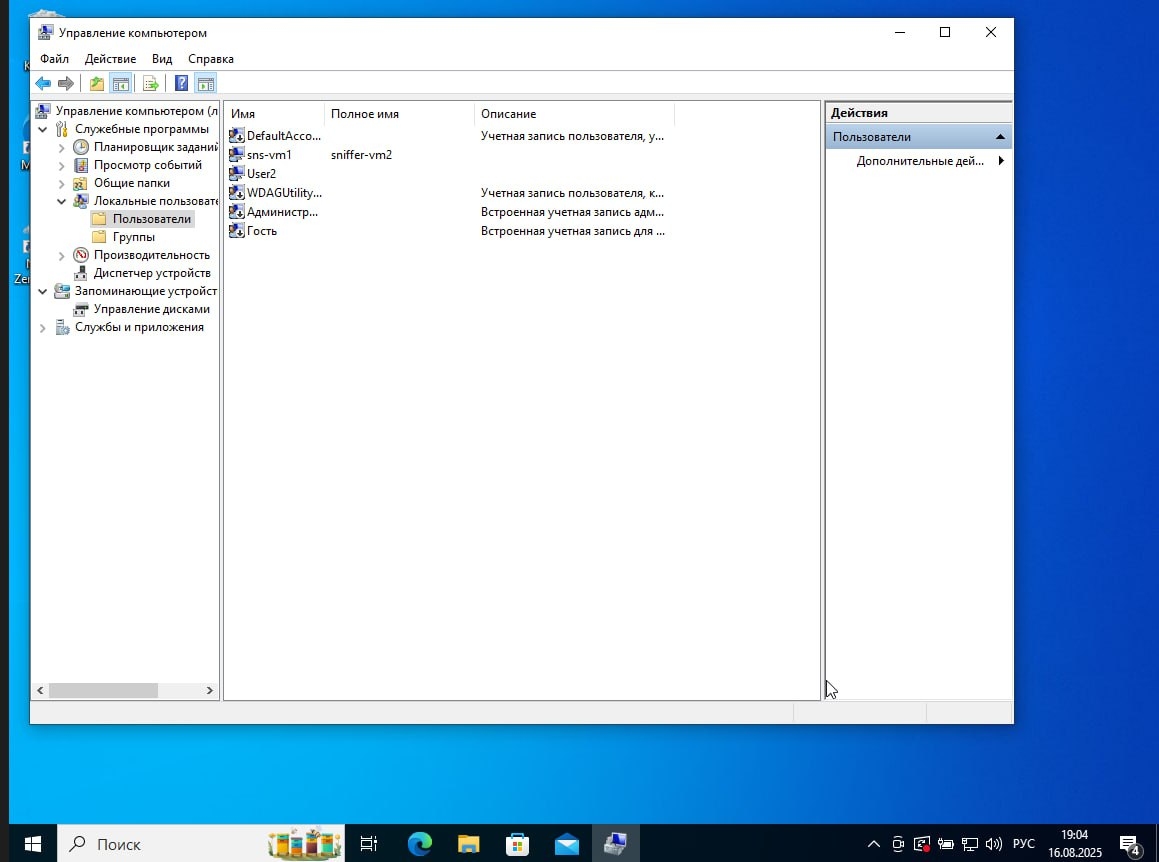


Рисунок 15 – удачное удаление пользователя

**Задание 2.1.5**. Создать группу пользователей.

Перед созданием группы заново создадим пользователя “User1”. Алгоритм создания пользователя был описан уже в прошлых заданиях. Для создания группы есть 2 способа. Через консоль и через GUI.

Рассмотрим в начале способ создания с помощью GUI. Для этого переходим во вкладку группы (Управление компьютером). Нажимаем ПКМ на “Группы” и далее “Создать группу…”. Диалоговое окно для создания новой группы представлено на рисунке 16.

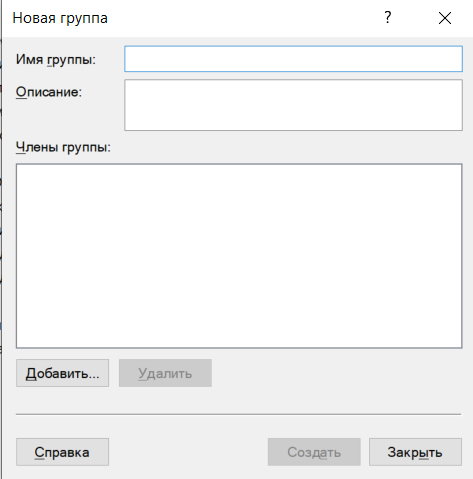


Рисунок 16 – создание новой группы

Рассмотрим теперь как можно создать группу при помощи командной строки. Рассмотрим примеры команд:

1) Вывод списка всех локальных групп на локальном сервере: *net localgroup*;

2) Добавить локальную группу «Group1» в локальную базу учетных записей пользователей: *net localgroup “Group1” /add* ;

3) Добавить учетные записи существующих пользователей «User1», «User2» в группу «Group1»: *net localgroup “Group1” “User1” “User2” /add* ;

4) Вывести список пользователей локальной группы «Group1»: *net localgroup Group1*.

