

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №4**

**ПО ДИСЦИПЛИНЕ«МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ И ИНФОРМАЦИОННЫМИ ПОТОКАМИ В КМПЬЮТЕРНЫХ СИСТЕМАХ»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

**1 Опишите параметры локальной политики безопасности операционной системы (по выбору): – кто имеет доступ к компьютеру; – какие ресурсы могут использовать пользователи на компьютере; – включение и выключение записи действий пользователей или группы пользователей в журнале событий.**

-Кто имеет доступ к компьютеру

Субъекты, имеющие доступ к компьютеру, определяются несколькими локальными политиками безопасности.

Локальный вход в систему- список пользователей, которые могут входить в систему.

Разрешение удаленного подключения- список пользователей, которые могут входить в систему через службы удаленных рабочих столов

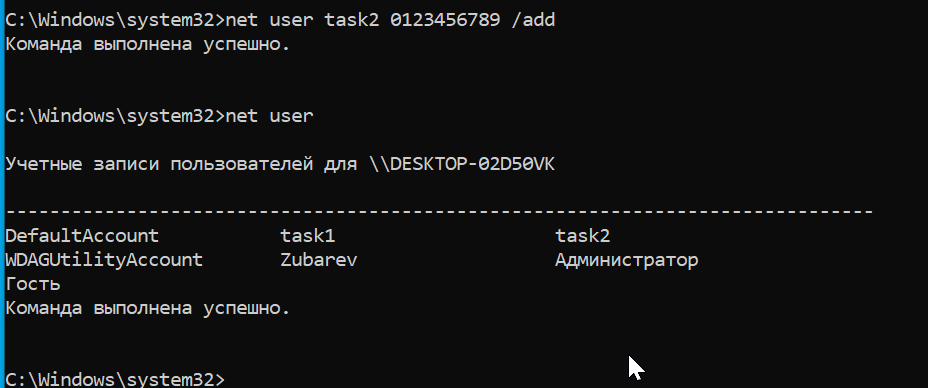
Параметры безопасности – в этом разделе

**2 Создайте новую учетную запись пользователя с помощью командной строки.**

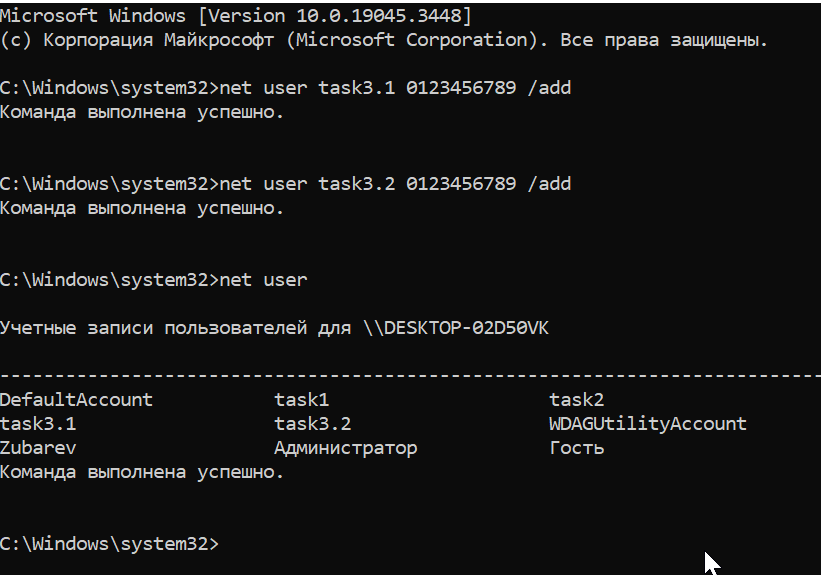
Для создания учетной записи через командную строку необходимо открыть последнюю от имени администратора и вписать команду

