

федеральное государственное автономное образовательное учреждение  
высшего образования  
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**ОТЧЕТ**

по лабораторной работе №1

«Учетные записи и авторизация в ОС MS Windows»

по дисциплине «**Информационная безопасность**»

Вариант 12

Автор: Кулаков Н. В.

Факультет: ПИиКТ

Группа: Р34312

Преподаватель: Маркина Т. А.



**УНИВЕРСИТЕТ ИТМО**

Санкт-Петербург 2023

## Содержание

1. Цель работы.....	4
2. Программные и аппаратные средства.....	4
3. Выполнение.....	5
3.1. Основная часть.....	5
3.1.1. Основные определения.....	5
3.1.2. Создание пользователя.....	6
3.1.2.1. Создание через Settings.....	6
3.1.2.2. Создание через control userpasswords2.....	8
3.1.2.3. Создание через групповые политики.....	10
3.1.2.4. Создание через консоль.....	11
3.1.2.5. Возможности пользователя.....	12
3.1.3. Создание администратора.....	16
3.1.3.1. Создание через Settings.....	17
3.1.3.2. Создание через control userpasswords2.....	18
3.1.3.3. Создание через групповые политики.....	18
3.1.3.4. Создание через консоль.....	19
3.1.3.5. Ограничения администратора.....	19
3.1.4. Параметры контроля учетных записей пользователей.....	21
3.1.5. Настройка механизмов защиты.....	23
3.2. Дополнительная часть.....	23

3.2.1. Windows Server. Создание и копирование профиля.....	23
3.2.2. Смарт-карты.....	24
3.2.3. Отличия биометрической службы Windows 10.....	24
4. Выводы.....	24

# 1. Цель работы

Изучить типы учетных записей пользователей, ознакомиться с основными принципами управления учетными записями. Изучить основные способы авторизации пользователей.

# 2. Программные и аппаратные средства

Hw-probe: [https://linux-hardware.org/?probe=cff5d02cde\](https://linux-hardware.org/?probe=cff5d02cde)

Вендор и модель ноутбука: HUAWEI NBLK-WAX9X 2019

Основные аппаратные средства:

- Ryzen 5 3500U with Radeon Vega Mobile Gfx
- 2x RAM HMA851S6CJR6N-VK 4GB Row Of Chips DDR4 2667MT/s
- NVMe SSD Controller SM981/PM981/PM983 512GB
- RTL8822CE 802.11ac PCIe Wireless Network Adapter

Основные программные средства:

- ОС GNU/Linux Gentoo 2.14
- Ядро 6.1.53-gentoo-r1-x86\_64

Программа эмуляции:

- libvirt (libvirt) 9.4.0 + QEMU emulator version 8.0.3 (virt-manager)
- Гипервизор KVM
- UEFI

Виртуальные машины:

- Windows 10 Enterprise N LTSC 21H2 19044.1288

- MEM 4096 МБ
- 4 vCPU
- SATA 40 ГБ
- Драйвера виртуальной машины: virtio-win

## **3. Выполнение**

### **3.1. Основная часть**

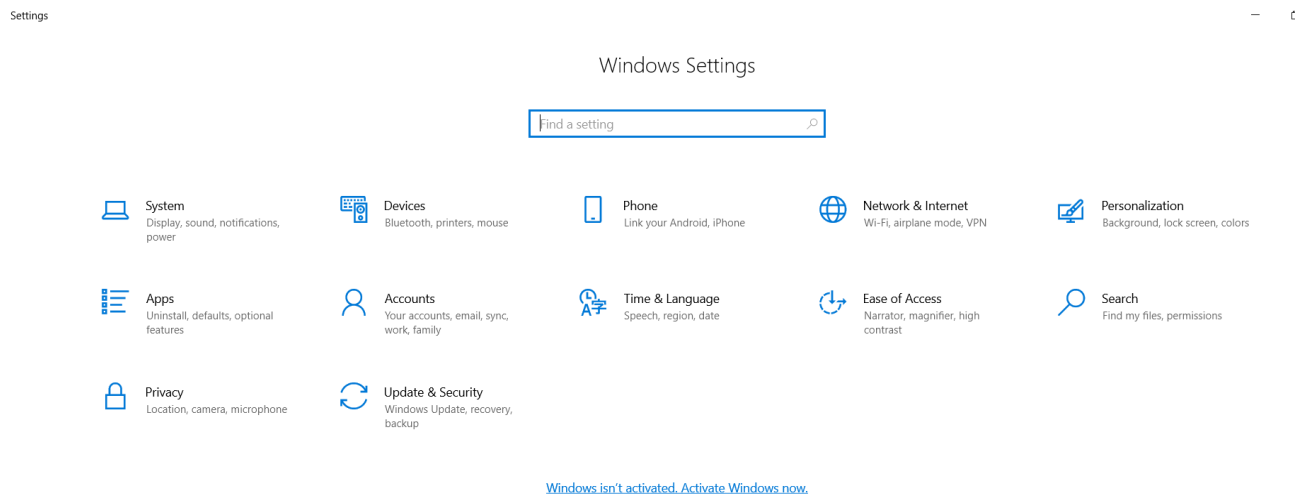
#### **3.1.1. Основные определения**

- Диспетчер учетных записей (SAM - Security Account Manager)
- Монитор безопасности (SRM - Security Reference Monitor)
- Маркер доступа (access token)
- Идентификатор безопасности (SID - Security Identifier)
- Привилегии пользователя
- Права пользователя (user rights)
- Права пользователя
- Объект доступа
- Субъект доступа
- Олицетворение (impersonation)
- Список контроля доступа (ACL - Access Control List)
- Учетная запись
- Домен

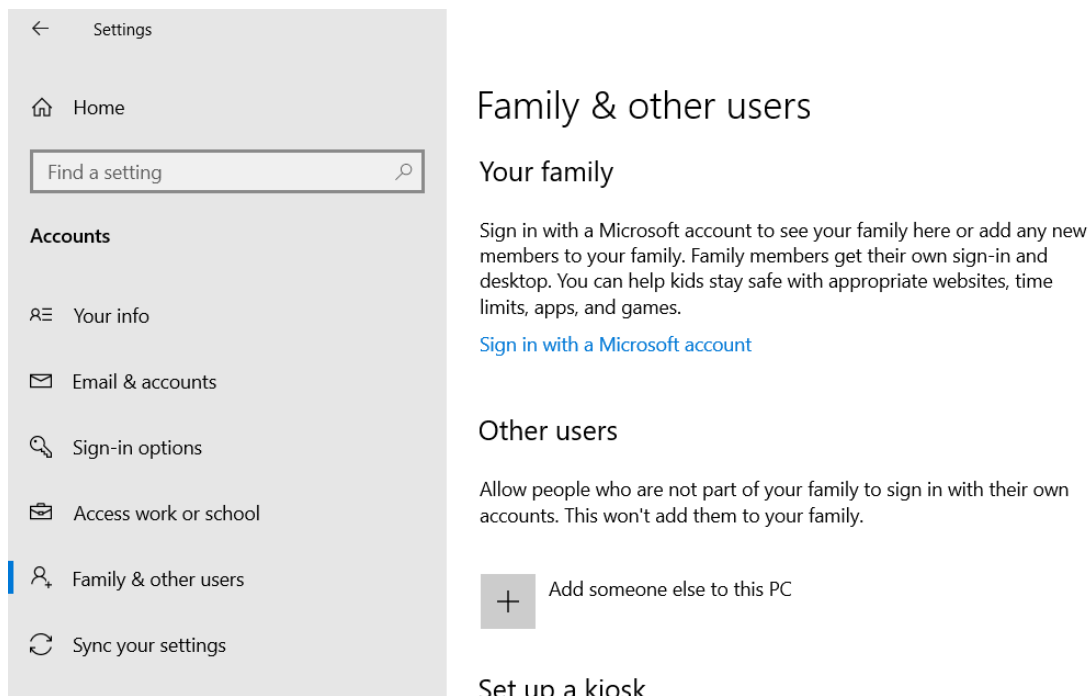
### 3.1.2. Создание пользователя

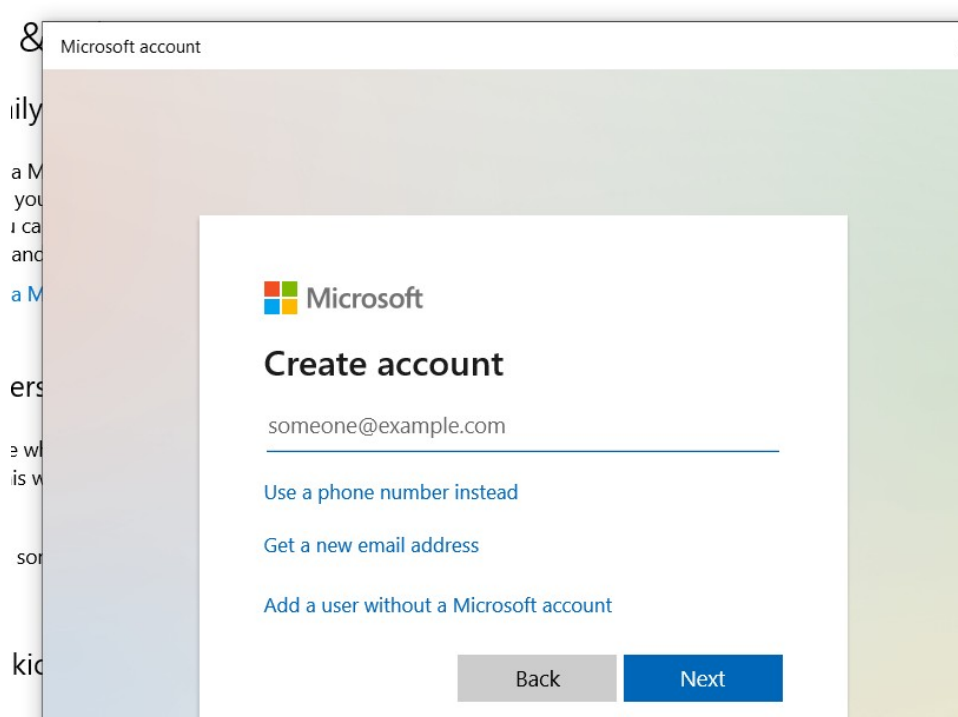
Создайте пользователя *User\_№ варианта*, входящего в группу «Пользователи». Опишите все способы создания, а также (на примерах) возможности данного пользователя по изменению конфигурации системы (минимум 3 примера).

#### 3.1.2.1. Создание через Settings



Переходим в панель Accounts → Family & other users.





Нажимаем создать без учетной записи.

but hard for others to guess.

Who's going to use this PC?

User\_12

Make it secure.

••••••

••••••

In case you forget your password

What was your first pet's name? ▾

a

What's the name of the city where you were born? ▾

a

What was your childhood nickname? ▾

## Family & other users


### Your family


Sign in with a Microsoft account to see your family members to your family. Family members get their own desktop. You can help kids stay safe with app limits, apps, and games.

[Sign in with a Microsoft account](#)

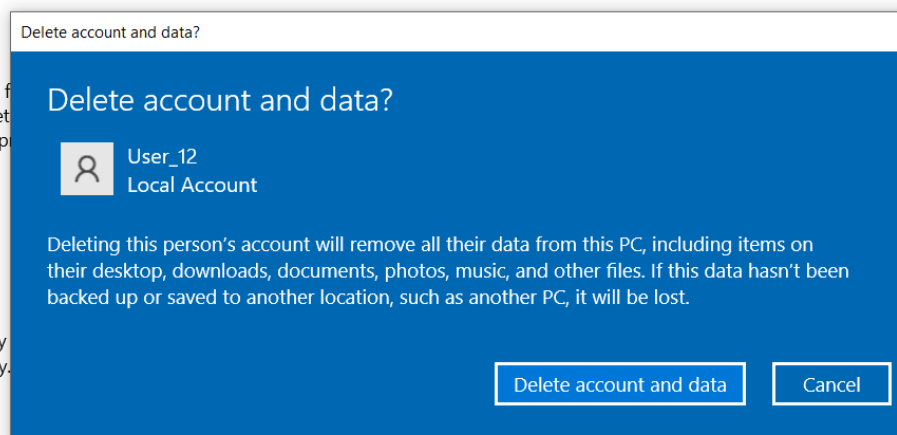
### Other users

Allow people who are not part of your family to use accounts. This won't add them to your family.

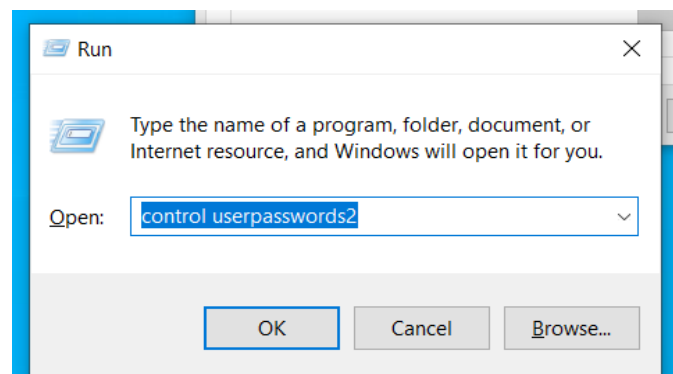
 Add someone else to this PC

 User\_12  
Local account

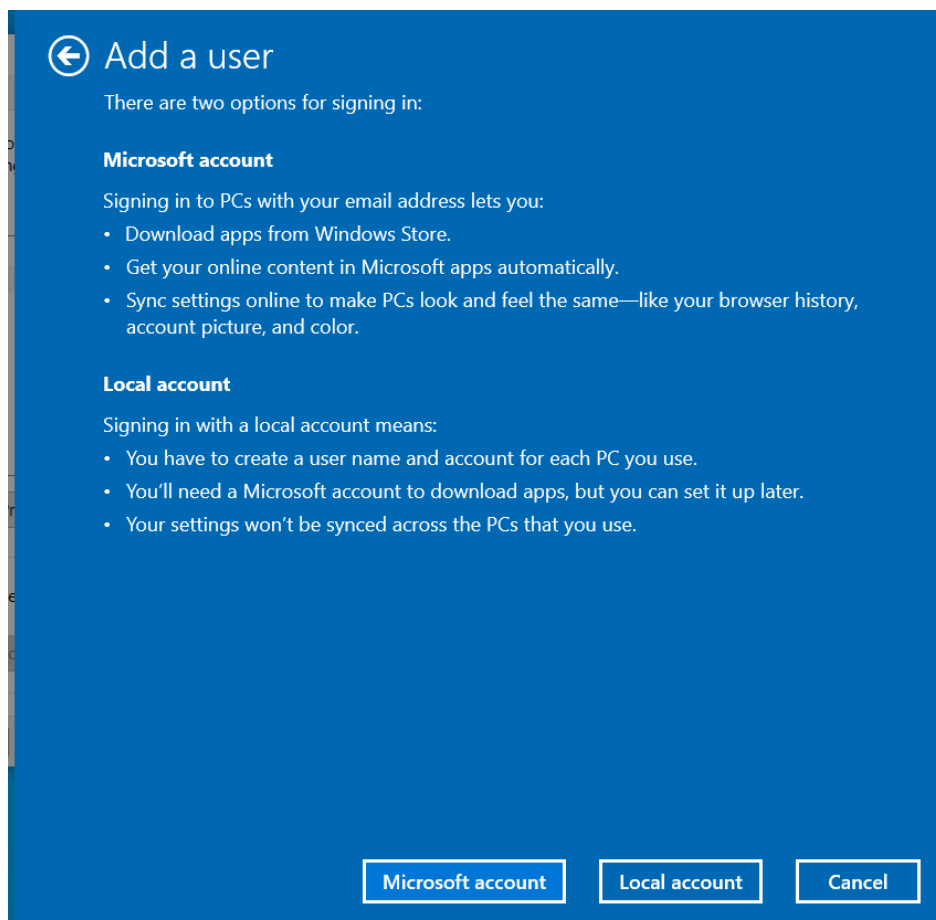
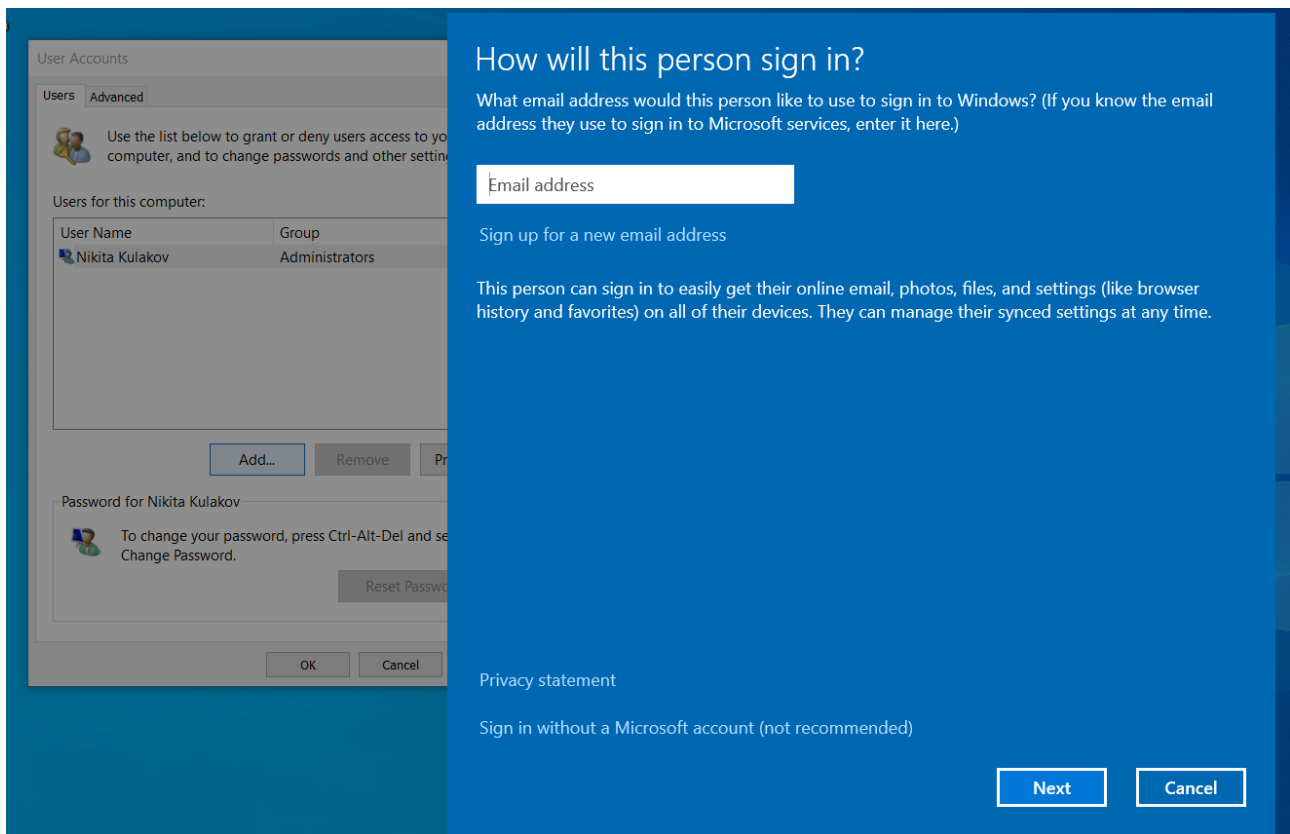
Change account typeRemove