Добавим пользователя “User 1” в группу “Опытные пользователи” при помощи командной строки. Для этого запустите CMD от имени администратора и вставьте команду: *net localgroup “Опытные пользователи” “User1” /add.* Результат выполнения команды представлен на рисунке 17.

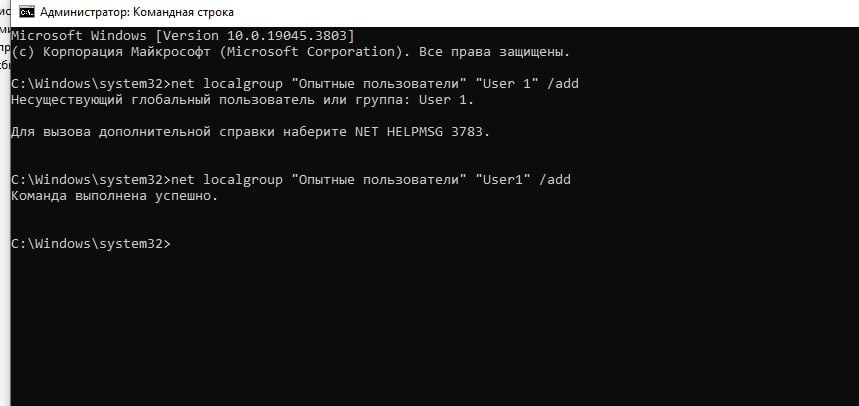


Рисунок 17 – добавление пользователя

Теперь проверим содержимое группы командой: *net localgroup “Опытные пользователи”*. Если всё было сделано правильно, результат должен выглядеть так, как представлено на рисунке 18.

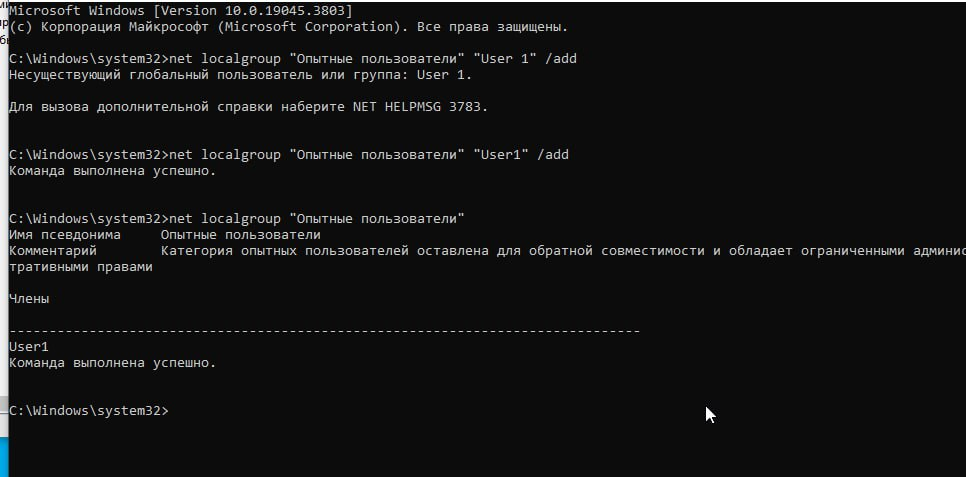


Рисунок 18 – проверка, что User1 находится в группе “Опытные пользователи”

Теперь попробуем 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. Результат представлен на рисунке 19.