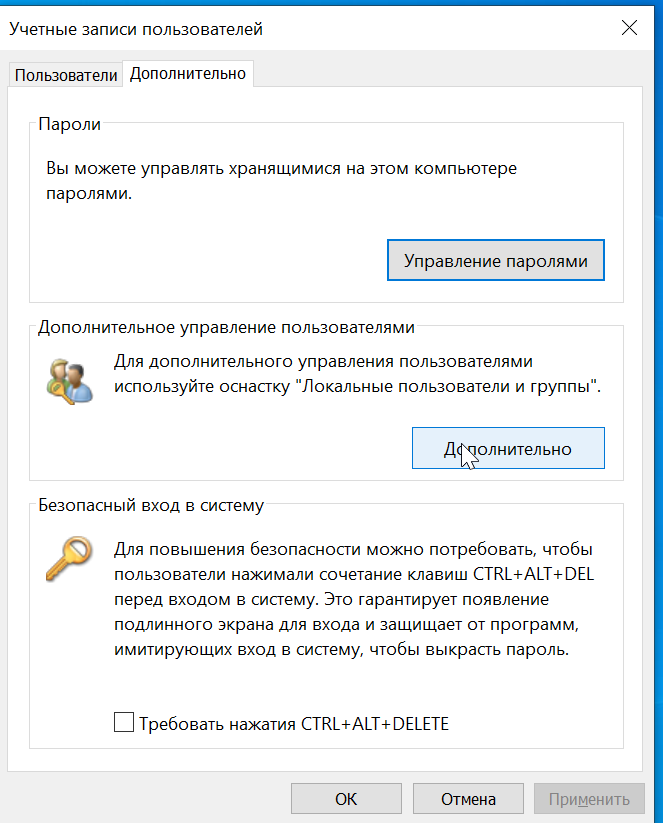
net user username password /add

Где username – имя учетной записи, а password – пароль.



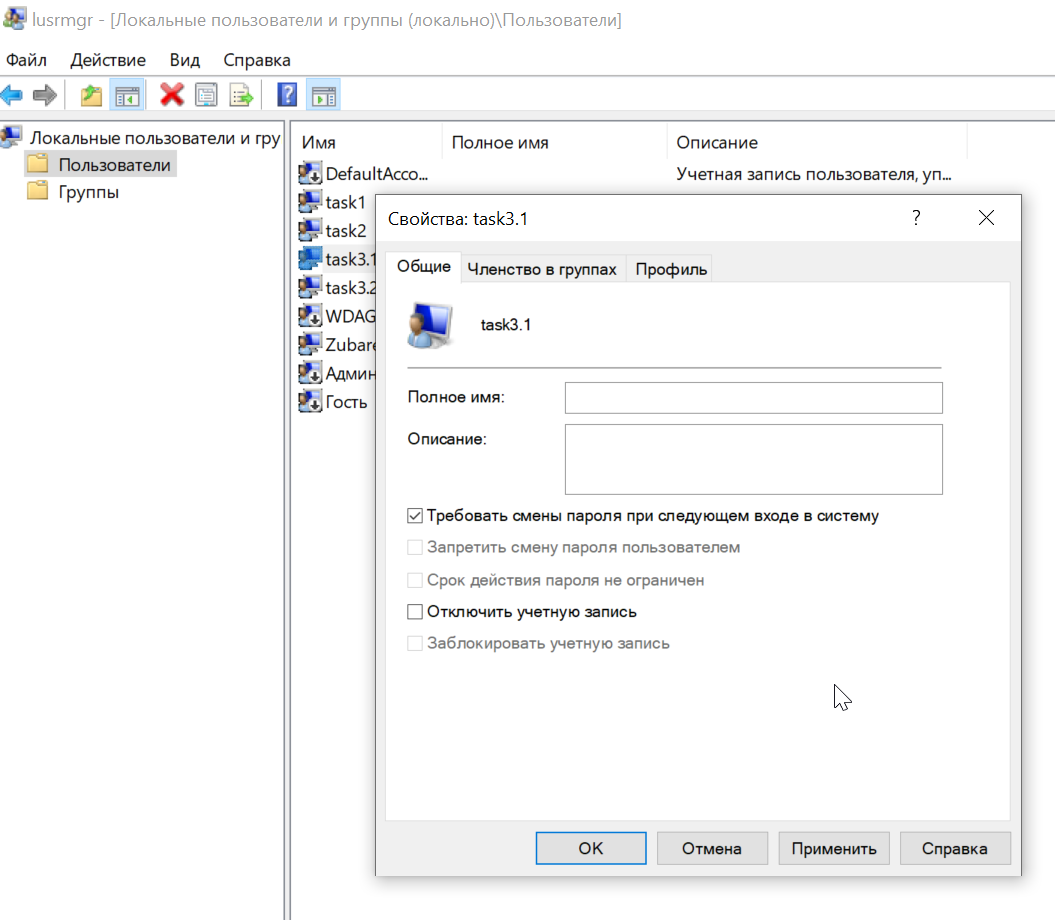
**3 Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем.**

Создание пользователей. 