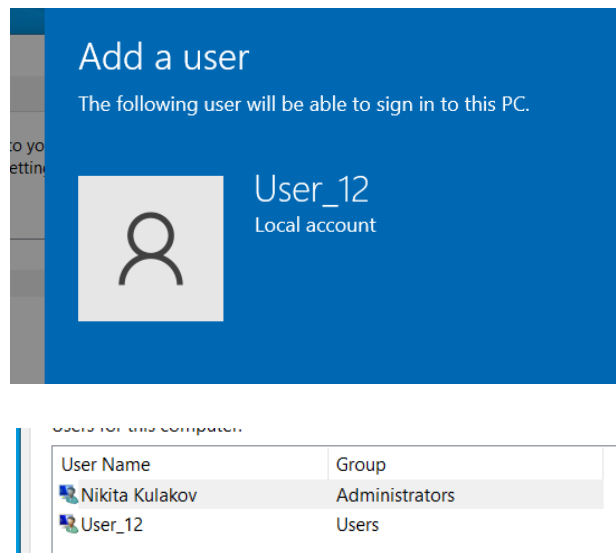


### 3.1.2.2. Создание через control userpasswords2

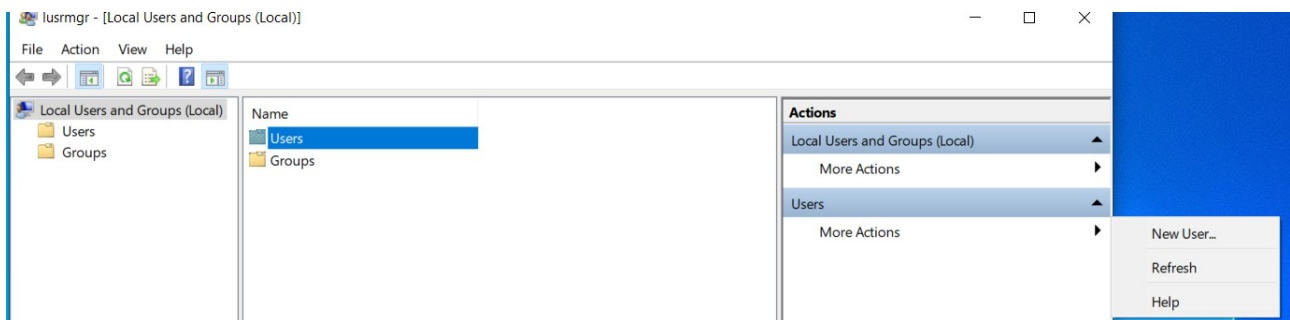
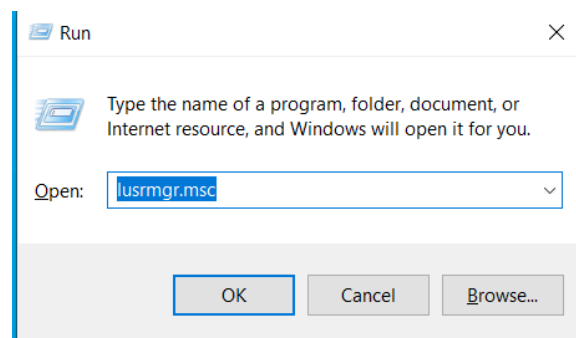




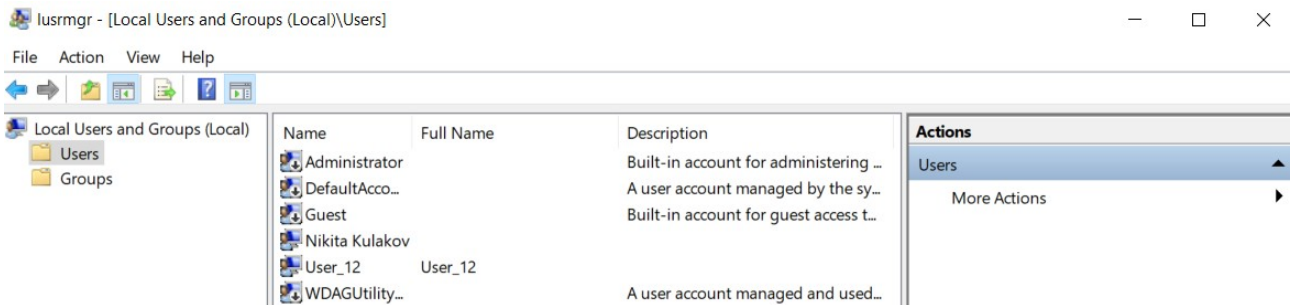
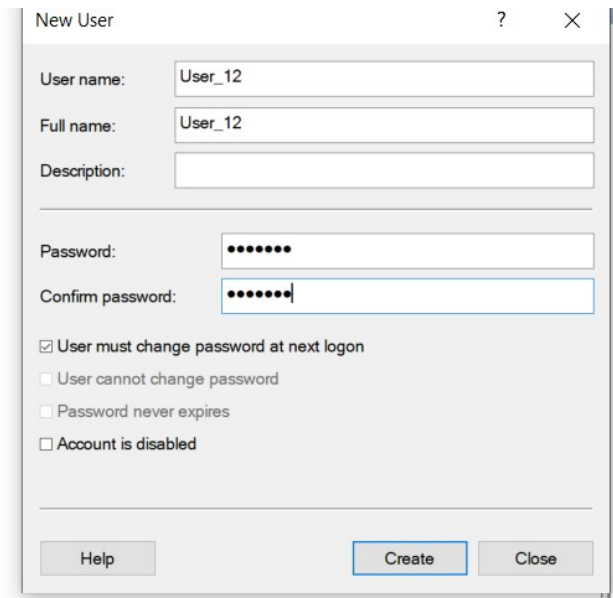




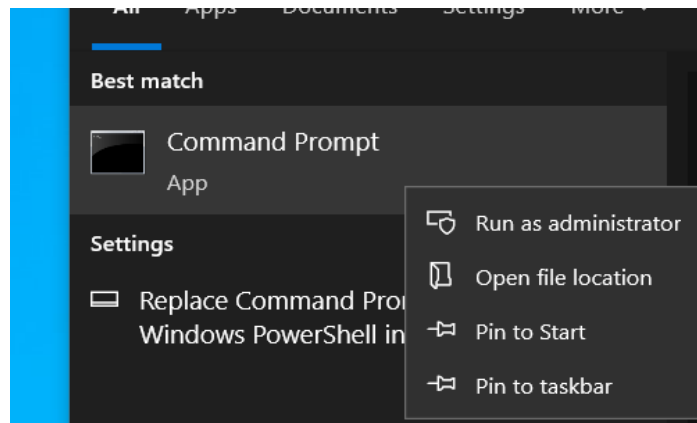
### 3.1.2.3. Создание через групповые политики



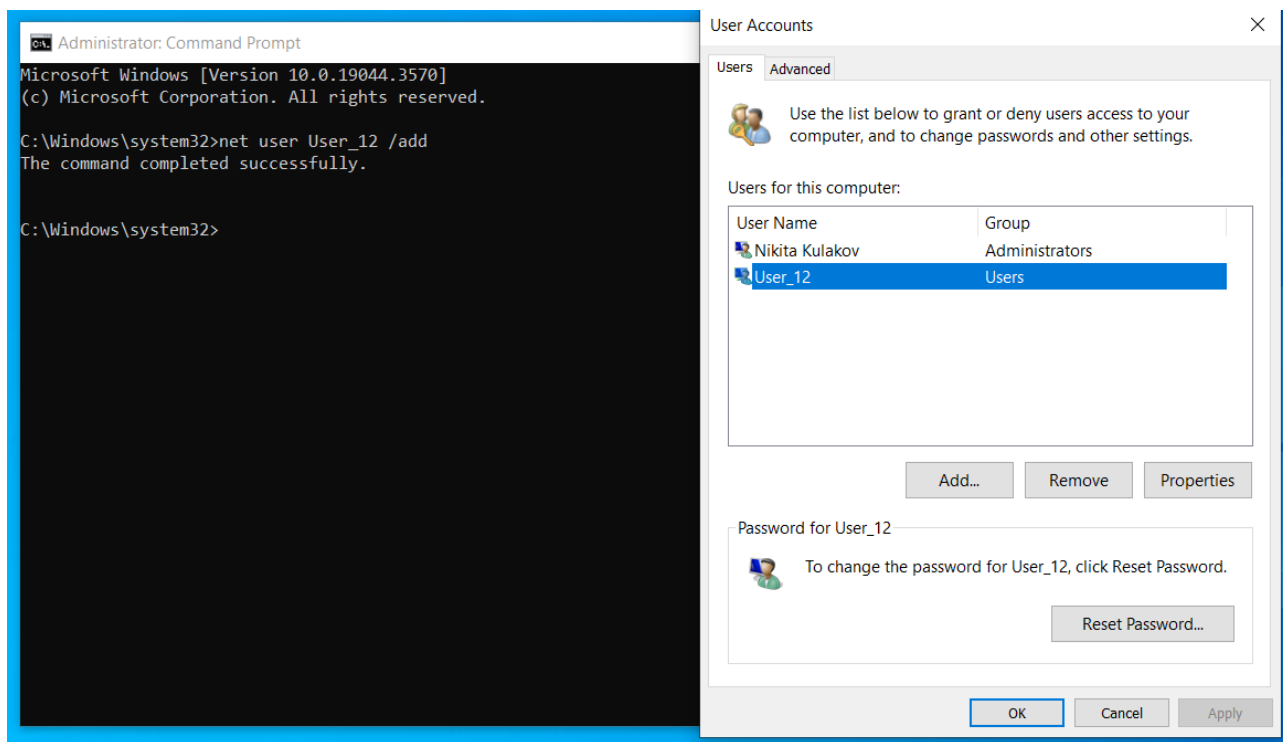
Нажимаем создать нового пользователя.