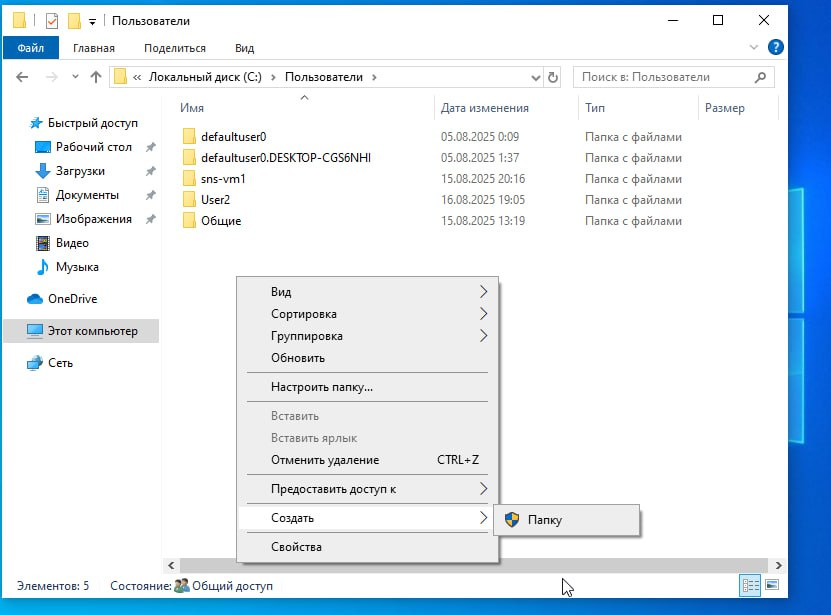


Рисунок 19 – ограничение на создание директории для User1

Теперь добавим User2 в группу “Администраторы”. Кликаем по группе администраторы и нажимаем кнопку добавить в отрывшемся окне. Снизу вписываем имя пользователя, как на рисунке 20.

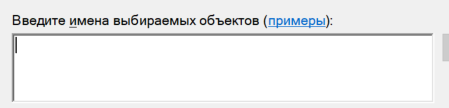


Рисунок 20 – добавление пользователя User2 в группу администраторов

В результате должно выйти то, что представлено на рисунке 21.

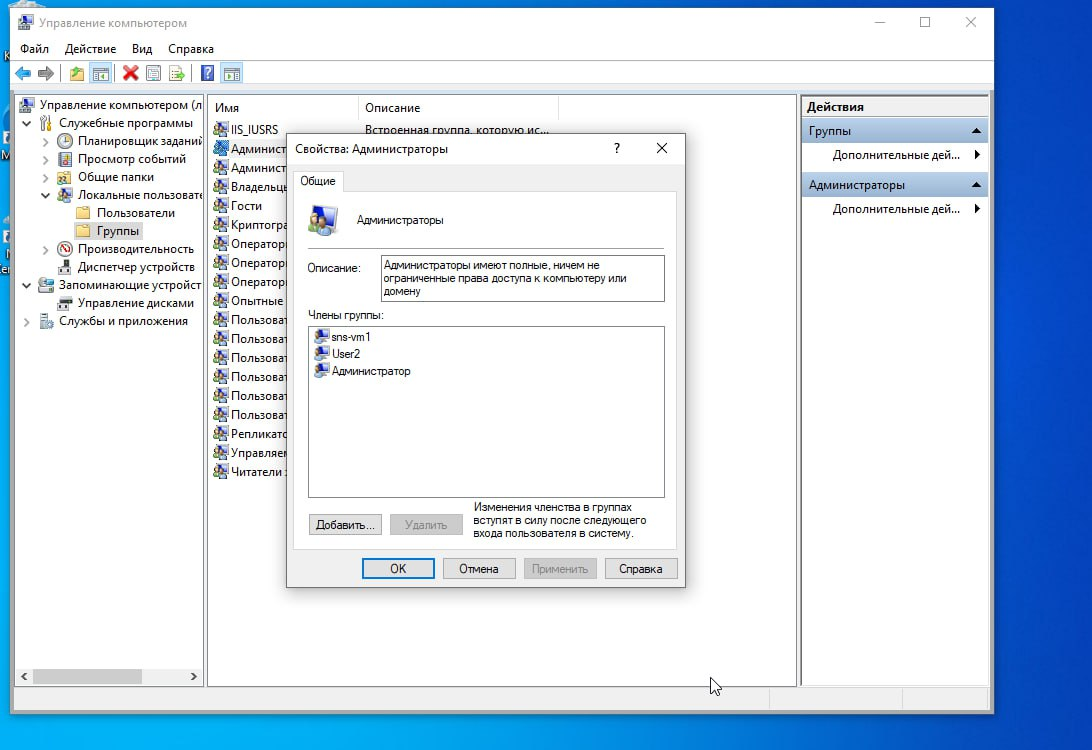


Рисунок 21 – успешное добавление User2 в группу администраторов

Теперь, если снова зайти за пользователя “User2”, должна появится возможность создать файлы (и выполнять другие действия) от имени администратора без ввода пароля. Результат представлен на рисунке 22.