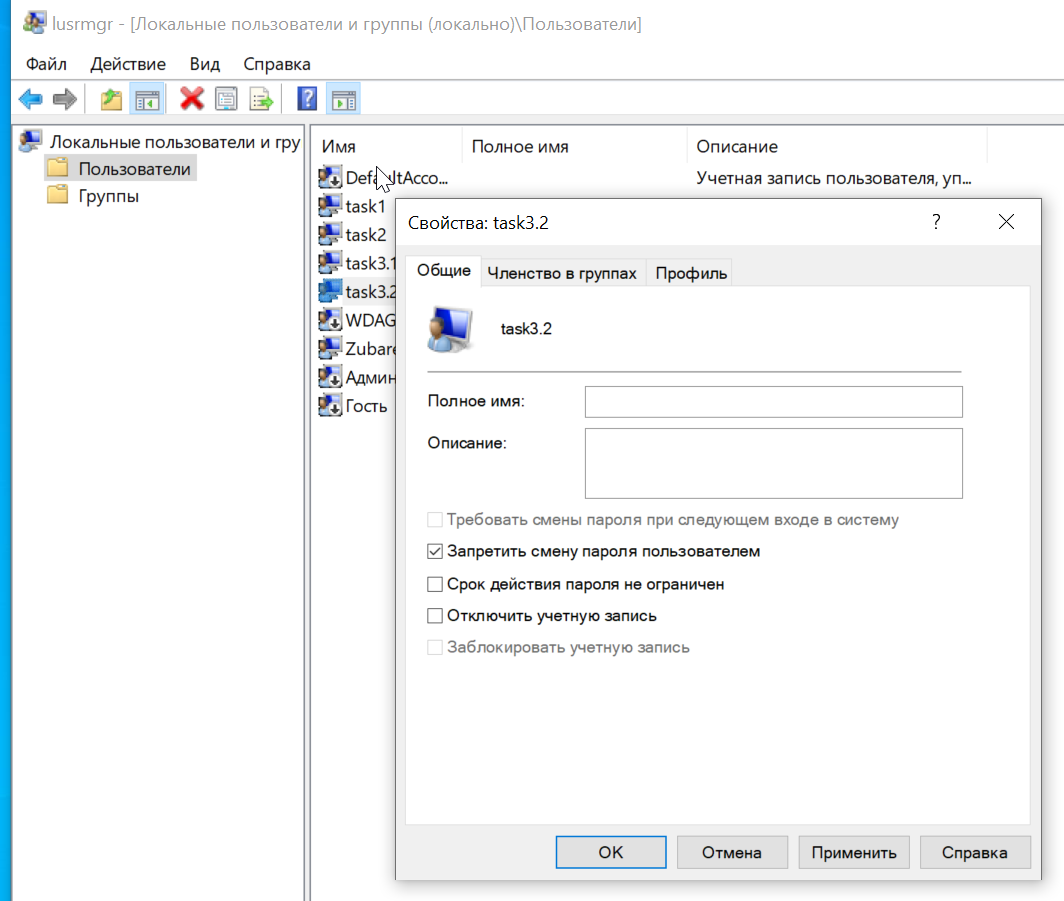
Для включения принудительной смены пароля при следующем входе необходимо открыть утилиту «netplwiz», в открывшемся окне перейти во вкладку «Дополнительно», в пункте «Дополнительное управление пользователями» также нажать «Дополнительно». 

В открывшемся окне перейти на вкладку «Пользователи», и выбрав нужную учетную записть дважды кликнуть по ней правйо кнопкой мыши. В окрывшемся диалоговм окне установить нужные флаги для учетной записи.