### 3.1.2.4. Создание через консоль

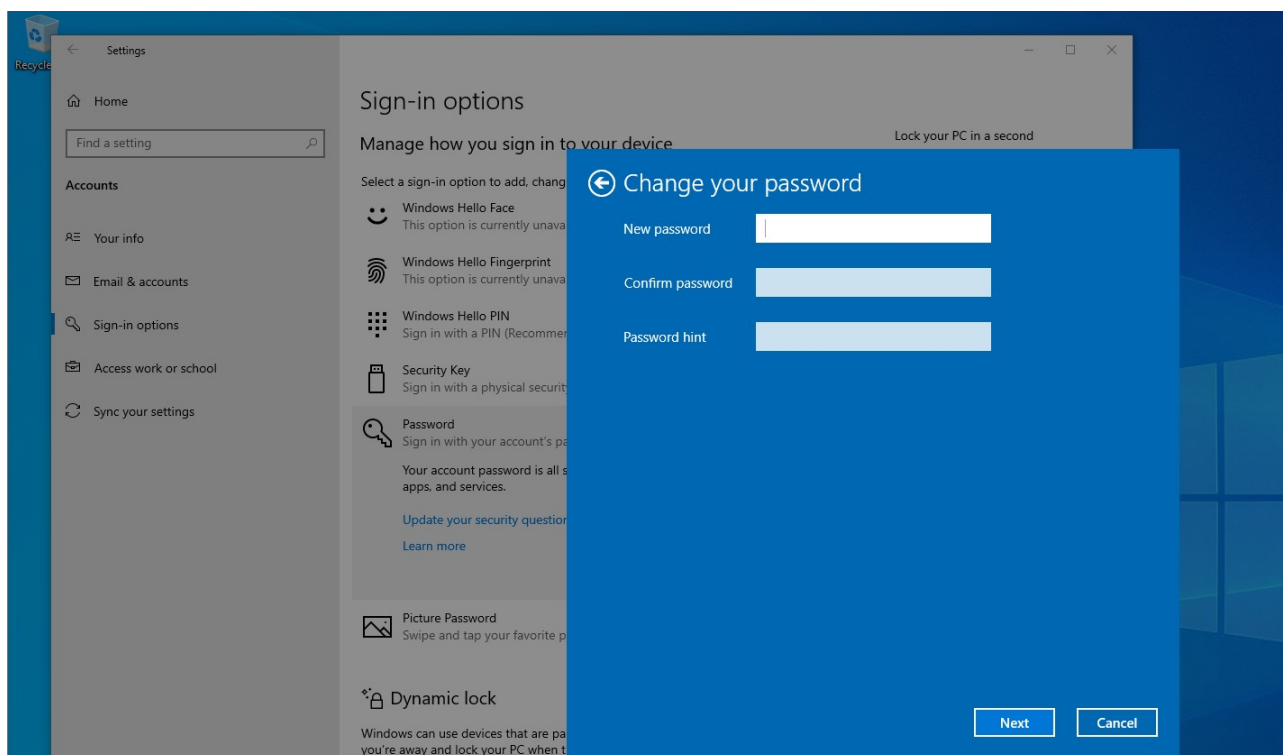


Запускаем от имени администратора

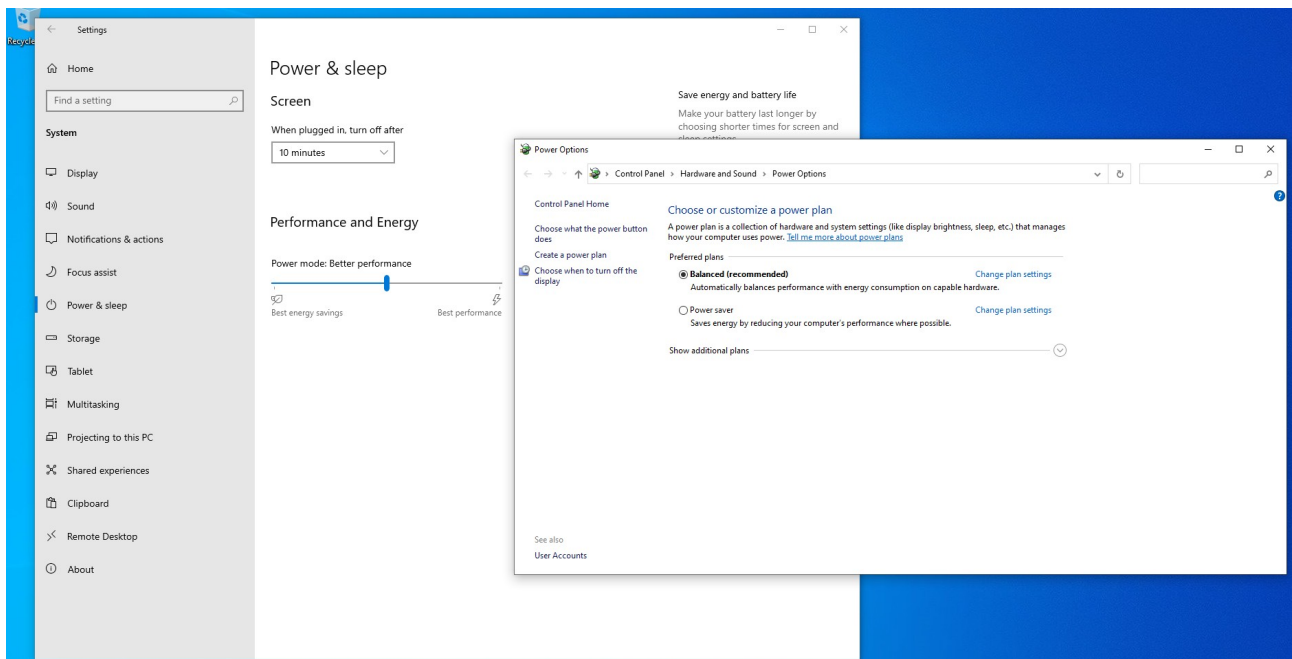


### 3.1.2.5. Возможности пользователя

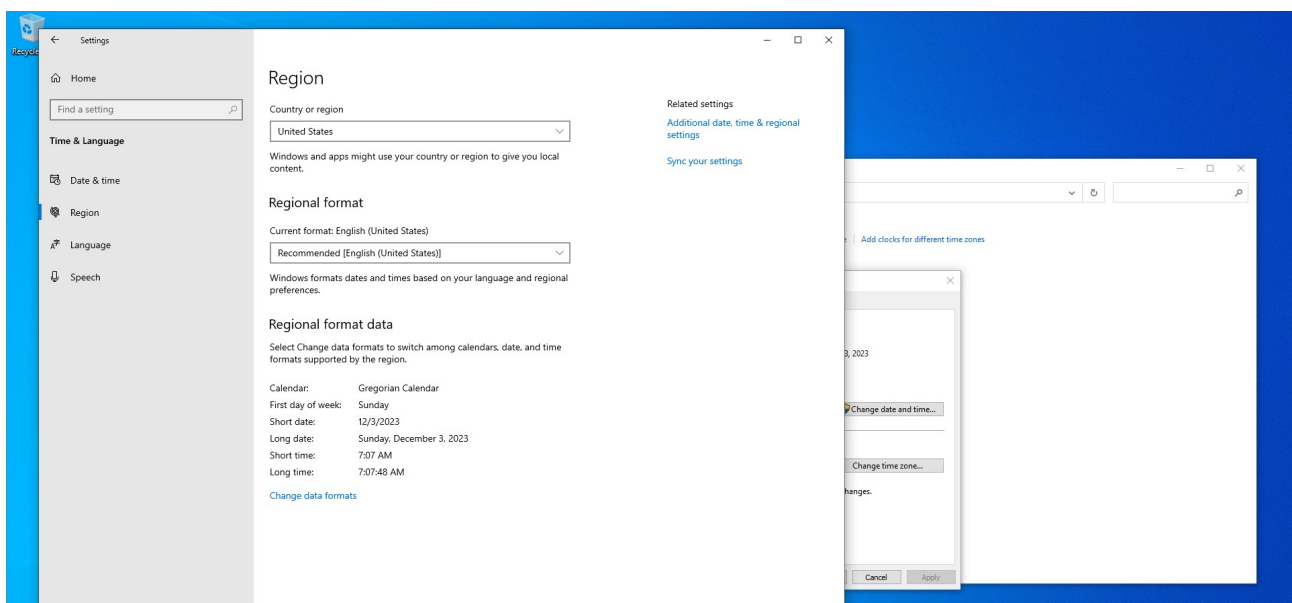
#### 1. Изменение пароля.



#### 2. Управление параметрами электропитания.



### 3. Управление часовым поясом и региональными настройками. Нельзя изменять время (требуется пароль администратора)



### 4. Управление персонализацией (если активировать Windows)

# Display



## Color

Night light

☐ Off

[Night light settings](#)

## Windows HD Color

Get a brighter and more vibrant picture for videos, games and apps that support HDR.

[Windows HD Color settings](#)

## Scale and layout

Change the size of text, apps, and other items

100% (Recommended) ▾

[Advanced scaling settings](#)

Display resolution

1920 × 1034 ▾

Display orientation

Landscape ▾

## Multiple displays

Older displays might not always connect automatically. Select Detect to try to connect to them.

Detect

[Advanced display settings](#)

## Sleep better

Night light can help you get to sleep by displaying warmer colors at night. Select Night light settings to set things up.

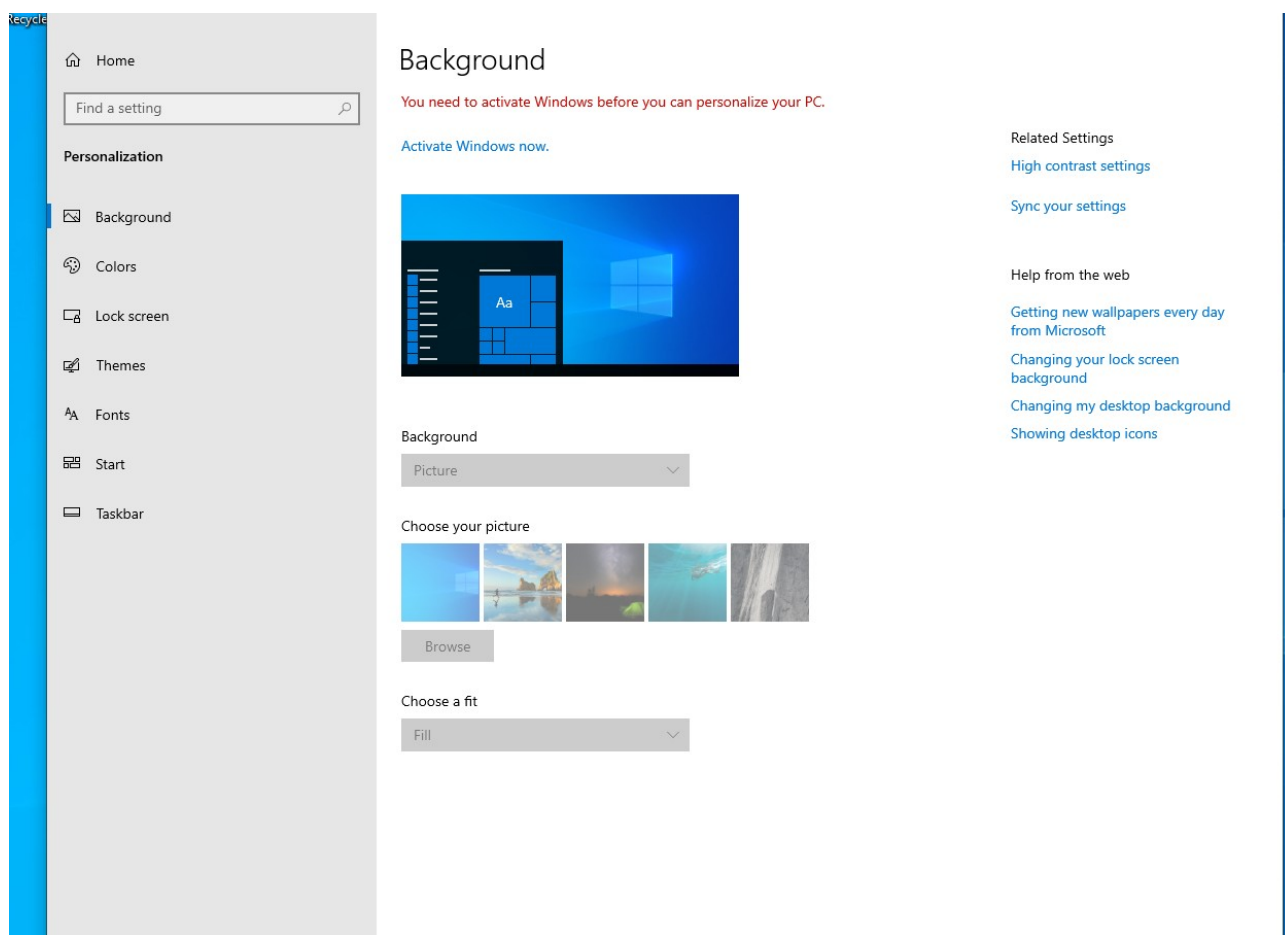
## Help from the web

[Connecting to a projector or PC](#)

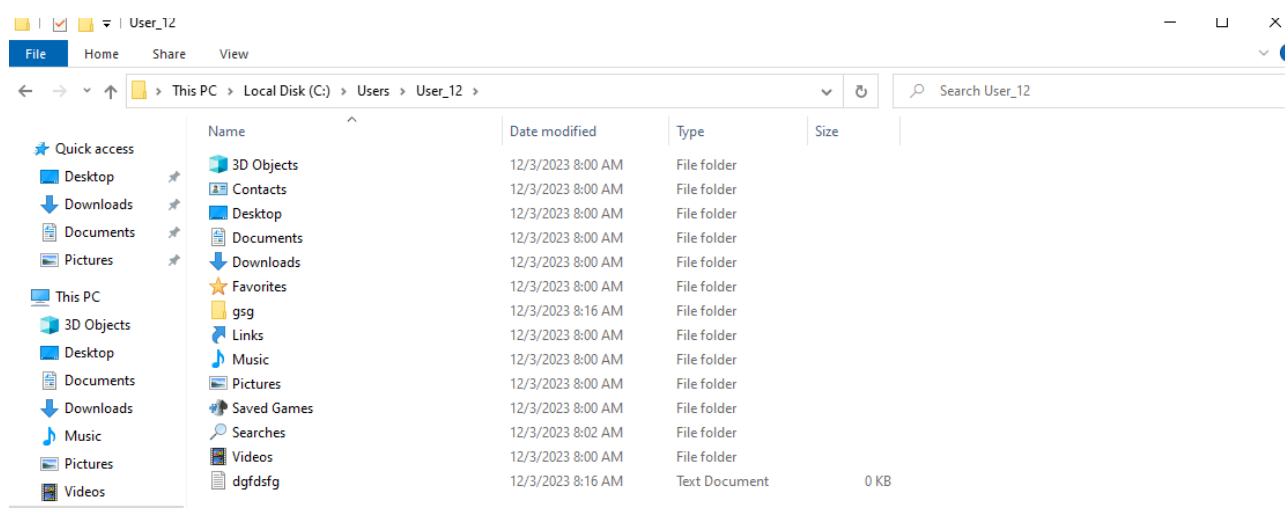
[Setting up multiple monitors](#)

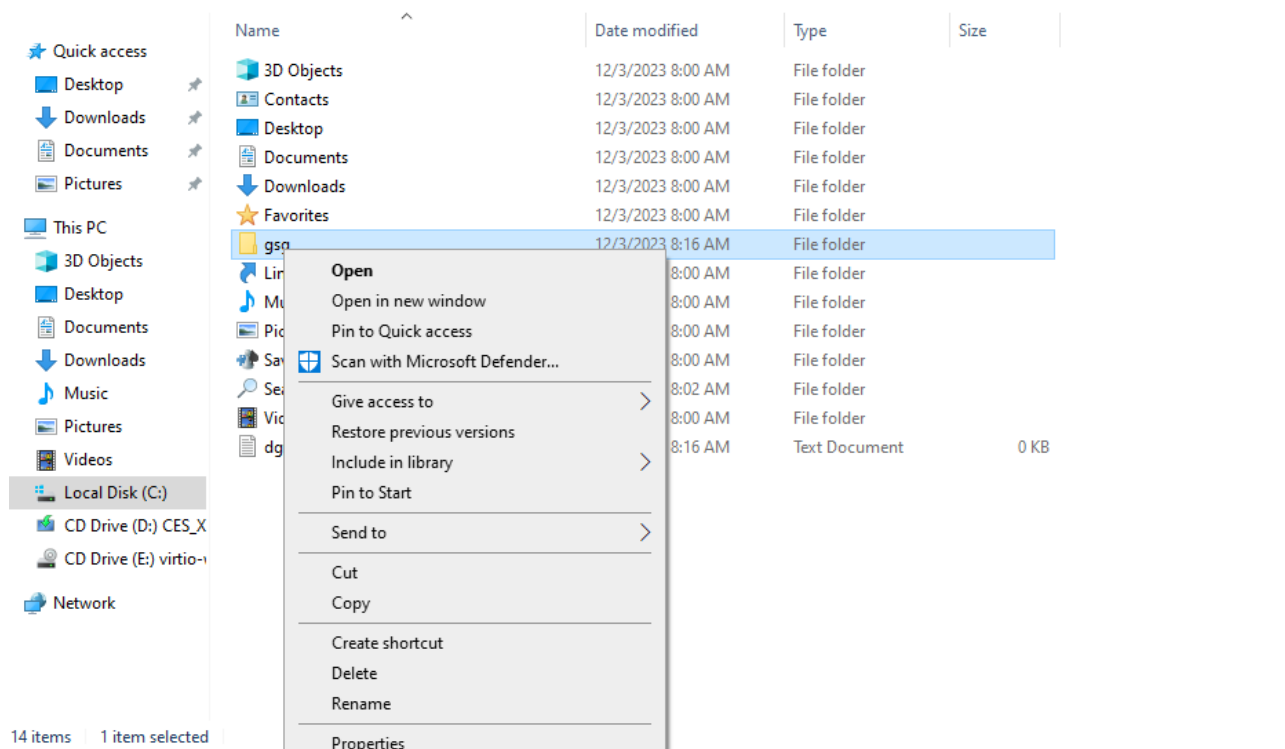
[Changing screen orientation](#)

[Changing screen brightness](#)

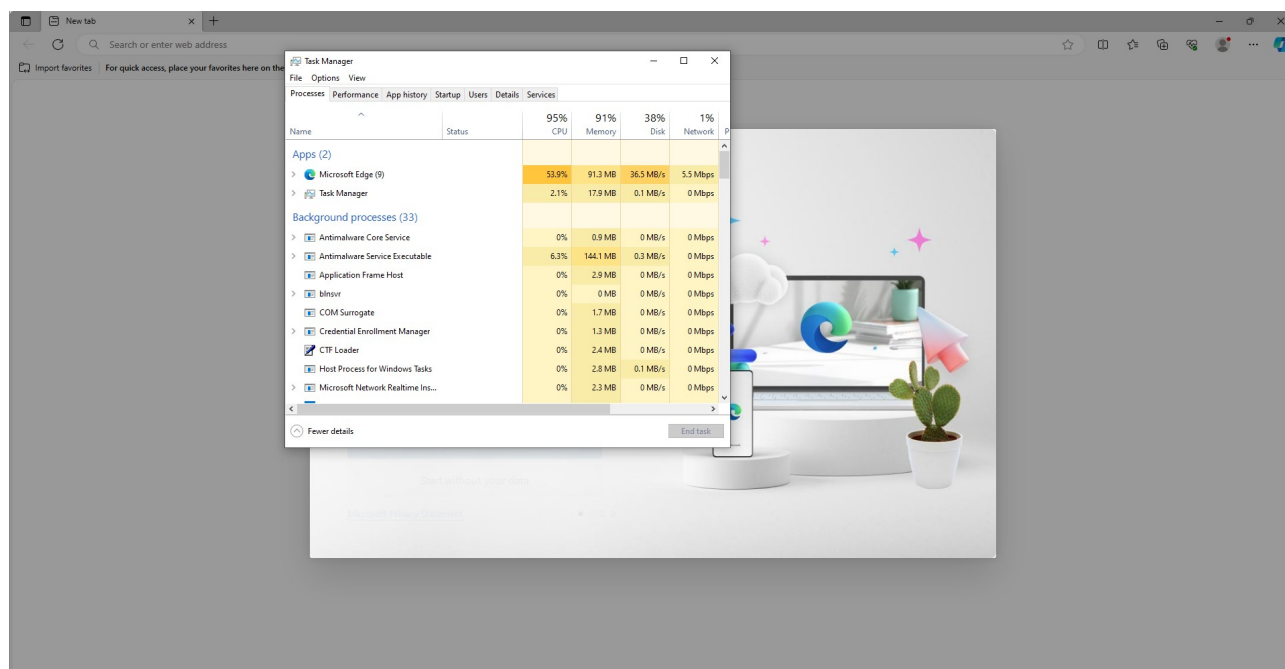


## 5. Создание, удаление, изменение содержимого файлов и папок в пределах папки личного пользователя.





## 6. Запуск приложений, не требующих прав администратора.



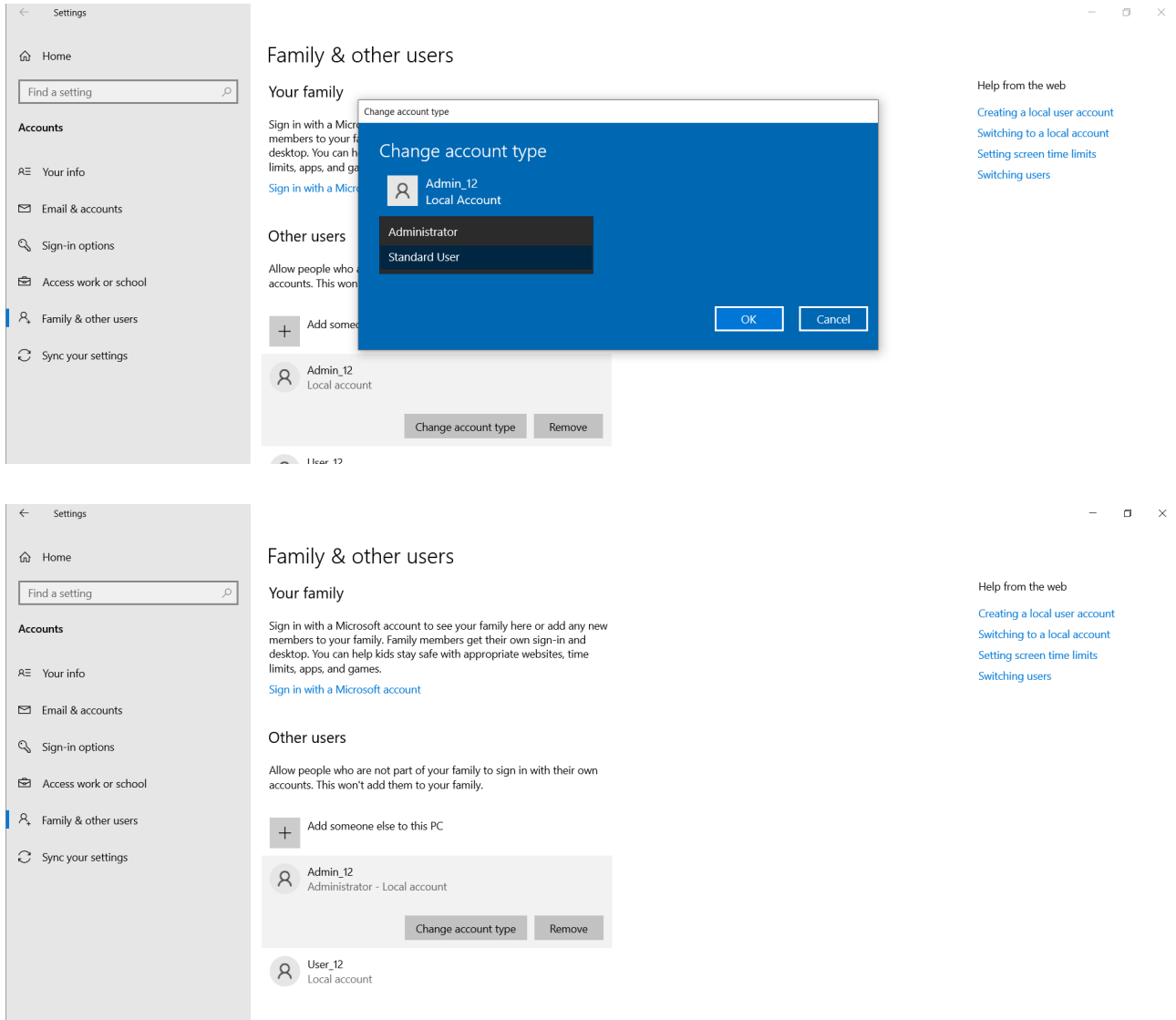
### 3.1.3. Создание администратора

Создайте администратора *Admin\_№* варианта, входящего в группу «Администраторы». Опишите все способы создания, а также (на примерах)