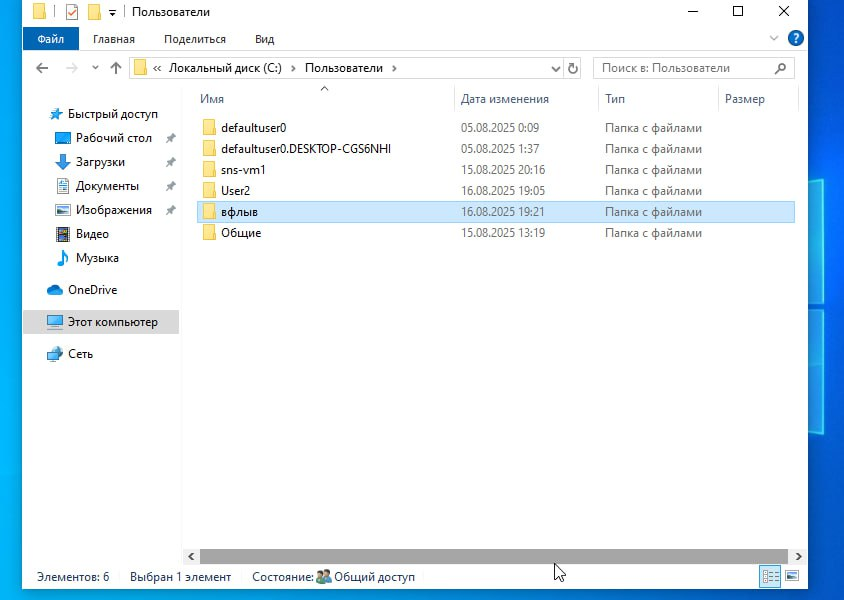


Рисунок 22 – удачное создание директории от имени User2

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

В моем случае бывают баги, что не работает поиск в “Пуск”, поэтому для запуска панели управления можно использовать следующий алгоритм: Win + R; control. В результате выполнения алгоритма из условия должно появиться такое окно, как нар рисунке 23.

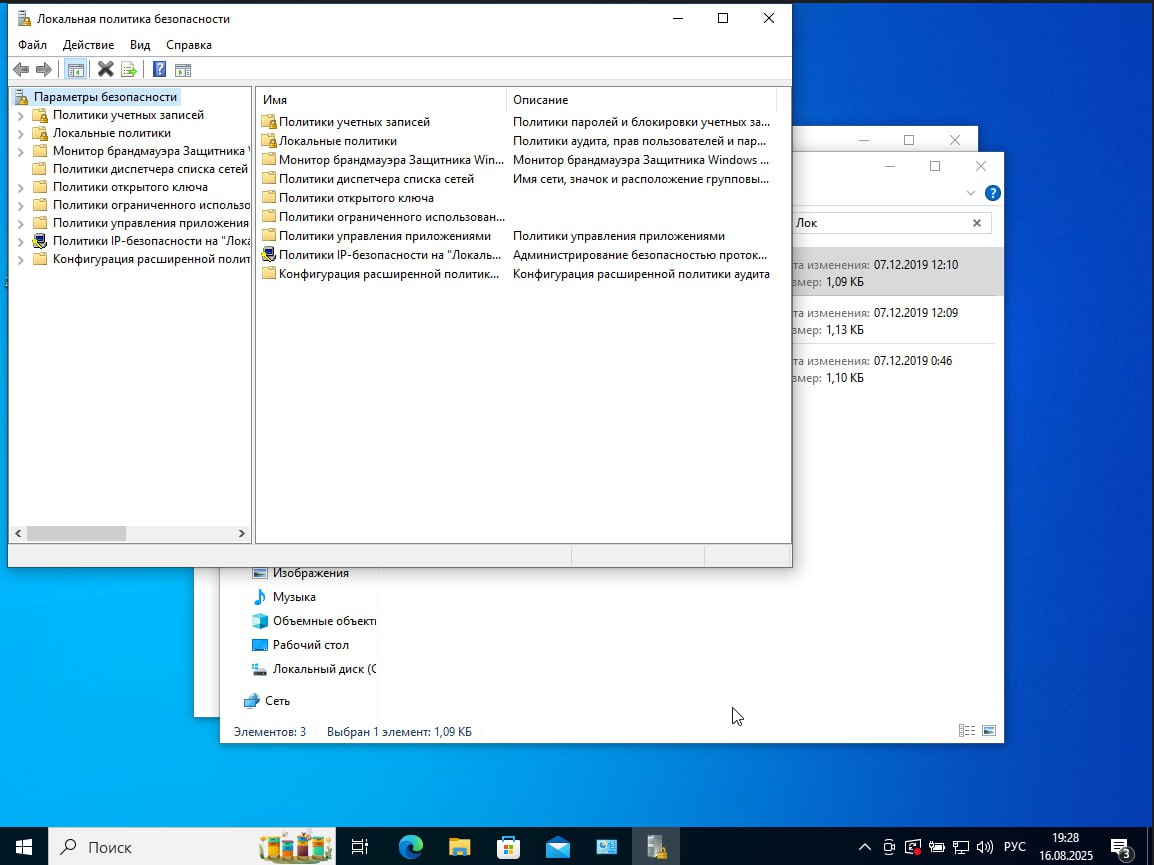


Рисунок 23 – Окно “Локальная политика безопасности”

**Задание 2.2.1.** Установите политику паролей для пользователей.

Для выполнения задания откройте вкладку «Политики учётных записей» → «Политика паролей». Установите минимальную длину пароля — 8 символов. Результат настройки представлен на рисунке 24.