Смена пароля при слудующем входе(учетная запись task3.1)

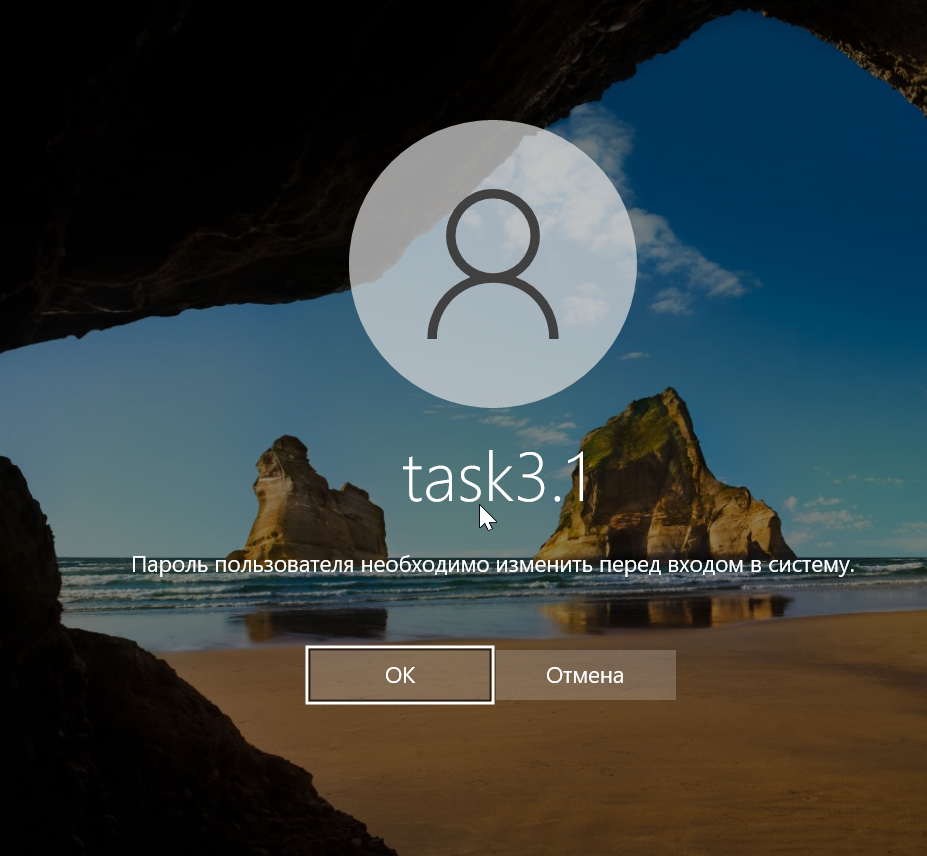


Запрет пользователю изменять пароль (учетная запись task3.2)