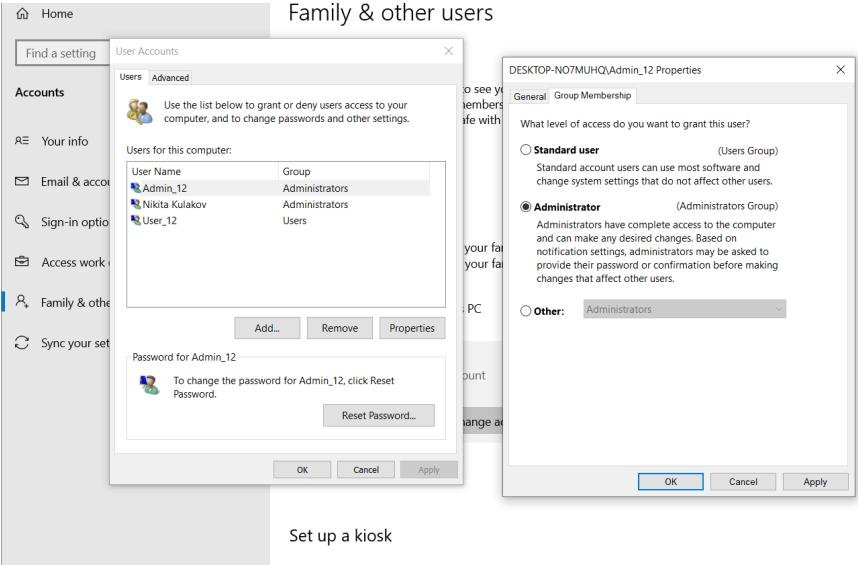


ограничения данного пользователя по изменению конфигурации системы (минимум 3 примера).

### 3.1.3.1. Создание через Settings



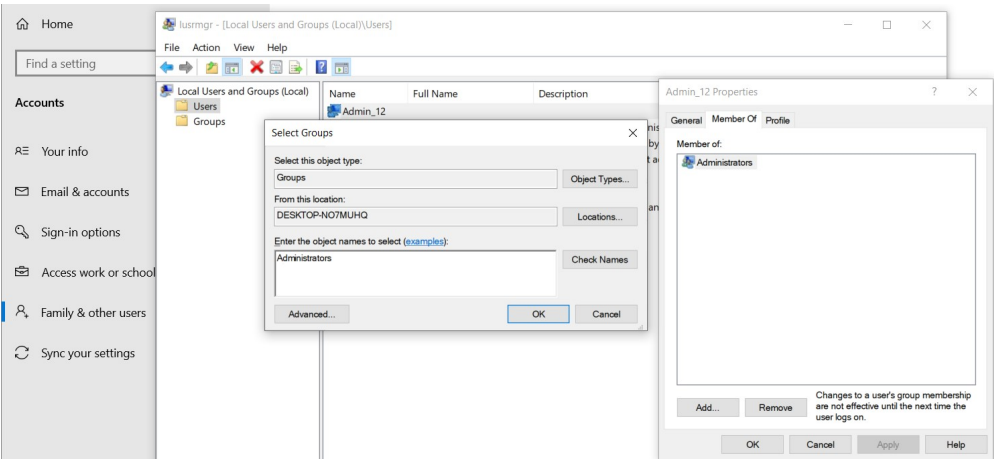
### 3.1.3.2. Создание через control userpasswords2



Help from the web

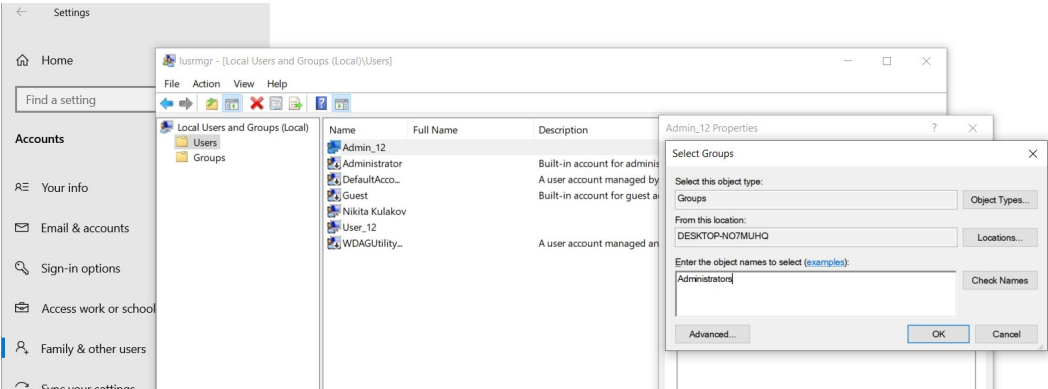
- [Creating a local user account](#)
- [Switching to a local account](#)
- [Setting screen time limits](#)
- [Switching users](#)

### 3.1.3.3. Создание через групповые политики



Help from the web

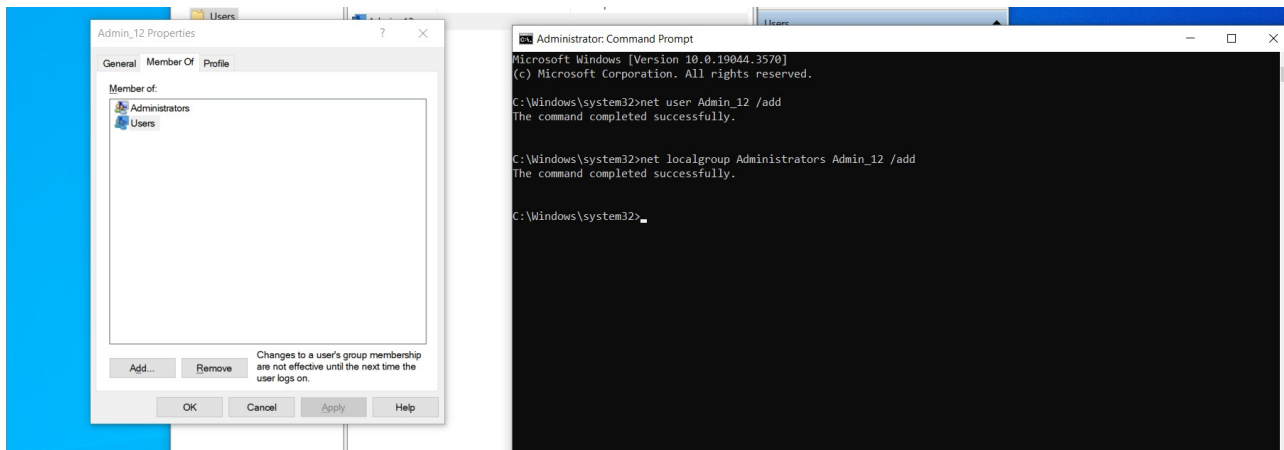
- [Creating a local user account](#)
- [Switching to a local account](#)
- [Setting screen time limits](#)
- [Switching users](#)



Help from the web

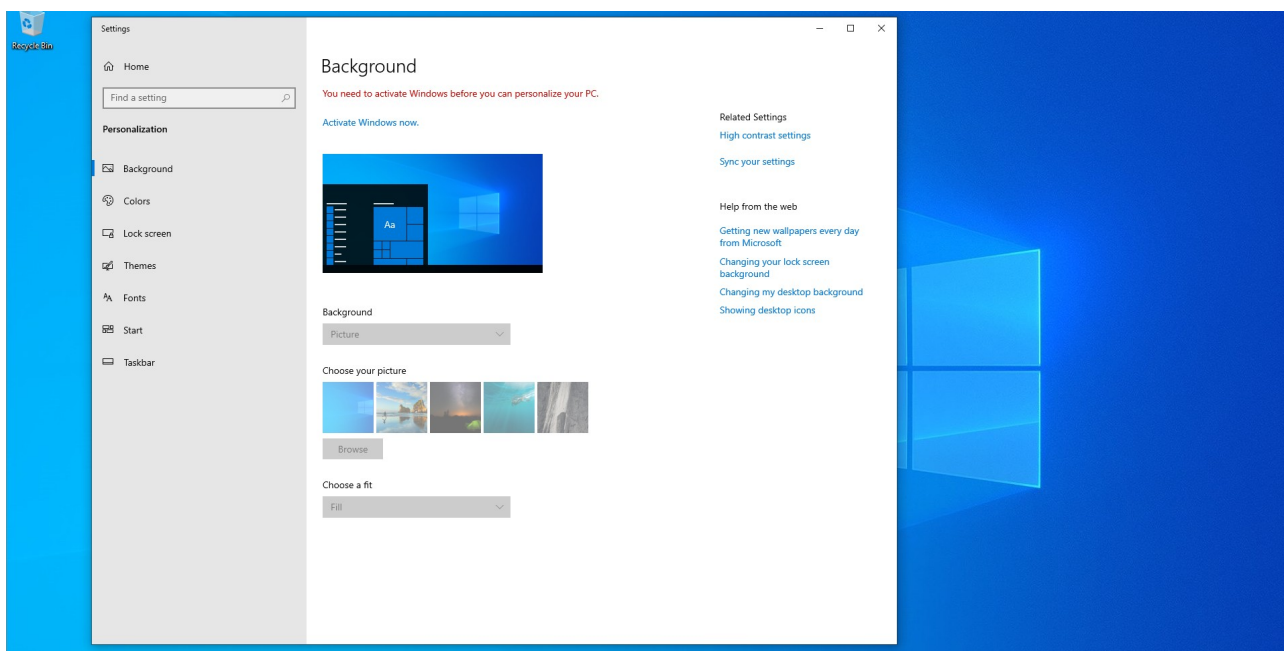
- [Creating a local user account](#)
- [Switching to a local account](#)
- [Setting screen time limits](#)
- [Switching users](#)

### 3.1.3.4. Создание через консоль

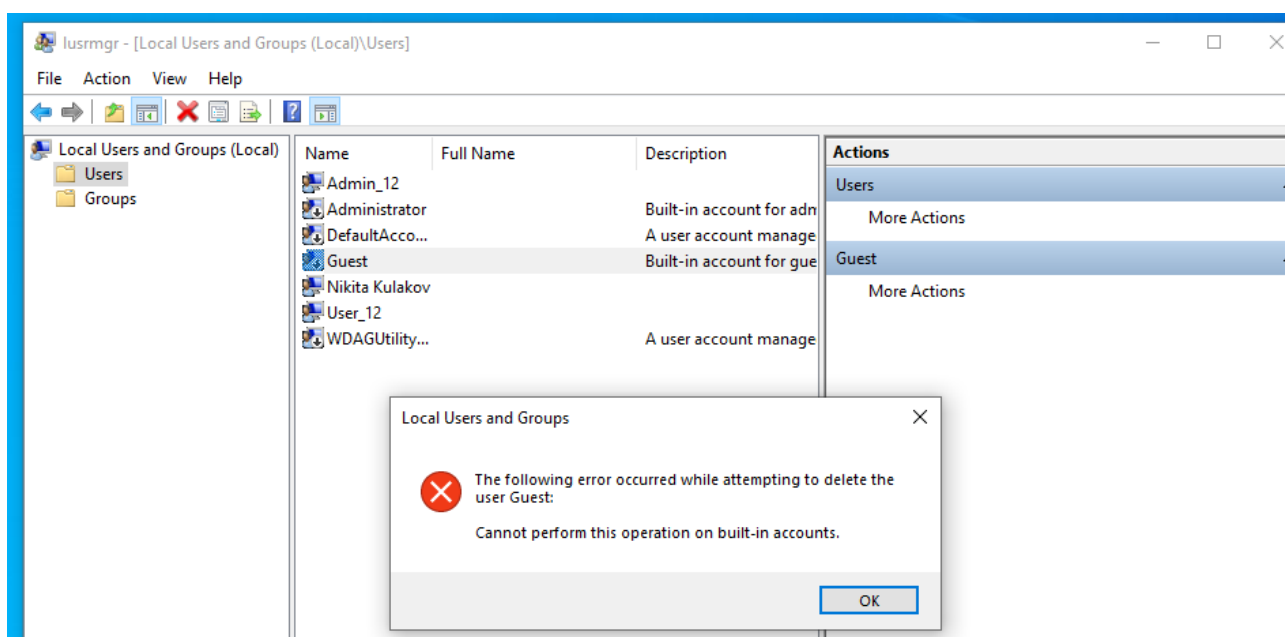
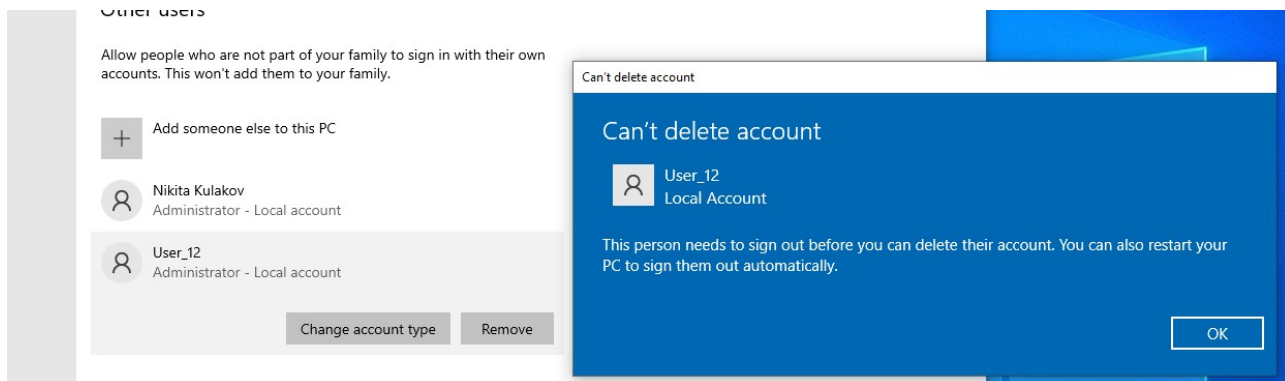


### 3.1.3.5. Ограничения администратора

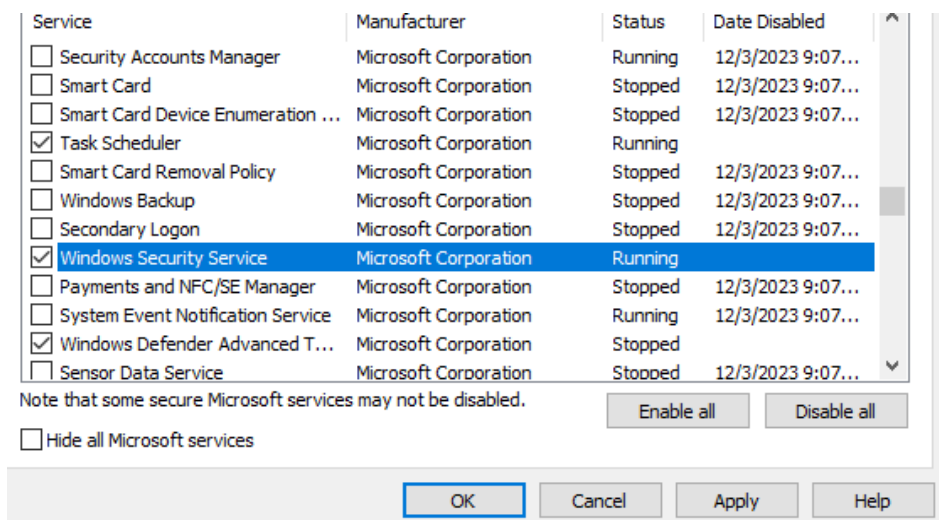
#### 1. Невозможность персонализации в случае неактивированной ОС