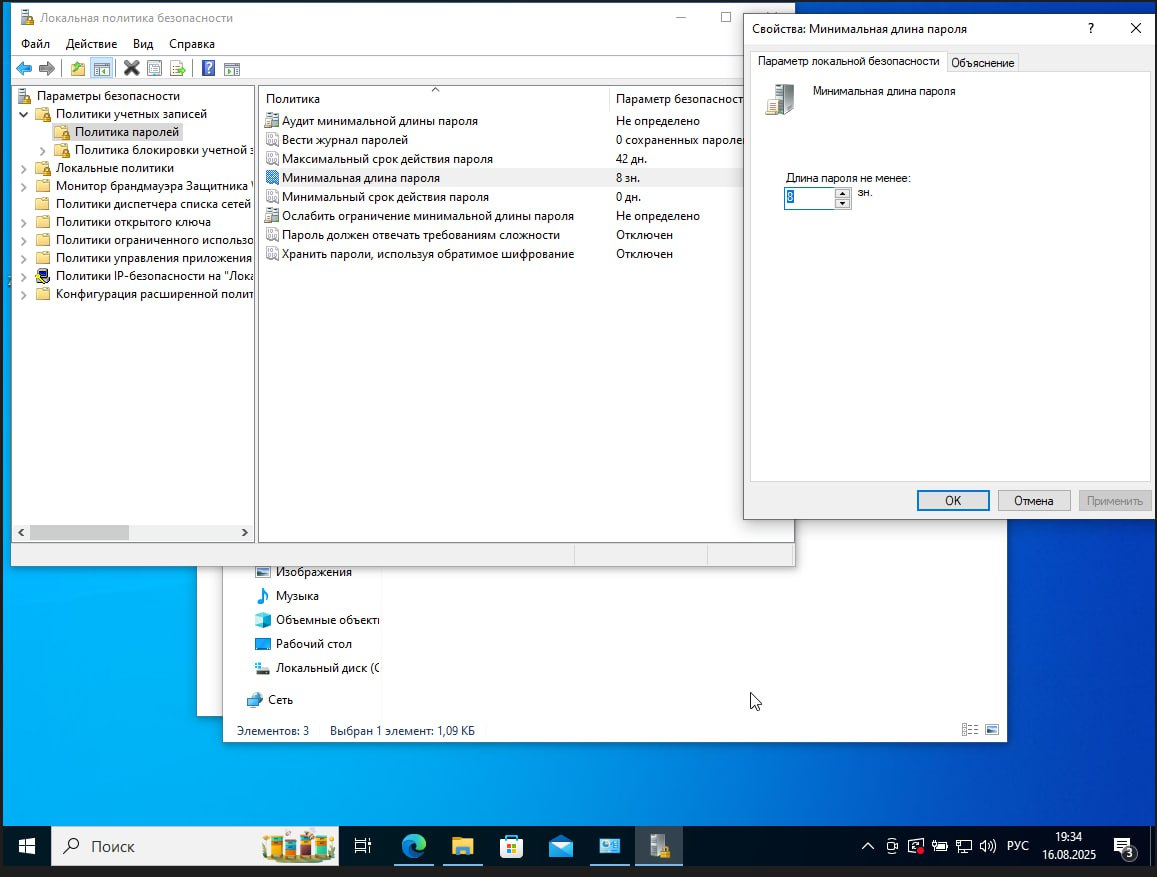


Рисунок 24 – настройка минимальной длины пароля

Теперь сменим пароль для пользователя “User1” и проверим, что он не может задать пароль длиной меньше, чем 8 символов. Результат представлен на рисунке 25.