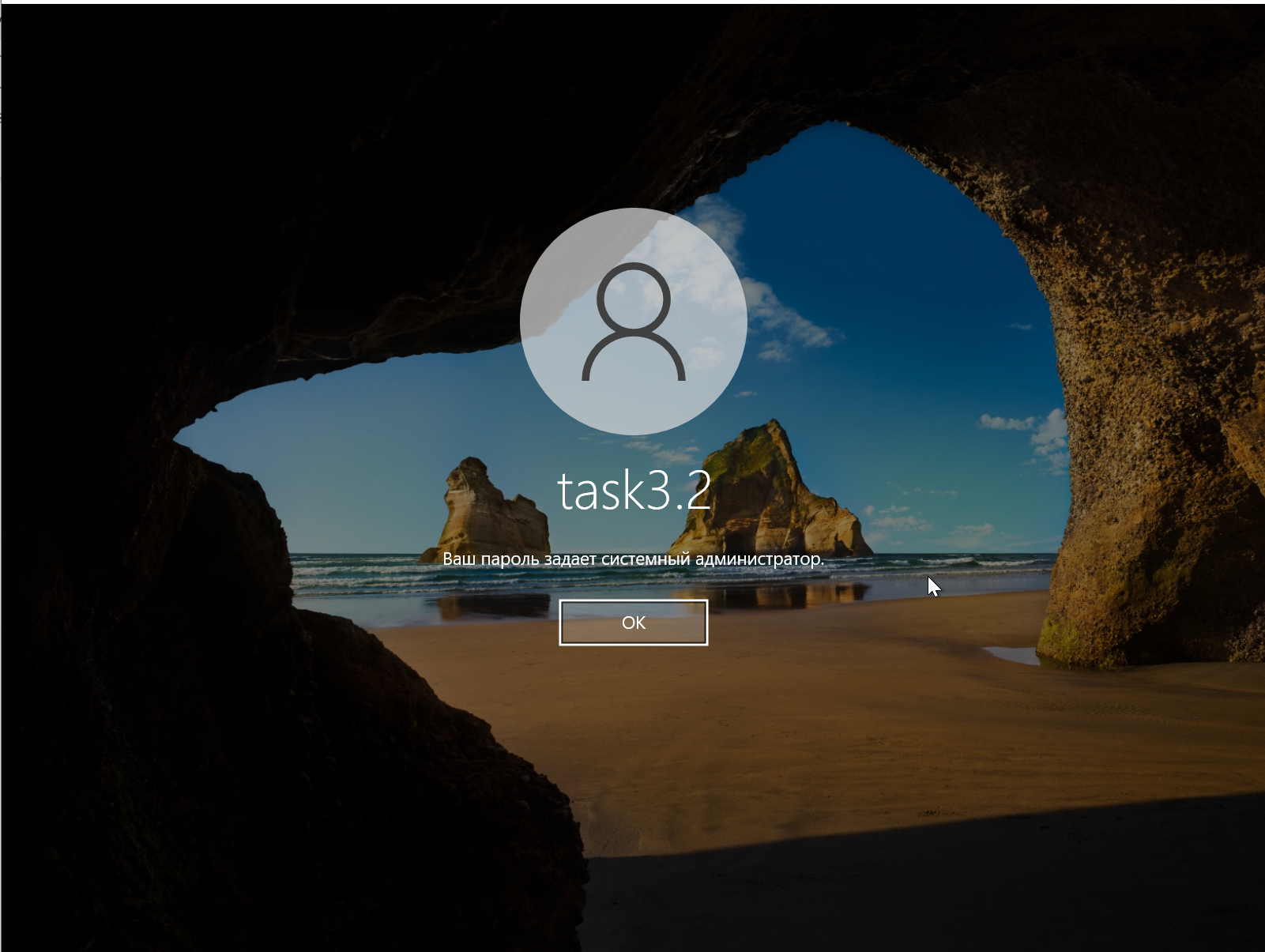


Для проверки высавленных ограничений необходимо сменить пользователяи и попытаться выполнить/не выполнить е действия на котопые наложены ограничения.

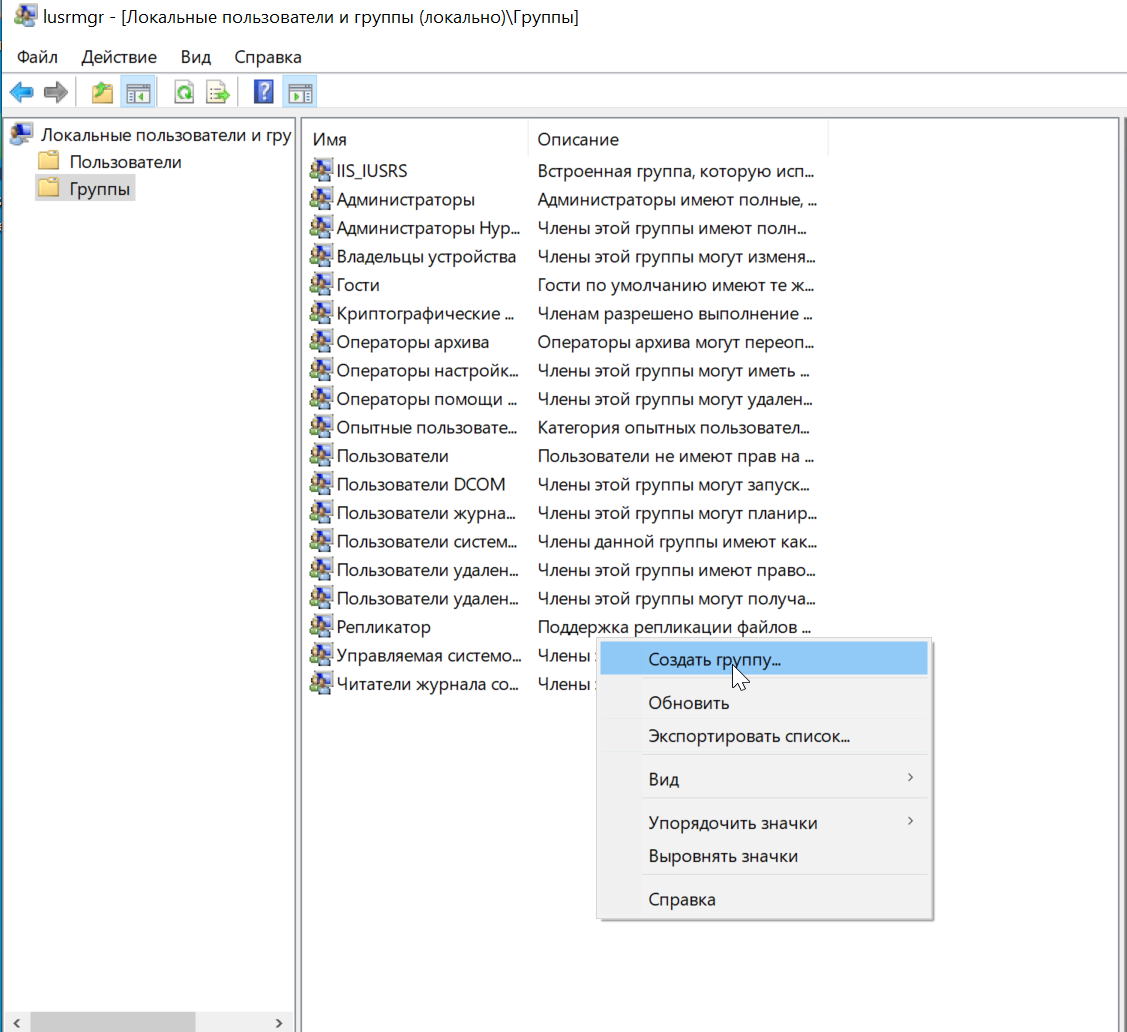
Задание 3.1(смена при входе)