## 2. Невозможность удаления своего же аккаунта, а также встроенных аккаунтов Guest и Administrator



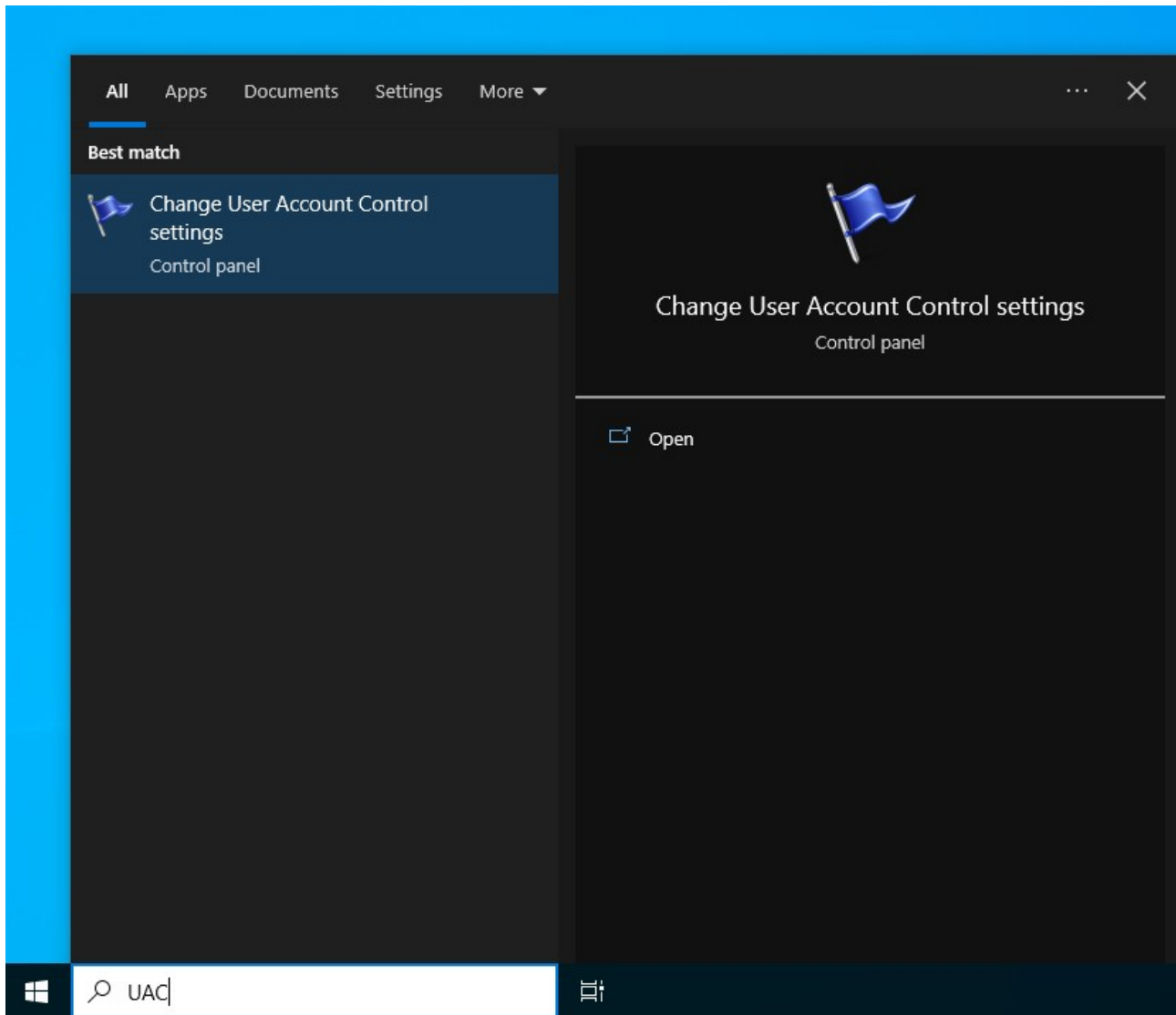
## 3. Невозможность отключения некоторых Service-ов Windows

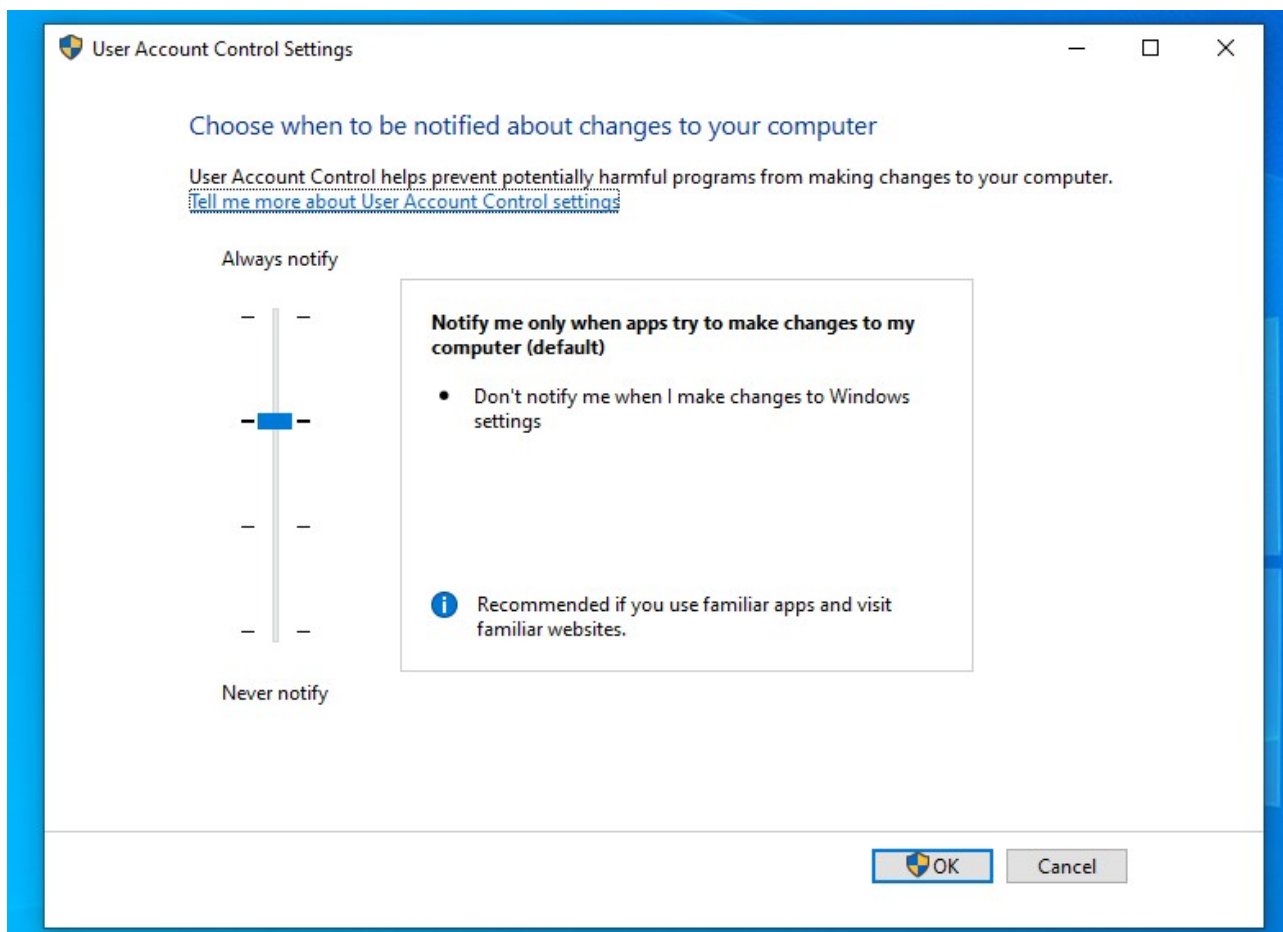


### 3.1.4. Параметры контроля учетных записей пользователей

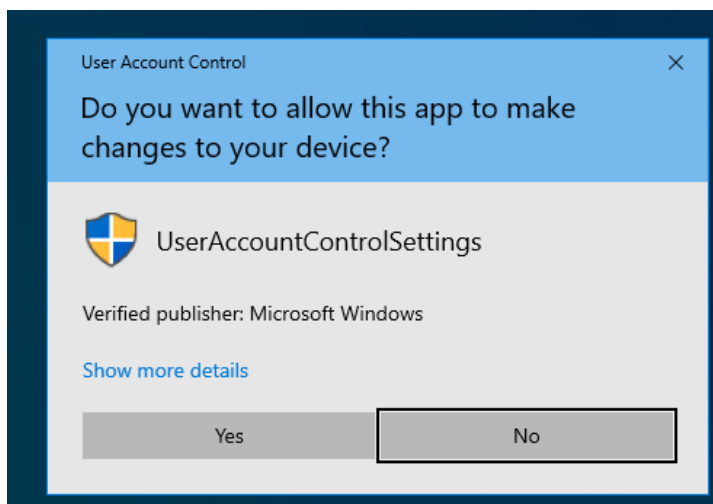
*Опишите параметры контроля учетных записей пользователей (UAC).*

Параметры UAC (контроля учетных записей) позволяют предотвратить внесение изменений потенциально опасным ПО, поскольку уведомления будут явно получены пользователем, который сможет отреагировать на них, разрешая или запрещая выделение прав администратора.





При выполнении изменений Windows явно спросит, применять ли настройки.



Существует 4 уровня настроек:

1. Уведомлять всегда. Уведомляет при изменении настроек Windows или при установке программного обеспечения. Рекомендуемо, если часто посещаете незнакомые web-сайты или часто устанавливаете ПО.

2. Уведомлять, когда приложения пытаются внести изменения в ваш компьютер (по умолчанию). В отличие от предыдущего, не будет уведомлять когда пользователь производить изменения настроек Windows.
3. Уведомлять, когда приложения пытаются внести изменения в ваш компьютер (не затемнять экран). Не будет уведомлять при изменении настроек Windows пользователем. Не рекомендуемый вариант.
4. Никогда не уведомлять при установке, либо изменениях настроек пользователем. Крайне не рекомендуемый вариант.

### **3.1.5. Настройка механизмов защиты**

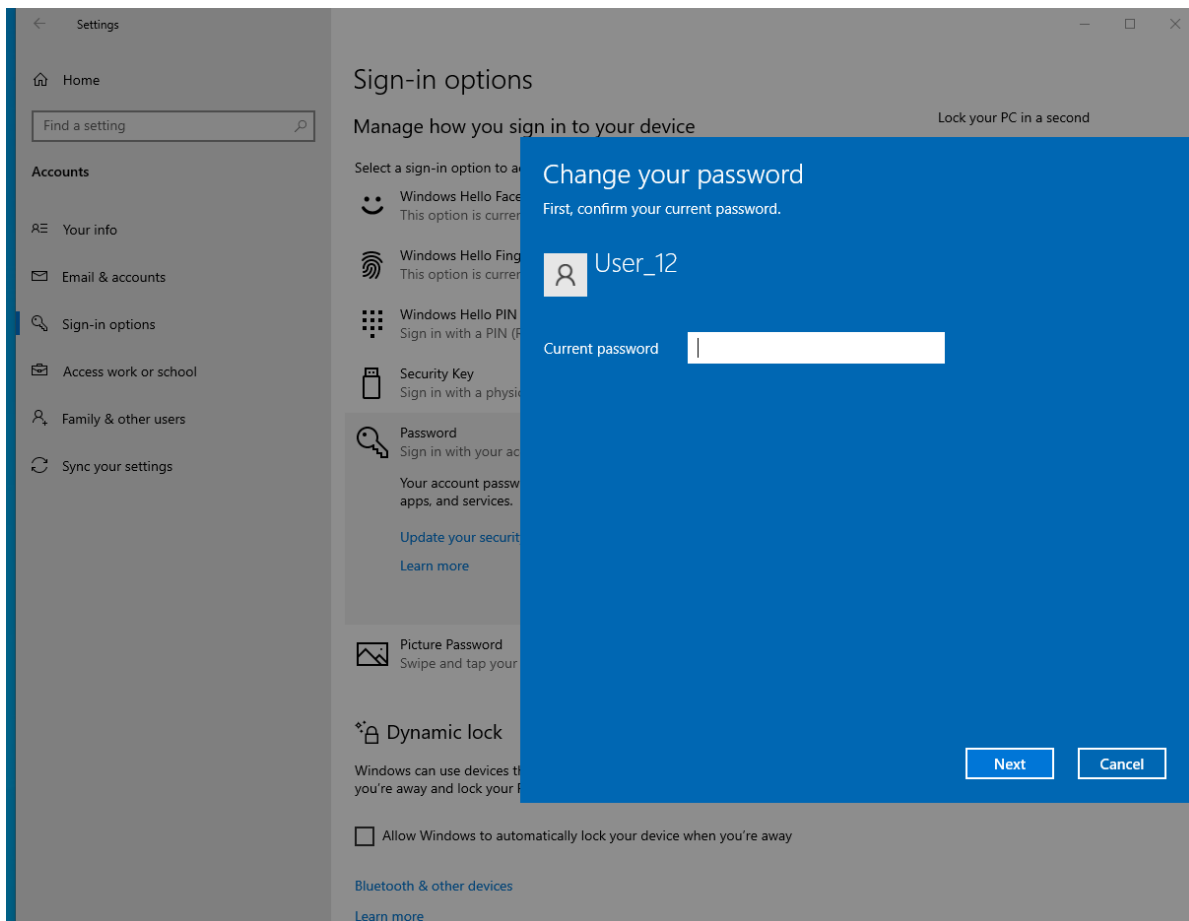
*Выполните настройки механизмов защиты ОС Windows в соответствии с вариантом. Проанализируйте выполненные Вами настройки механизма защиты в части выполнения ими требований руководящих документов в области защиты информации. Сформулируйте, в чем не выполняются данные требования. Проанализируйте реализацию в ОС Windows механизма защиты в целом (не конкретно для Вашего примера).*

*Вариант 2. Настроить вход пользователя в систему в безопасном режиме по паролю. Рассмотреть и реализовать возможные способы усиления парольной защиты.*

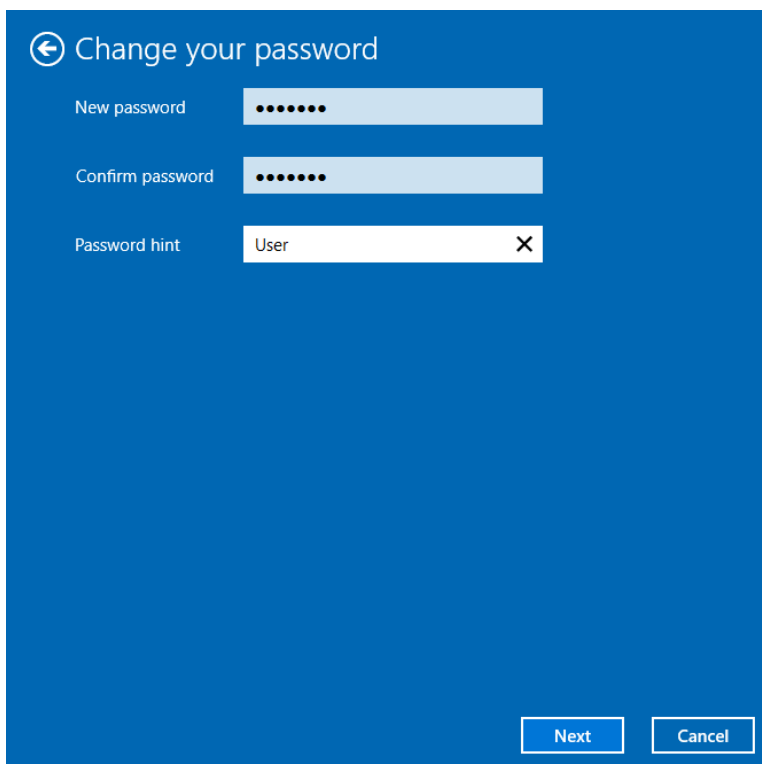
#### **3.1.5.1. Установка пароля пользователя**

Переходим в Settings → Accounts, выполняем изменение пароля пользователя.

Вводим предыдущий пароль.