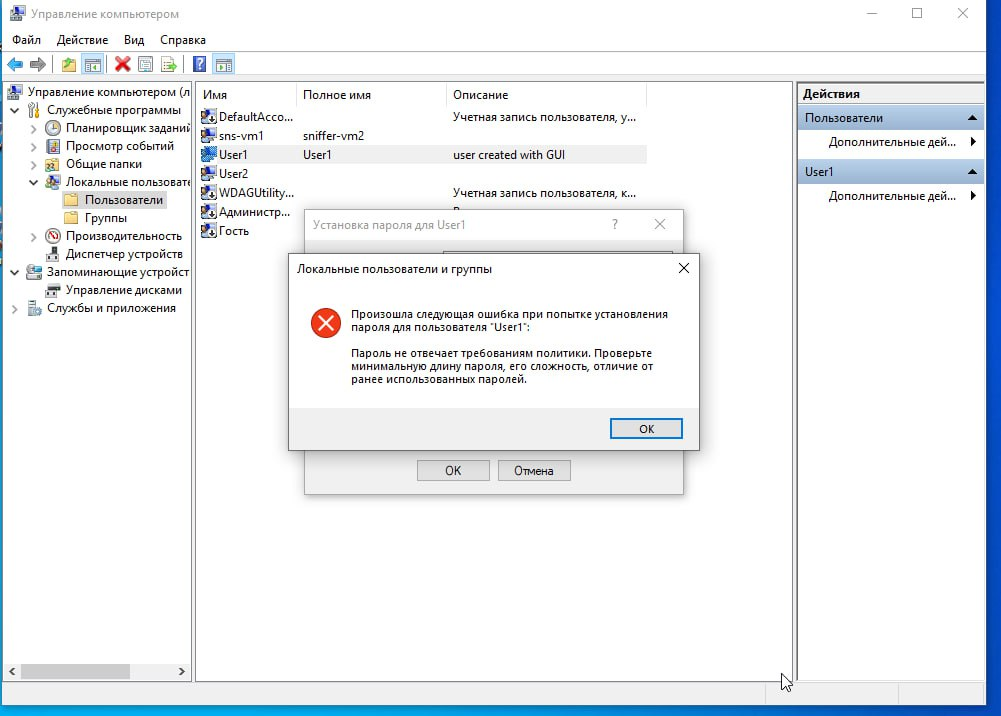


Рисунок 25 – ошибка о том, что пароль слабый

**Задание 2.2.2.** Заблокировать учетную запись.

Переходим во вкладку “Политика блокировка учётной записи” и выбираем “Пороговое значение блокировки”. Ставим значение на 3. Остальные параметры ОС предложит автоматически.

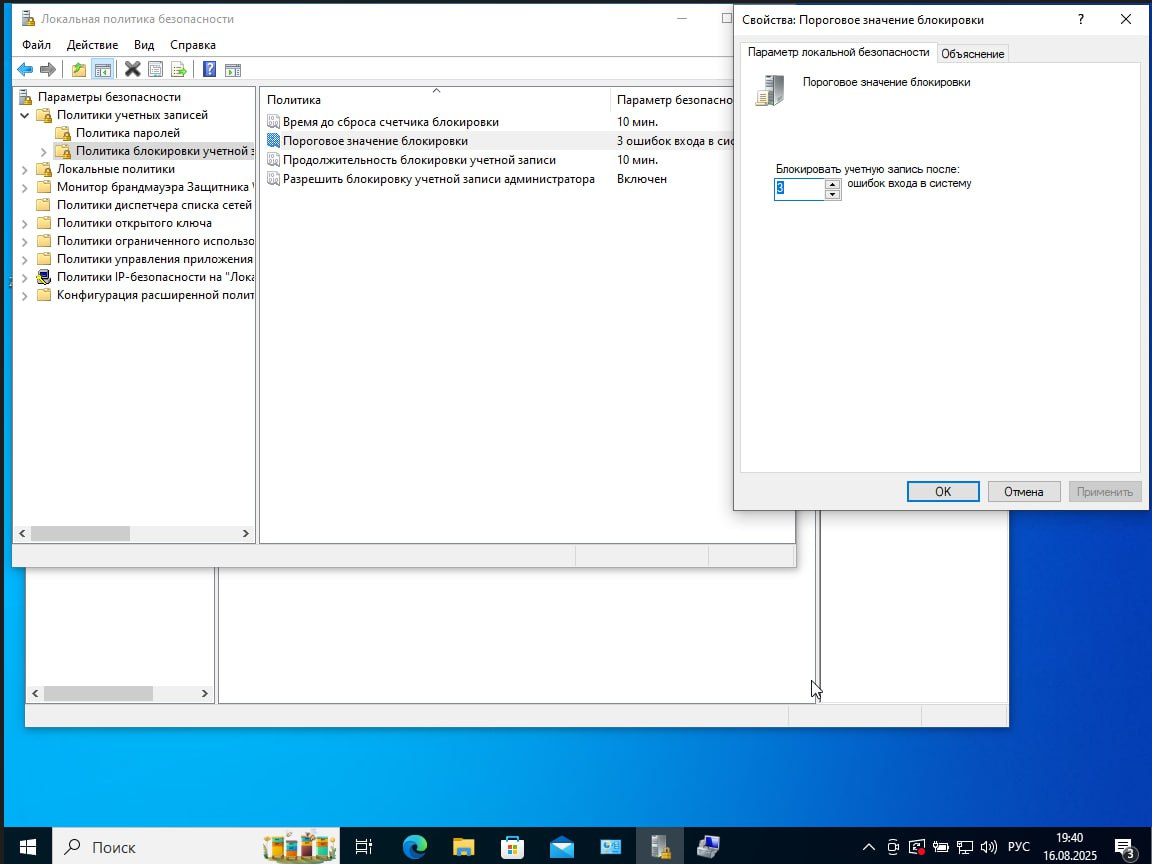


Рисунок 26 – настройка порогового значения блокировки

Если всё было сделано правильно, то при попытке ввода неправильно пароля 3 раза при входе любого юзера, то выведется: “Учётная запись пользователя заблокирована и не может быть использована для входа в сеть”

Данная ошибка пропадёт спустя 10 минут (или же через указанное время в продолжительности блокировки учётной записи).