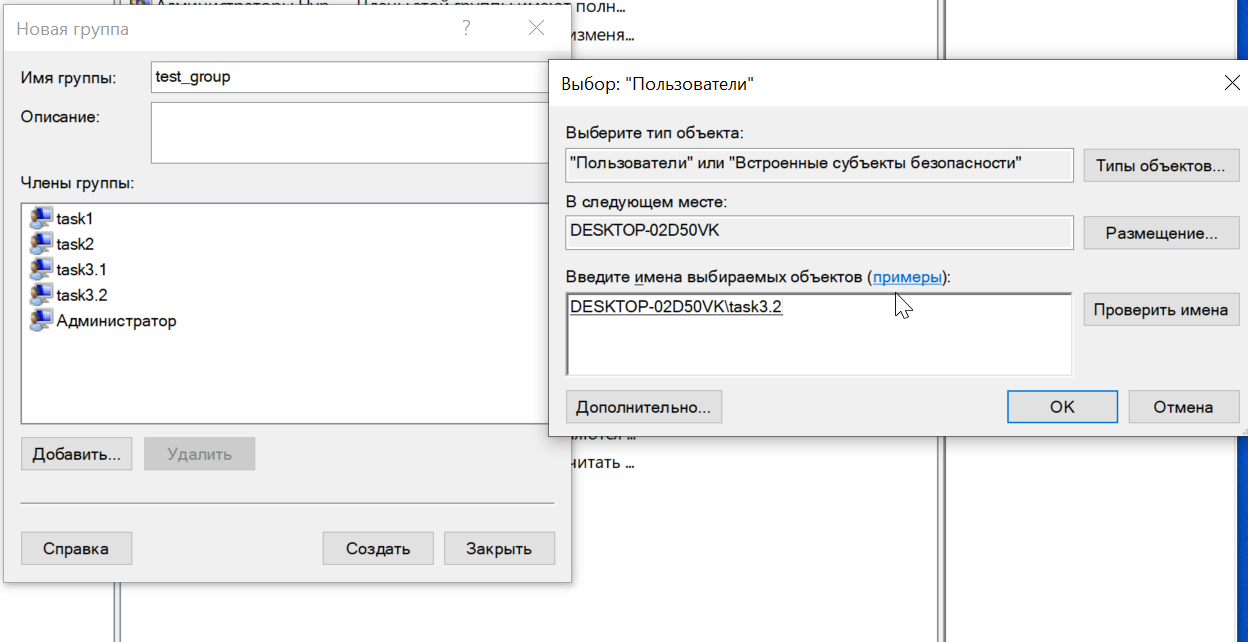


Задание 3.2(отсутвие смены пароля)