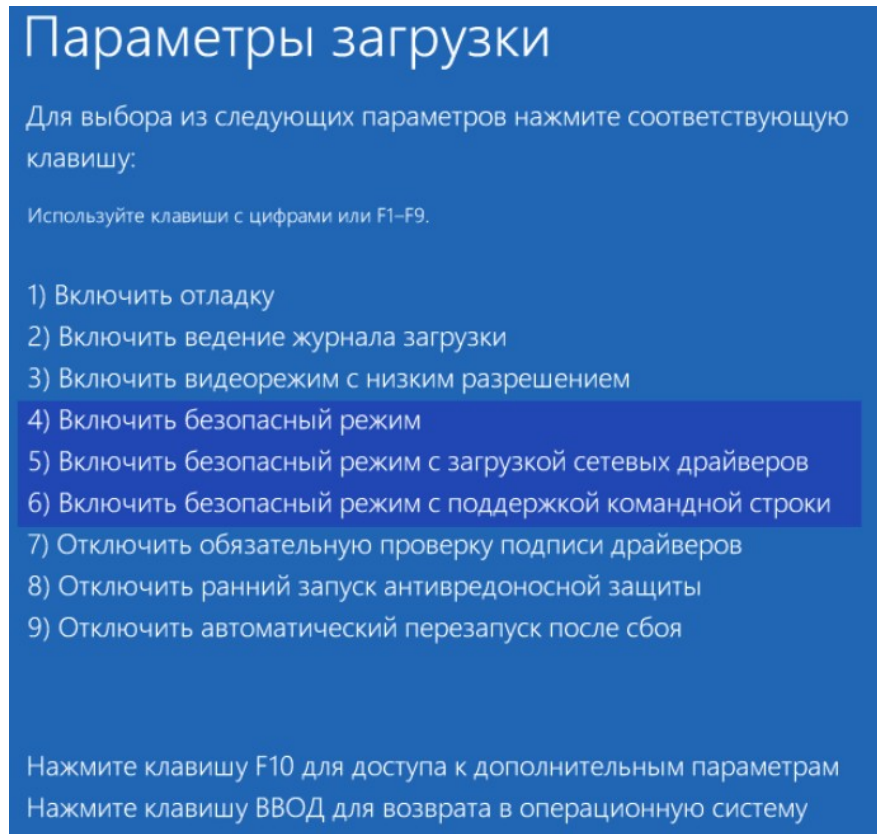
Вводим новый пароль.



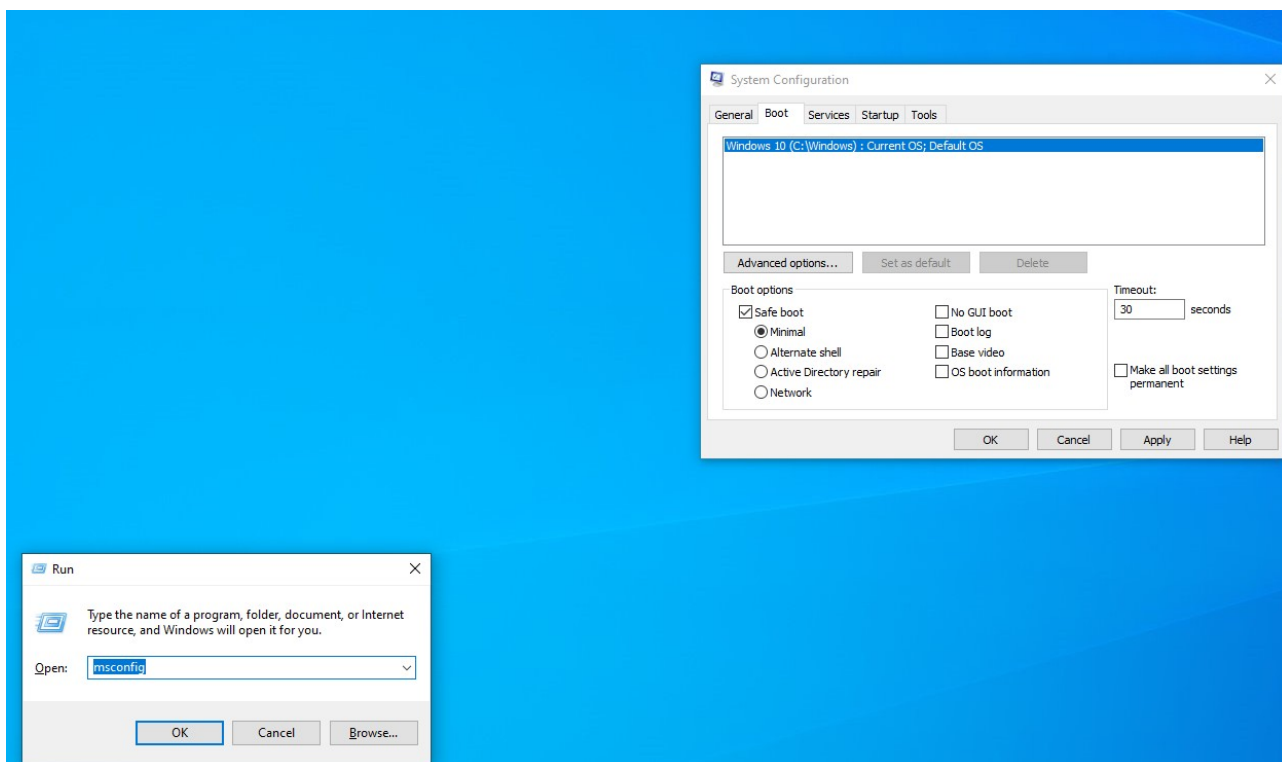


### 3.1.5.2. Загрузка в безопасном режиме

Выполним загрузку в безопасный режим через msconfig. Также это можно было бы сделать через восстановление, выбрав пункт включения безопасной загрузки в параметрах загрузки:

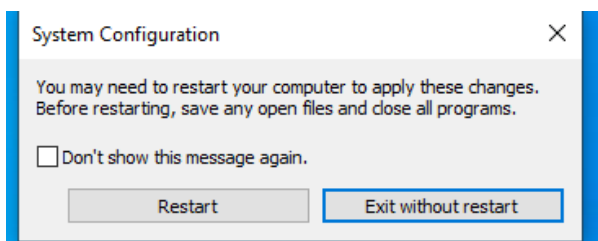


Через msconfig:



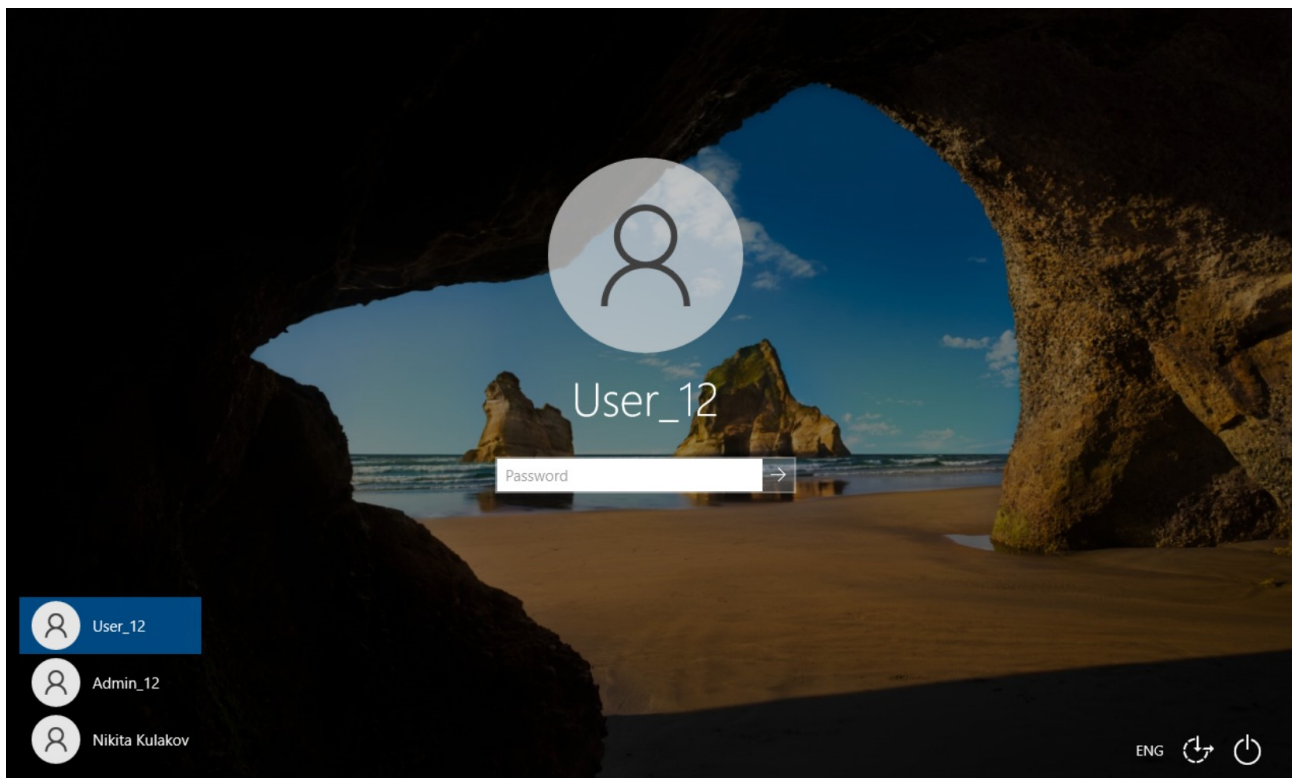
Включим Safe boot в Boot options, выберем вариант с загрузкой с минимальными возможностями с включенным графическим интерфейсом. Включим OS boot information. Применим настройки.

Произведем перезагрузку.

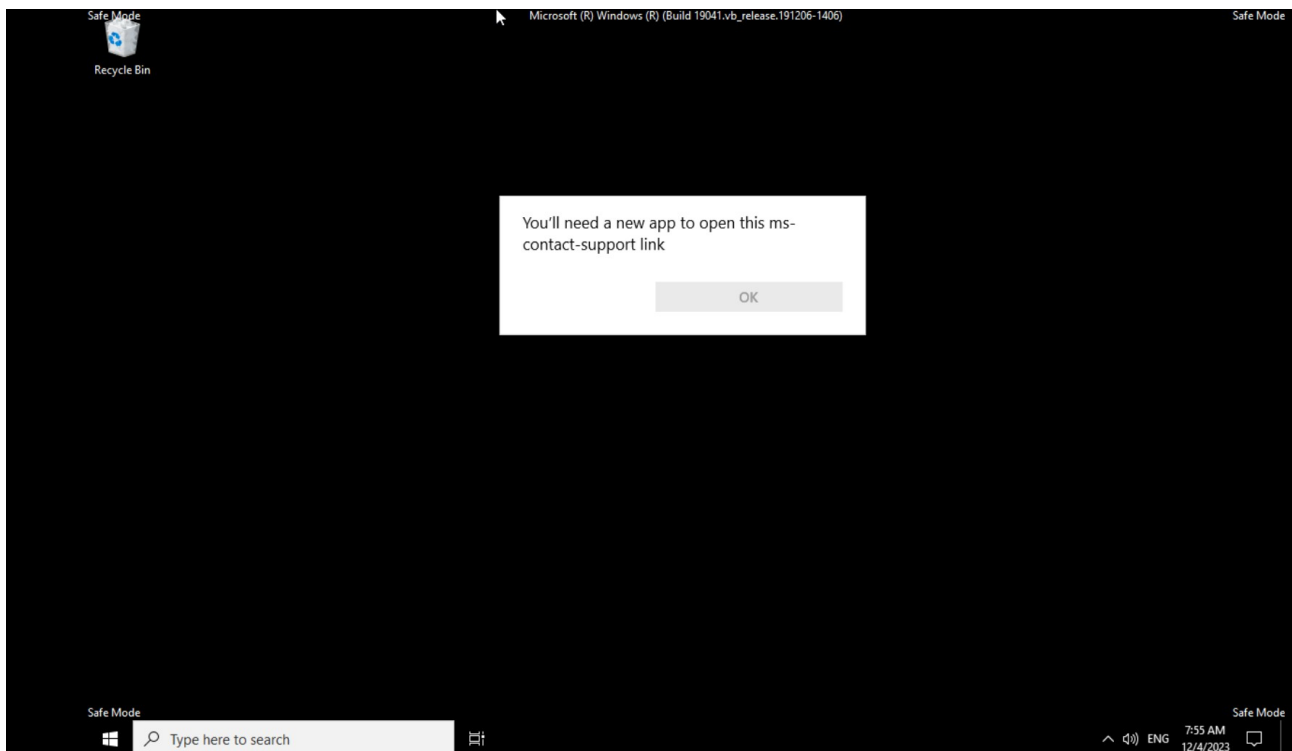


Поскольку был выбран вариант с минимальными возможностями, графические драйвера для виртуальной машины также не были загружены.

Введем пароль пользователя для входа в систему в безопасном режиме.



Как видим, система была запущена в безопасном режиме.



### **3.1.5.3. Возможные способы усиления парольной защиты**

Усиление самого пароля для удовлетворения требованиям сложности:

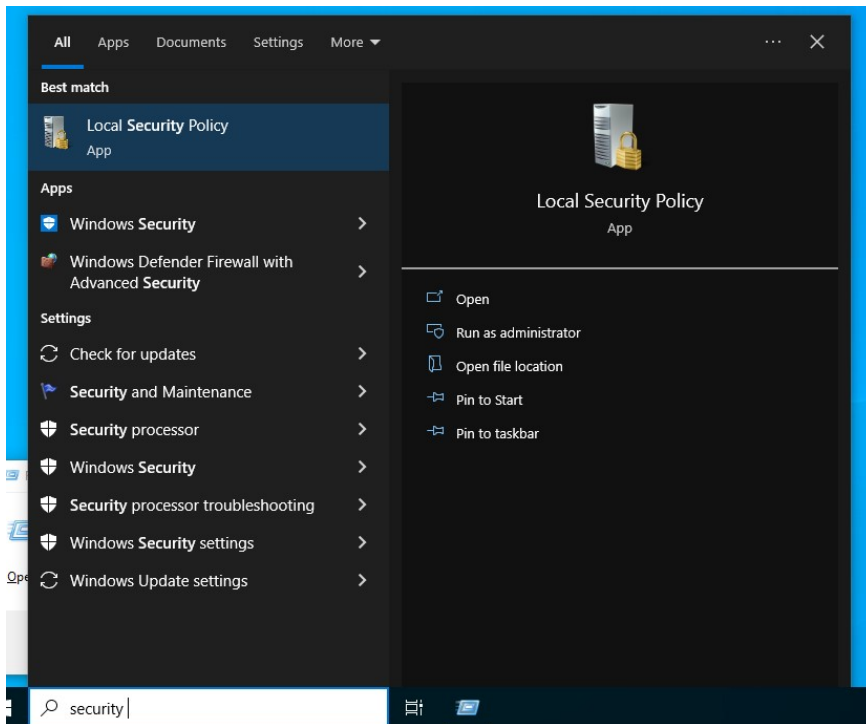
- Увеличение длины пароля
- Использование большего алфавита символов: букв, цифр, спец-символов ( , . % \$ ... ) , различных алфавитов
- Избегание использования личных данных, а также предсказуемых последовательностей, таких как имена, номера телефонов и другая личная информация.
- Использование автоматически-сгенерированных паролей, учитывающих пункты выше

Усиление мер:

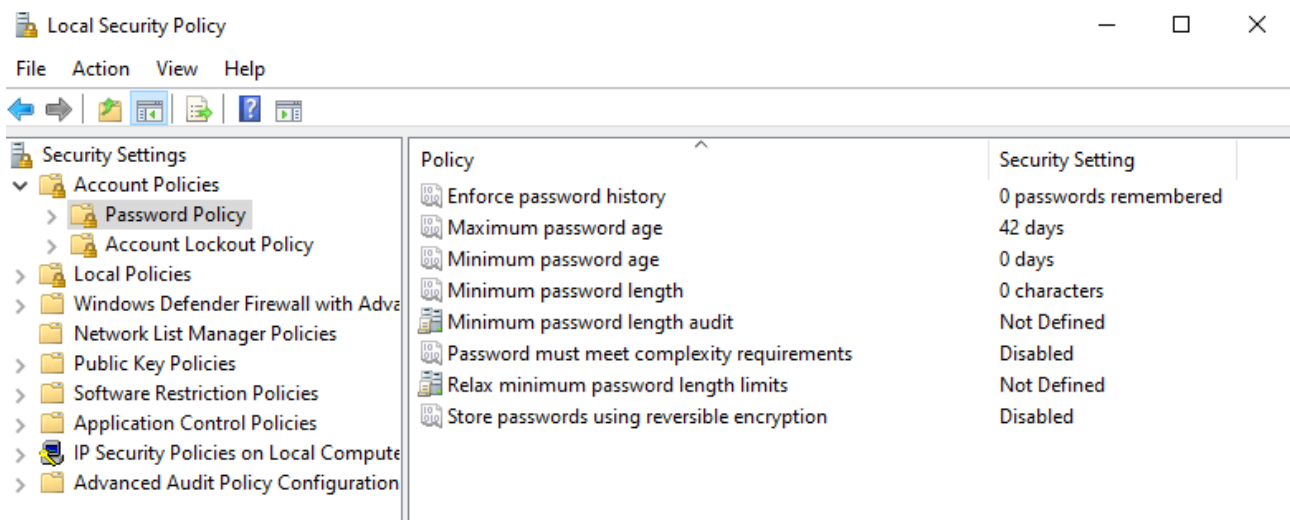
- Управление сроком действия пароля, периодической сменой
- Ограничение числа попыток ввода паролей, а также блокировка входа при использовании всех доступных попыток, либо timeout
- Использование неповторяемых паролей для различных ресурсов
- Ведение журнала аудита, а также его периодическая проверка
- Использование шифрования для хранения паролей

Часть мер можно установить в локальной политике безопасности Windows.