**Задание 2.2.3**. Настроить аудит.

Переходим во вкладку “Политика блокировка учётной записи” и выбираем “Пороговое значение блокировки”. Ставим значение на 3. Остальные параметры ОС предложит автоматически. Результат настройки представлен на рисунке 27.

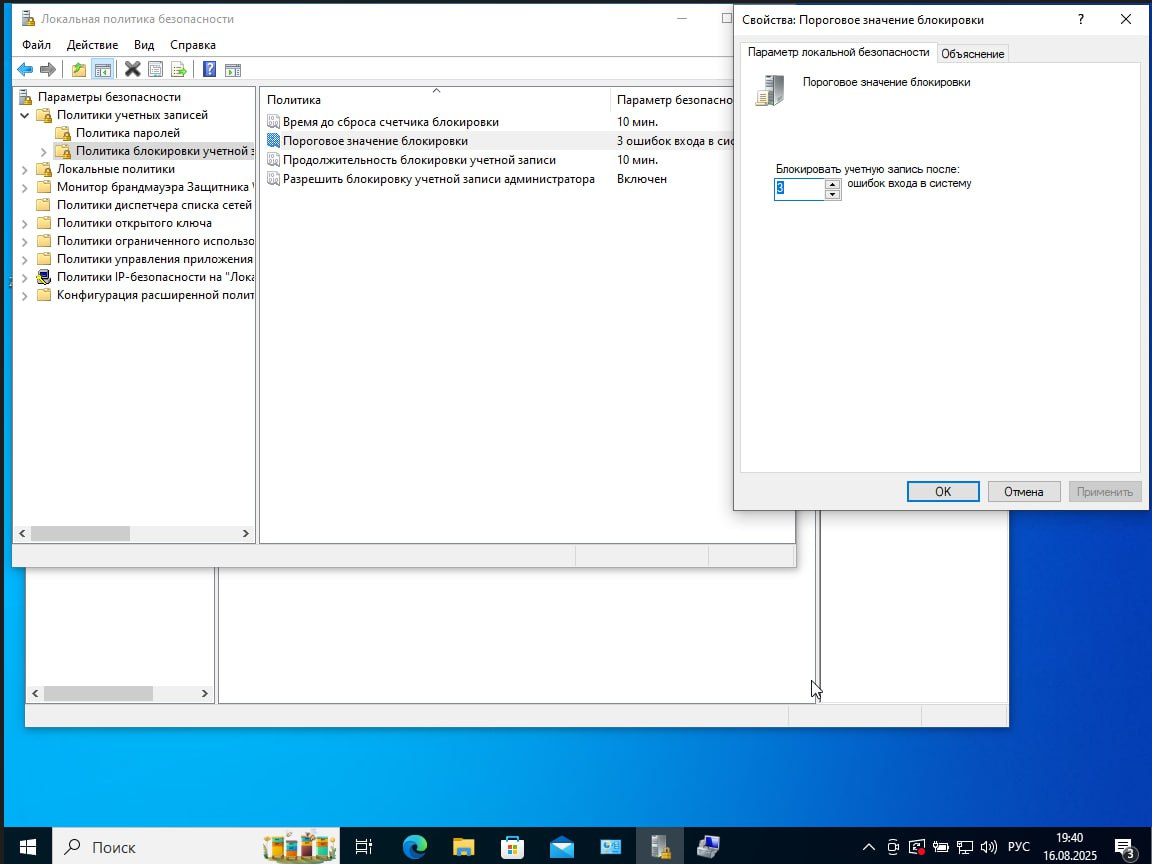


Рисунок 27 – настройка количество попыток входа перед блокировкой

Теперь выставим везде настройки аудита, как сказано в методическом материале. Результат представлен на рисунке 28.

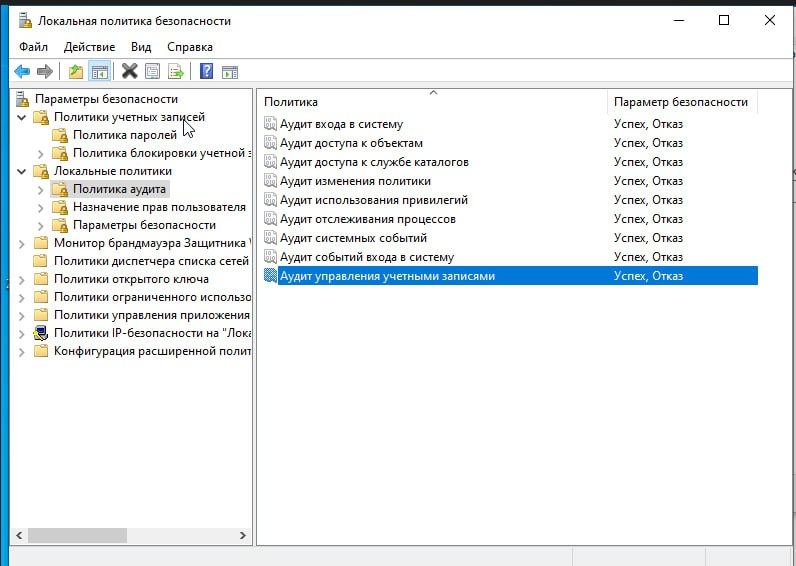


Рисунок 28 – настройка аудита

После переходим в “Управление компьютером” -> “Служебные программы” -> “Просмотр событий” -> “Журналы Windows” -> “Безопасность”