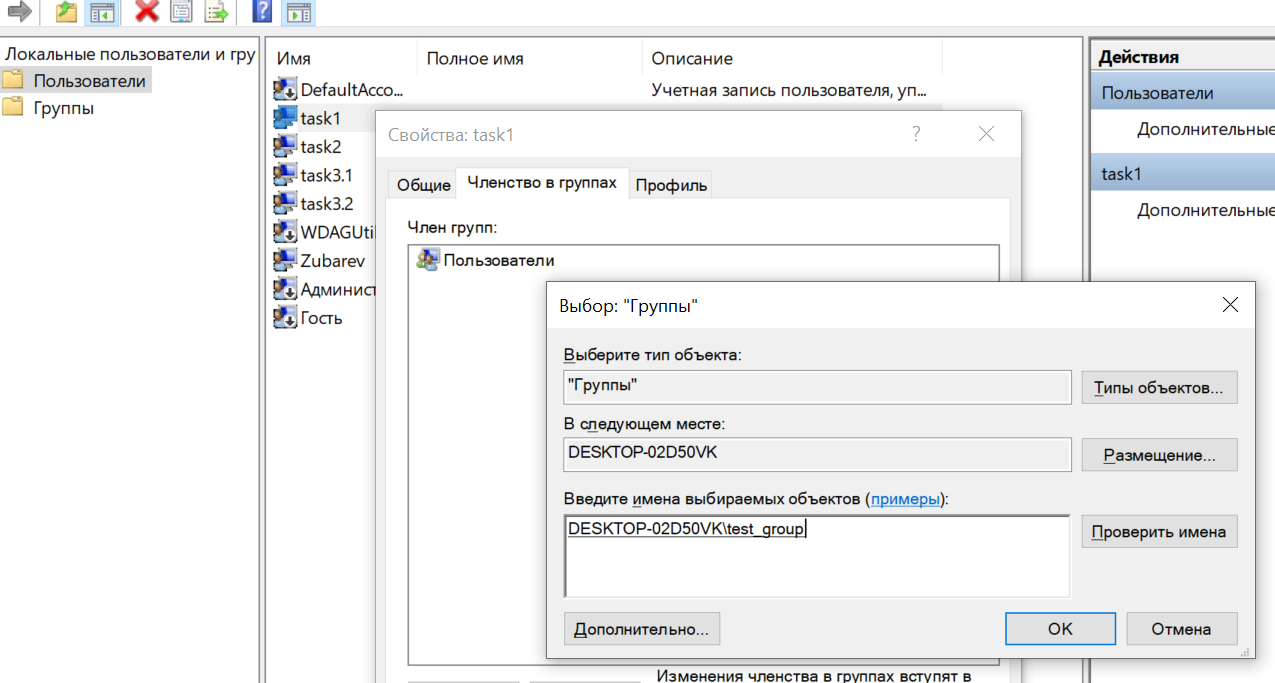


**4 Создайте локальную группу. Поместите в локальную группу созданных вами пользователей и административного пользователя. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя.**

Для создания группы надо нажать сочетание клавиш win+r, и в строке ввода написать «lusrmgr.msc». В открывшемся окне надо перейти во вкладку «Группы», нажать ЛКМ в пустом месте а окне и выбрать «Создать группу». 

В появившемся окне надо ввести имя группы, описание(опционально) и добавить участников(опционално). Добавление происходит через отдельное диалоговое окно, где нужно ввести имя учетной записи для добавления. 

Для выполнения такихже действия через окно свойтв пользователей, необходимо выбрать в этом же окне перейти из вкладки «Группы» во вкладку «Пользователи», выбрать нужного пользователя, нажать на него два разал ПКМ и в открывшемся окне перейти во кладку «Членство в группах», нажать добавить и ввсети имя группы. Сделать аналогичные действия для всех пользователей, которые должны состоять в определенной группе.



По варианту задания пароль должен состоять из минимум L=10 символов. Пароль может быть состоять из латинских и русских букв, а также спецсимволов. Алфавит N=139 символов (33 кириллица прописные\заглавные, 26 латиница прописные\заглавные 21 спецсимвол). Так как пароль может не соответствовать требованиям безопасности, символы могут повторяться. Тогда возможное число комбинаций = 13910.

При мощности 3.1 тфлопс, время подбора пароля T**≈**10052 года.