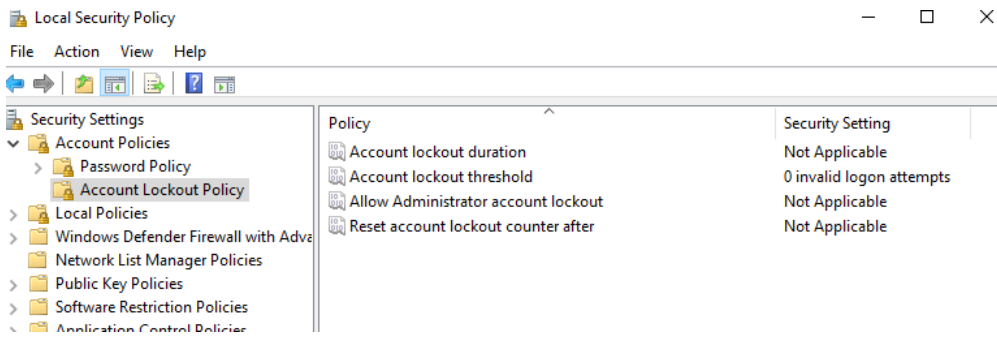
Открываем Local Security Policy:



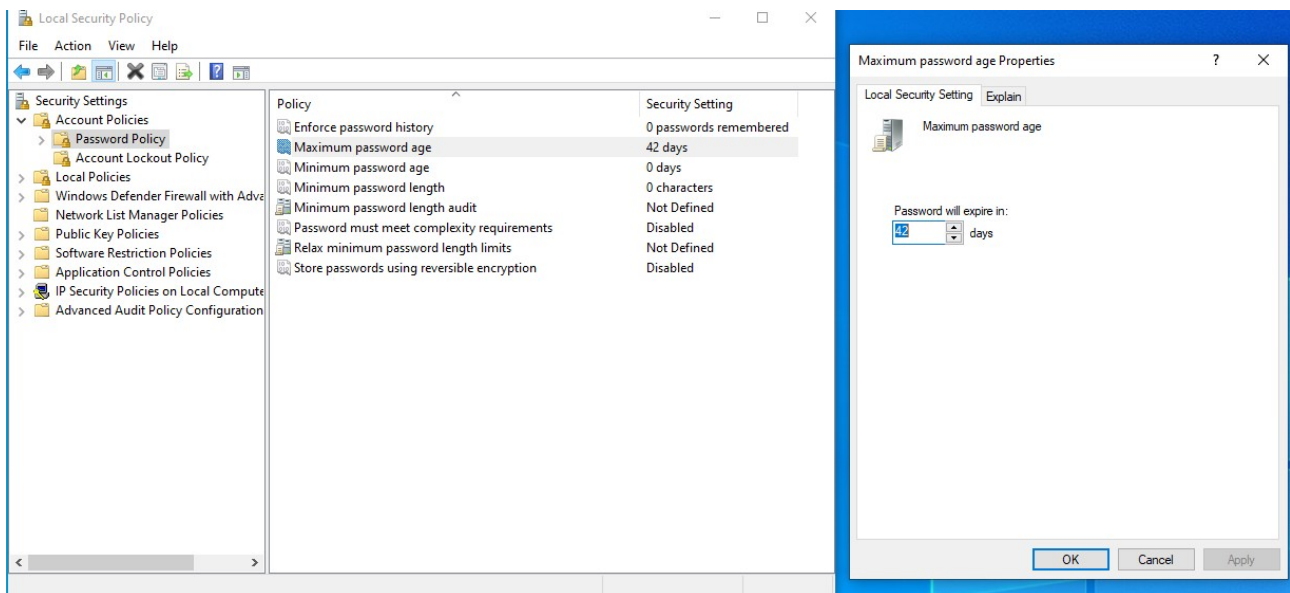
Политики безопасности паролей:



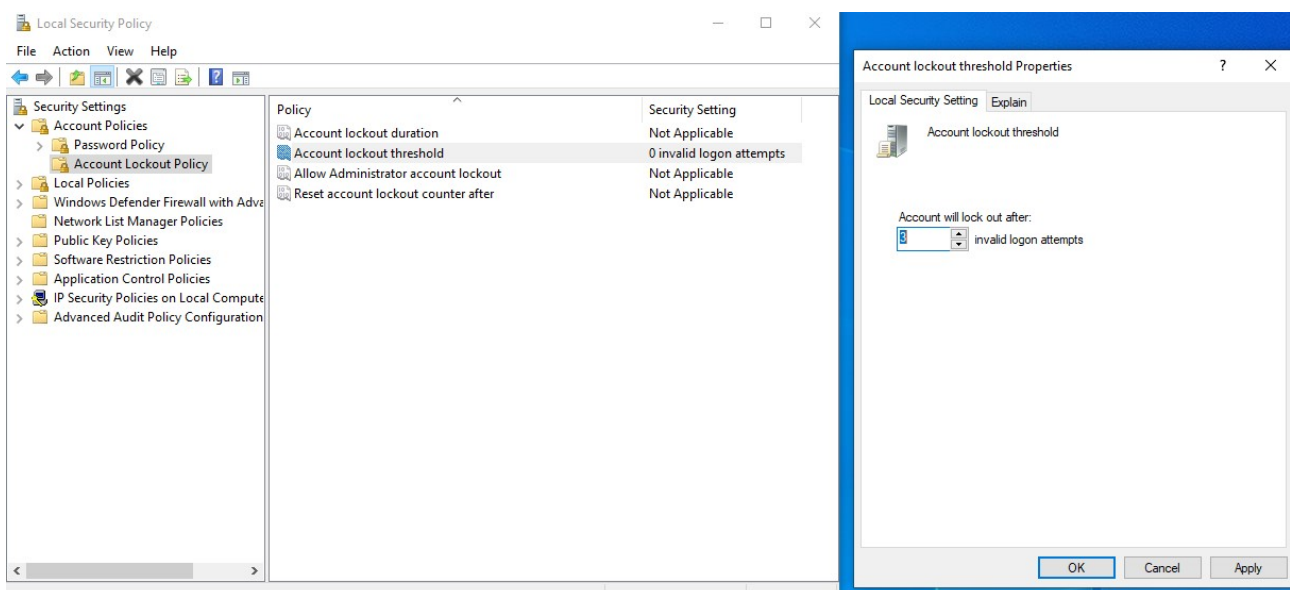
## Политики блокировок аккаунтов:



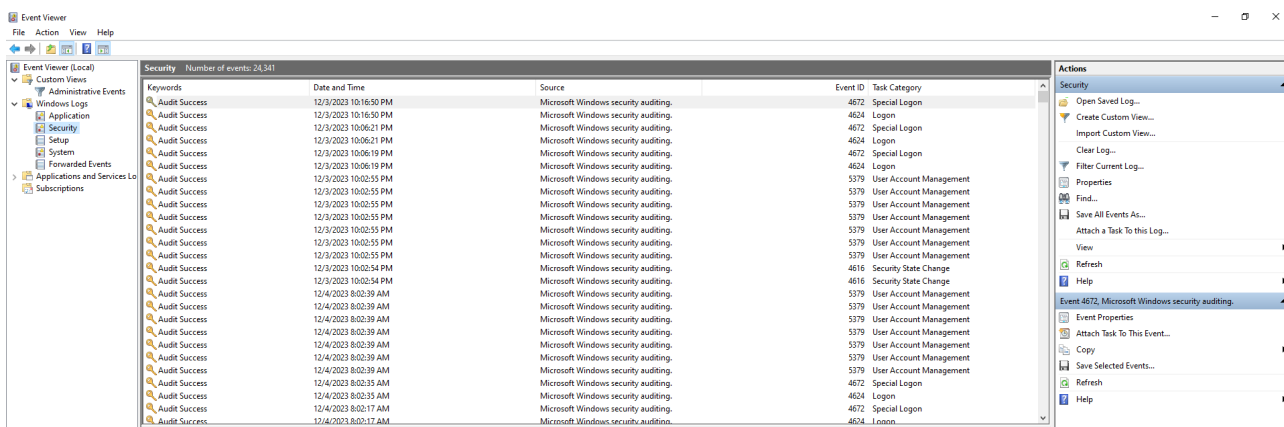
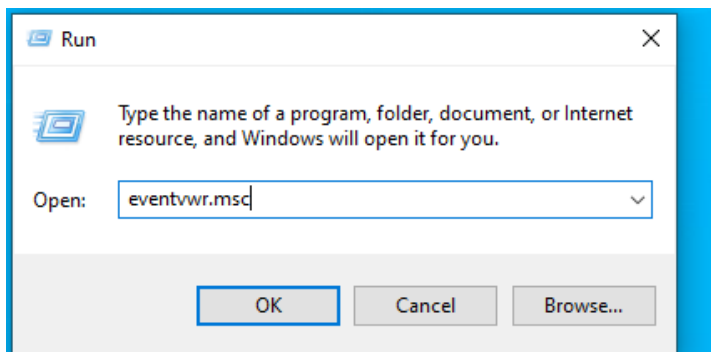
## Установим время жизни пароля:



## Установим lockout threshold:



## Журнал событий:



Произведенные мною действия не соответствуют руководящим и нормативным документам регуляторов РФ в области защиты персональных данных:

- После 15 минут бездействия (неактивности) пользователя сеанс должен быть автоматически заблокирован
- Пароль должен состоять из спец-символов (например, !, @, #, \$, &, \*, % и т. п.), однако у меня такового не выполняется
- Пароль не должен включать в себя легко вычисляемые сочетания символов, я использую префикс `User\_`
- Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре, я использую постфикс 12

- При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях, однако я изменил позицию только в 1 символе

#### **3.1.5.4. Анализ реализации механизма защиты Windows 10 в целом**

Windows 10 Enterprise прошла сертификационные испытания ФСТЭК России по требованиям доверия. Полученный сертификат №4369 подтверждает, что Windows 10 Enterprise соответствует изложенным требованиям, предоставленным в документах:

- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 6 Уровню доверия.
- «Требования по безопасности информации к операционным системам» (ФСТЭК России, 2016).
- «Профиль защиты операционных систем типа А шестого класса защиты. ИТ.ОС.А6.ПЗ» (ФСТЭК России, 2017)

Однако 2022 года ФСТЭК принял решение приостановить действие сертификатов на все программное обеспечение Microsoft, поэтому следует быть осторожным при использовании Windows 10 Enterprise.

С точки зрения руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» ОС Windows 10 Enterprise удовлетворяет 6 классу защищенности, соответствуя следующим показателям:

- Дискреционный принцип контроля: должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам



(файлам, программам, томам и т. д.), что в Windows реализовано посредством связи пользователя с группой

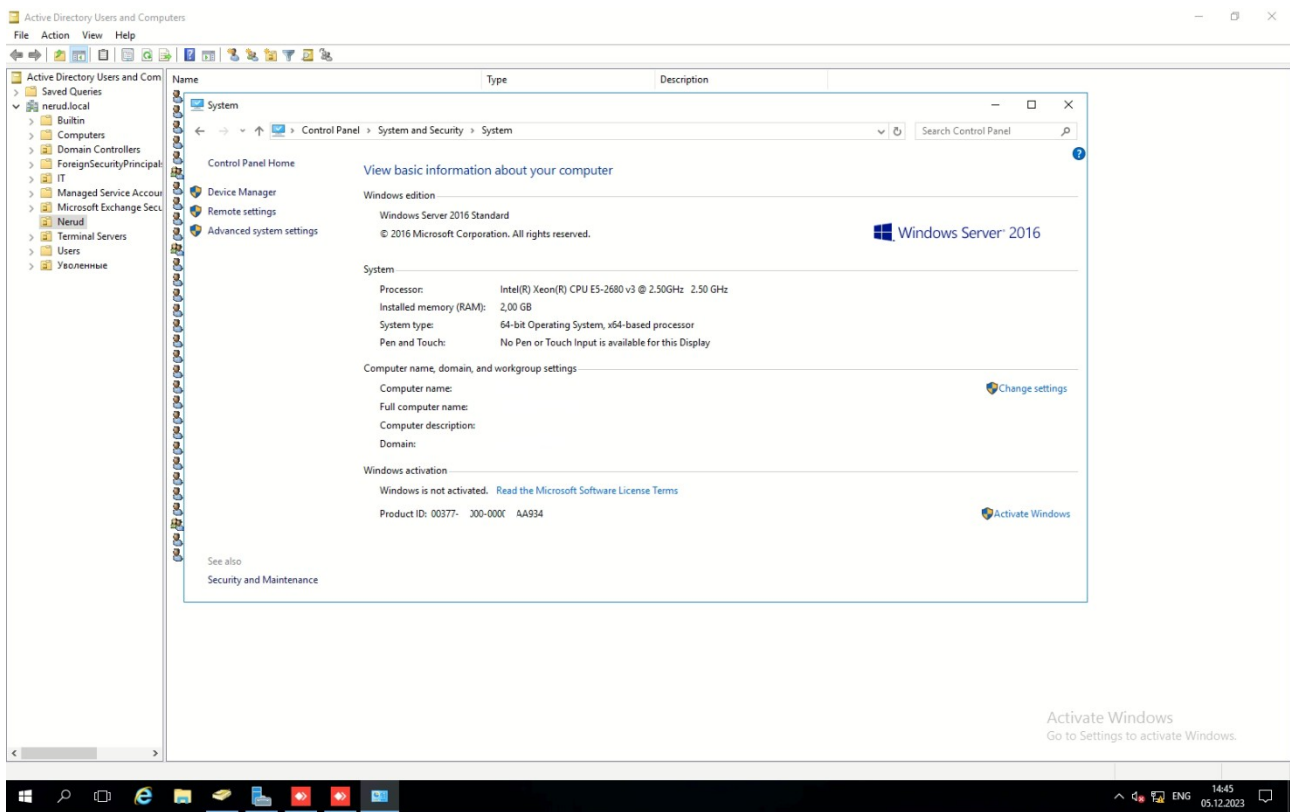
- Идентификация и аутентификация: пользователь обладает возможностью аутентификации и идентификации, а система должна обеспечивать проверку подлинности пользователя, и препятствовать получению доступа к защищаемым ресурсам от неаутентифицированных пользователей. В Windows реализовано при помощи биометрических данных и ввода логина и пароля
- Руководство пользователя, тестовая документация: система должна иметь документацию и краткое руководство пользователя. Windows 10 имеет документацию и справку.
- В Windows 10 не выполняется периодически контроль целостности, только вручную с помощью команды DISM.exe

## **3.2. Дополнительная часть**

### **3.2.1. Windows Server. Создание и копирование профиля**

*Опишите создание профиля пользователя и его копирование (на основе Windows Server).*

Информация об используемой системе:

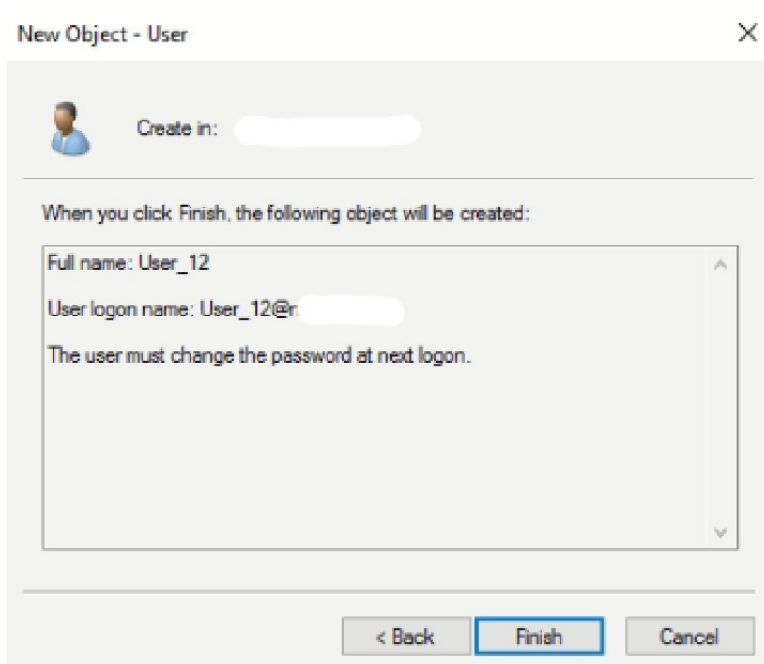


Вводим пользовательские данные, пароль пользователя:

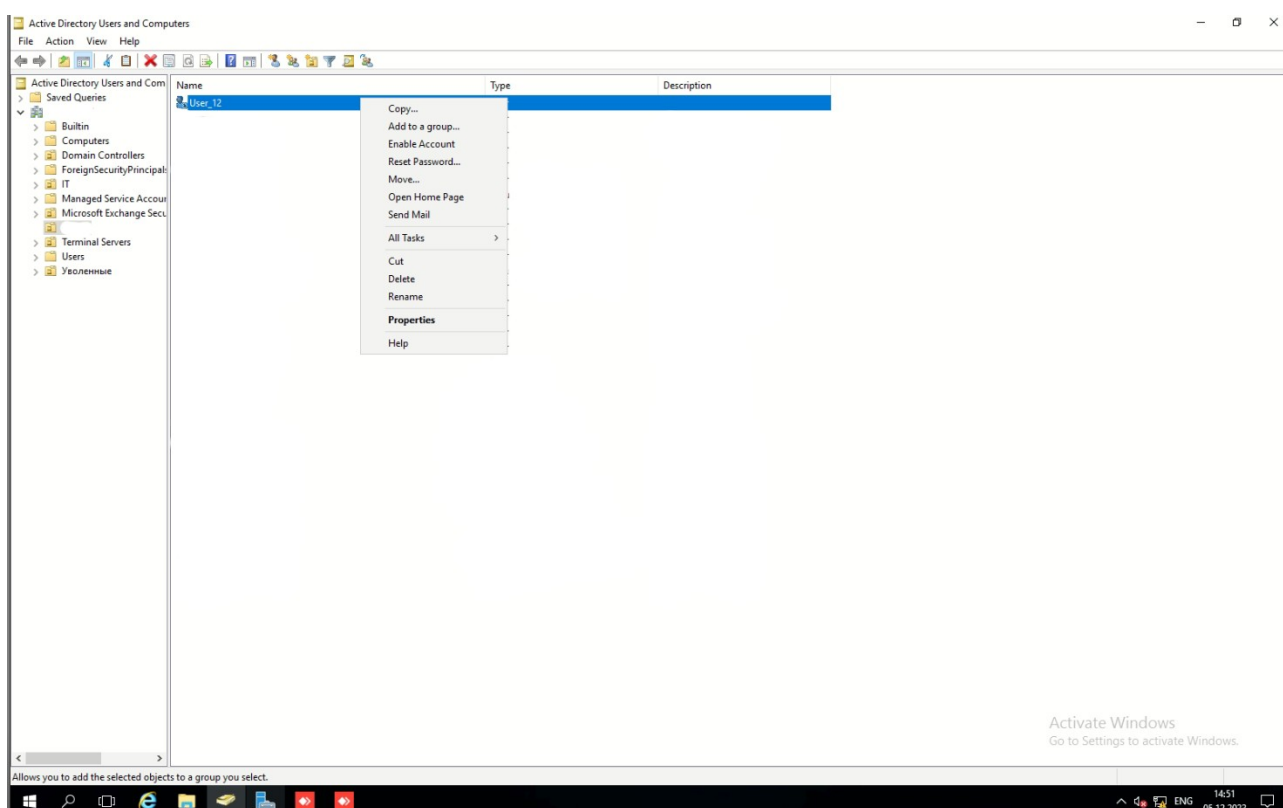
The 'New Object - User' dialog box is shown with the following details:

- Create in:** /Nerud
- Password:** [Redacted]
- Confirm password:** [Redacted]
- Options:**
  - ☒ User must change password at next logon
  - ☐ User cannot change password
  - ☐ Password never expires
  - ☐ Account is disabled
- Buttons:** < Back, Next > (highlighted), Cancel

Информация о созданном пользователе:



Копируем созданного пользователя (Copy):



Copy Object - User

Create in: [redacted]

First name: User\_121 Initials: [redacted]

Last name: [redacted]

Full name: User\_121

User logon name: User\_121 [redacted]

User logon name (pre-Windows 2000): [redacted] User\_121

< Back Next > Cancel

Вводим пароль от нового создаваемого пользователя:

Copy Object - User

Create in: [redacted]

Password: [redacted]

Confirm password: [redacted]

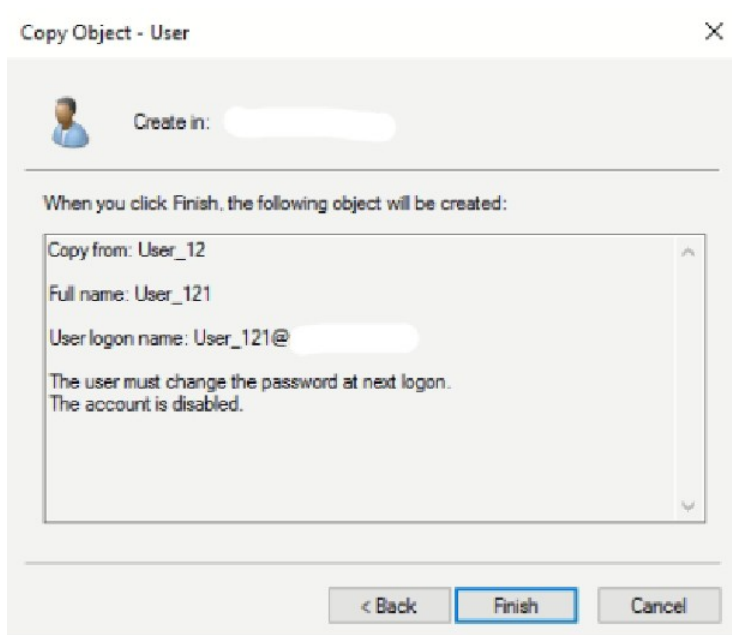
☒ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☒ Account is disabled

< Back Next > Cancel



Список созданных пользователей:

Name	Type	Description
User_12	User	
User_121	User	

### 3.2.2. Смарт-карты

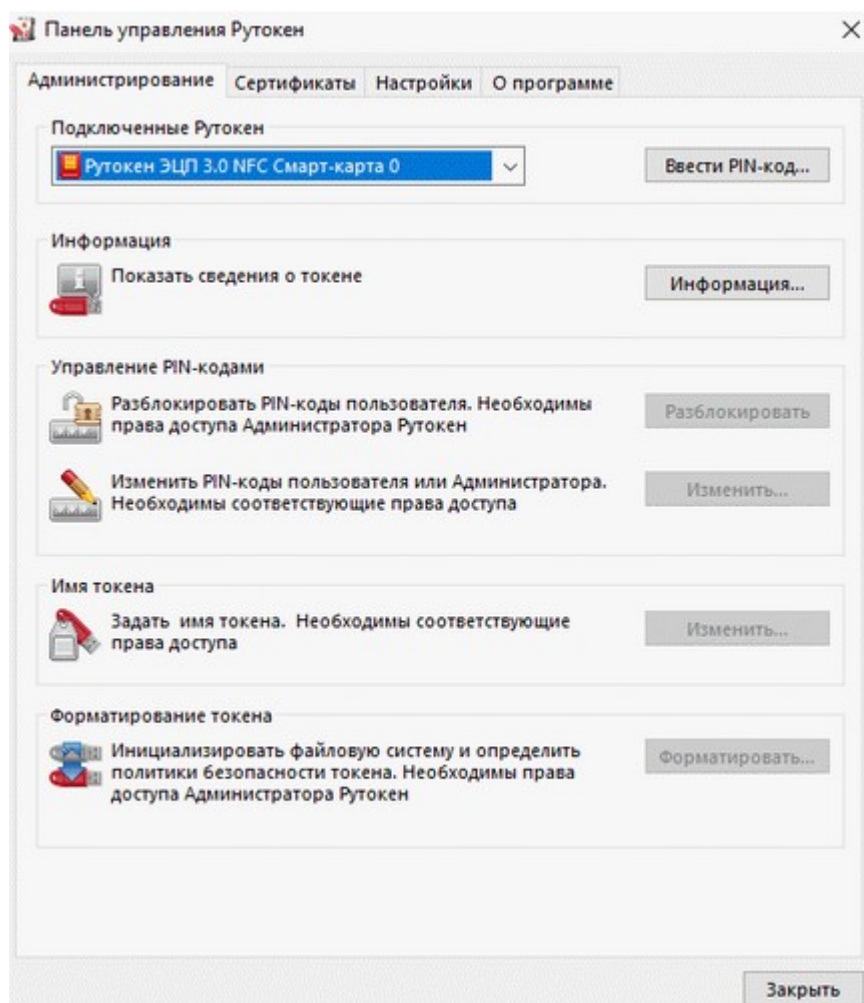
*Опишите настройку и работу со смарт-картами (локально и в домене).*

#### 3.2.2.1. Начало работы со смарт-картами и описание принципа функционирования

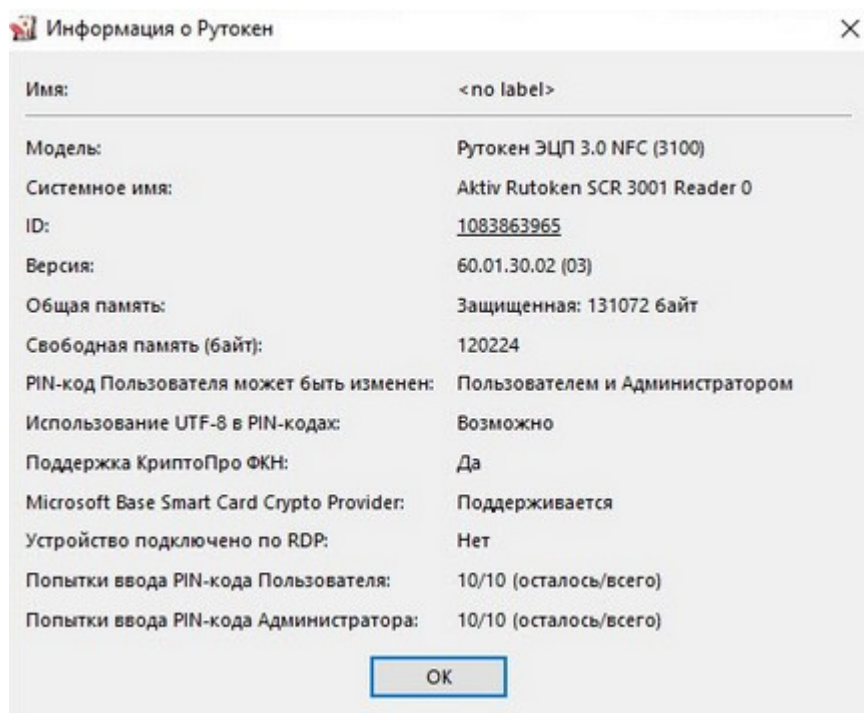
Для работы со смарткартами необходим контактный или бесконтактный считыватель для смарт-карт, и соответствующие драйвера и программное обеспечение, позволяющее взаимодействовать со смарт-картами.

Опишу на примере работы со смарт-картами Rutoken.

После установки драйверов появится специальная программа «панель управления Rutoken», с помощью которой настраивается смарт-карта.



С помощью ПО можно узнать следующую информацию об устройстве:



Перед использование некоторых смарт-карт необходимо проинициализировать ее, установив пин-код или другие параметры, например алгоритм шифрования, криптопровайдер или другую информацию.

По идентификатору смарт-карты определить, какой это пользователь.

Свободная память может быть использована для различных целей: там могут храниться хеши паролей, сертификаты, ключи шифрования, по которым можно аутентифицировать пользователя. Также внутреннее хранилище может быть использовано для хранения другой информации, например, лог последних операций по карте, идентификаторы счетов в банке и т. п.

Таким образом, смарт-карта может быть использована для следующих сценариев:

- Аутентификация пользователя. Пользователь вставляет смарт-карту в reader, вводит пин-код. Система после успешного ввода проверяет данные и дает доступ, если аутентификация пройдена.
- Хранение персональных данных. Как было сказано ранее, на смарт-карте могут храниться различные данные, к которым можно получить доступ только после ввода пин-кода.

При выполнении операции со смарт-картой информация считывается reader-ом. Для дальнейшей работы с пользователем, владельцу карты может потребоваться ввести пин-код.

Затем ПО на сервере или локально проверяет данные, необходимые для аутентификации (идентификатор, либо то, что лежит во внутреннем хранилище), и, если карта зарегистрирована и аутентификация пройдена, разрешает пользователю доступ к ресурсам.

### **3.2.2.2. Работа со смарт-картами локально**

При входе в Windows по смарт-карте, после загрузки операционной системы на экране монитора появится окно авторизации пользователя, где вместо привычного ввода имени и пароля будет предложено ввести ПИН-код подключённой к компьютеру смарт-карты.

### **3.2.2.3. Работа со смарт-картами в домене**

Для проверки подлинности смарт-карт в Active Directory необходимо правильно настроить рабочие станции Smartcard, Active Directory и контроллеры домена Active Directory. Active Directory должна доверять центру сертификации для проверки подлинности пользователей на основе сертификатов из этого ЦС. Рабочие станции smartcard и контроллеры домена должны быть настроены с правильно настроенными сертификатами.

При работе со смарт-картами в домене также при входе в систему пользователя как правило попросят ввести пин-код от смарт-карты, затем будет считан сертификат со смарт-карты, и пользователю, при успешной аутентификации и правильной настройке сервера, предоставится доступ к определенным доменным ресурсам.

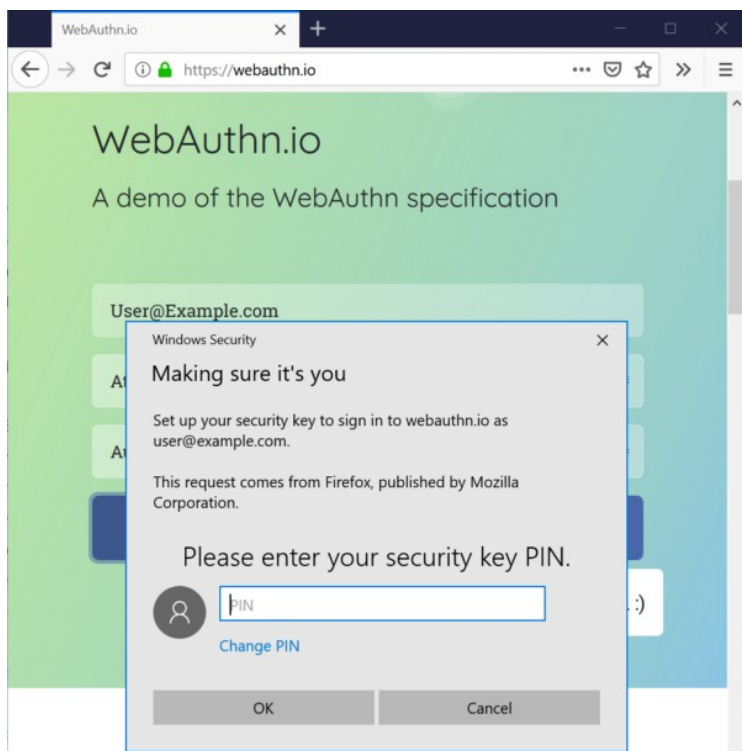
### **3.2.3. Отличия биометрической службы Windows 10**

*Опишите отличия компонентов биометрической службы Windows 10 от предыдущих версий ОС.*

В Windows был добавлен компонент Windows Hello, который обеспечивает:

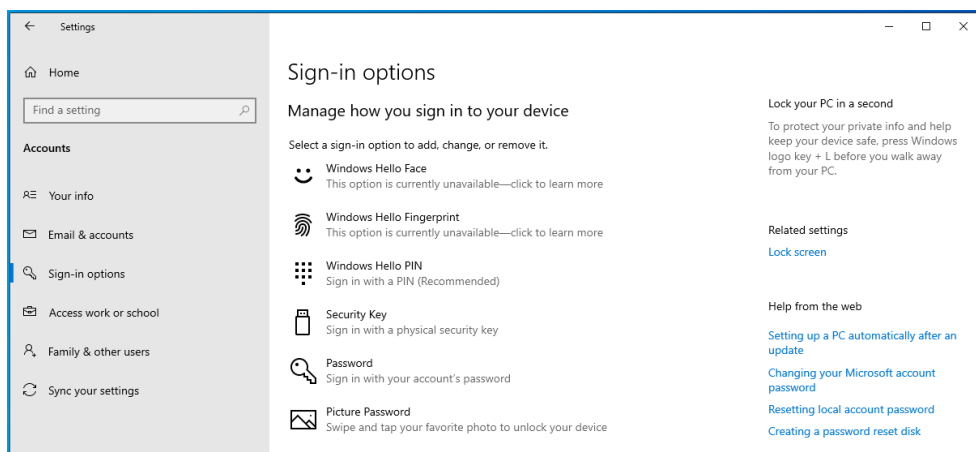
- Интеграцию с веб-сайтами и приложениями.





- Универсальную поддержку биометрических устройств. Windows Hello был реализован так, чтобы поддерживать различные биометрические устройства, обладающими функциями распознавания лиц или радужек глаза (вебкамеры), сканеры отпечатков пальцев.
- Для бизнеса реализована возможность использования Windows Hello для обеспечения двухфакторной аутентификации.

Благодаря универсальной поддержке настройки биометрики были вынесены в раздел sign-in options в настройках пользователя, в то время как в предыдущих версиях требовалось настраивать биометрику отдельно для конкретных устройств, а также устанавливать драйвера. Это было связано с тем, что в предыдущих версиях Windows основным компонентом использовался Windows Biometric Framework, который является компонентом, предоставляющим более низкоуровневые методы.



Таким образом, Windows Hello предоставляет более высокоуровневую платформу аутентификации, в то время как Windows Biometric Framework (WBF) является более низкоуровневым механизмом. Windows Hello использует WBF для обеспечения совместимости с устройствами, которые не поддерживают полный набор функций Windows Hello.

## 4. Выводы

В ходе выполнения лабораторной работы я узнал о том, как перейти в безопасный режим Windows 10, и воспользоваться им. Также узнал об UAC, и как его можно изменять. Также, при выполнении дополнительных заданий познакомился с работой со смарт-картами, воспользовался Windows Server для создания и копирования пользователя. Для выполнения анализа ознакомился с некоторыми руководящими документами ФСТЭК.