Здесь нужно найти события, в которых находится информация об изменениях политик аудита. Проще использовать комбинацию клавиш CTRL + F и вводим в поиск “Изменение политики”. Если всё было сделано правильно, то данные события будут найдены. Если политики менялись все подряд, то должно быть 8 событий Аудита успеха с разными кодами событий, относящиеся к категории задач “Audit Policy Change”. Результат представлен на рисунке 29.



Рисунок 29 – логи изменения политик

Теперь, нужно проверить работоспособность аудита. Чтобы проверить функции аудита, зайдём в User2 и введём неправильно пароль 3 раза, чтобы выполнить блокировку пользователя, а затем отследим данное событие в аудите. Блокировка пользователя представлена на рисунке 30.

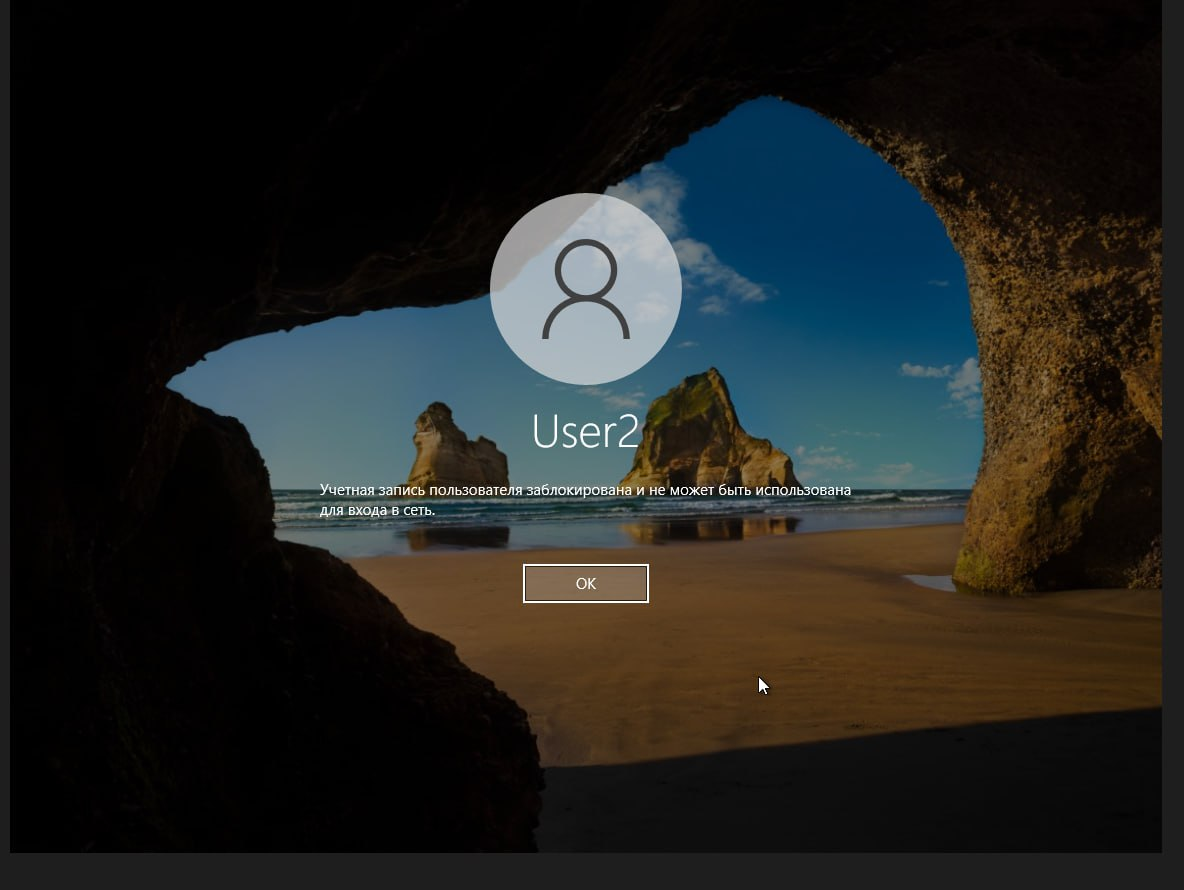


Рисунок 30 – блокировка пользователя User2

Теперь перейдем обр