ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Информационная безопасность

Отчет по лабораторной работе №1  
«Учетные записи и авторизация в ОС MS Windows»

Выполнил:  
Студент группы №P34101

*Патутин В.М.*Преподаватель:  
*Маркина Т. А.*

Санкт-Петербург

2022

Оглавление

[**Цель работы** 3](#_Toc120559085)

[**Вариант:** 3](#_Toc120559086)

[**Программные и аппаратные средства, используемые при выполнении работы:** 3](#_Toc120559087)

[**Основная часть** 4](#_Toc120559088)

[**2.** **Создайте пользователя User\_№ варианта, входящего в группу «Пользователи». Опишите все спообы создания, а также (на примерах) возможности данного пользователя по изменению конфигурации системы (минимум 3 примера).** 4](#_Toc120559089)

[*Способ 1:* 5](#_Toc120559090)

[***Способ 2:*** 9](#_Toc120559091)

[***Способ 3:*** 11](#_Toc120559092)

[***Способ 4:*** 12](#_Toc120559093)

[***Возможности данного пользователя по изменению конфигурации системы:*** 13](#_Toc120559094)

[**3.** **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) (в отчете: подробное описание выполнения задания со скриншотами).** 15](#_Toc120559095)

[***Способ 1:*** 16](#_Toc120559096)

[***Способ 2:*** 18](#_Toc120559097)

[***Способ 3:*** 19](#_Toc120559098)

[***Возможности данного пользователя по изменению конфигурации системы:*** 23](#_Toc120559099)

[**4.** **Опишите параметры контроля учетных записей пользователей (UAC) (в отчете: перечислить параметры и дать им определение).** 24](#_Toc120559100)

[**5.** **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) (в отчете: подробное описание выполнения задания со скриншотами, анализ выполненных настроек, ответ на вопрос о невыполнении требований, анализ реализации в ОС).** 25](#_Toc120559101)

[***Возможные способы парольной защиты:*** 27](#_Toc120559102)

[***Анализ реализации механизма защиты в ОС Windows 10*** 28](#_Toc120559103)

[**Дополнительная часть** 30](#_Toc120559104)

[**1.** **Опишите создание профиля пользователя и его копирование (на основе Windows Server) (в отчете: подробное описание выполнения задания со скриншотами).** 30](#_Toc120559105)

[**2.** **Опишите настройку и работу со смарт-картами (локально и в домене) (в отчете: подробное описание выполнения задания со скриншотами).** 30](#_Toc120559106)

[**3.** **Опишите отличия компонентов биометрической службы Windows 10 от предыдущих версий ОС (в отчете: подробное описание выполнения задания со скриншотами).** 31](#_Toc120559107)

[**Вывод:** 32](#_Toc120559108)

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

# **Вариант:**

Номер варианта 22

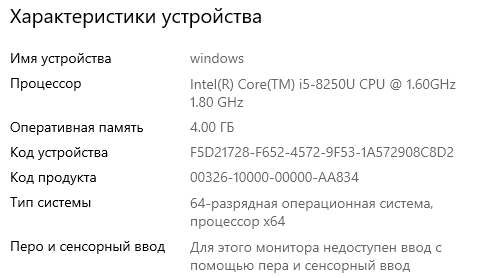
# **Программные и аппаратные средства, используемые при выполнении работы:**

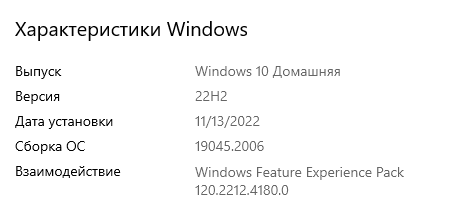
При выполнении работы было использовано ПО Oracle VM VirtualBox (ver.7.0.2).

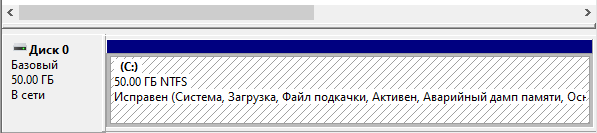


Характеристики созданной виртуальной машины:

* Операционная система Windows 10 Home (64-бит).
  + 4GB оперативной памяти
  + 50GB жесткого диска
  + Процессор: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz





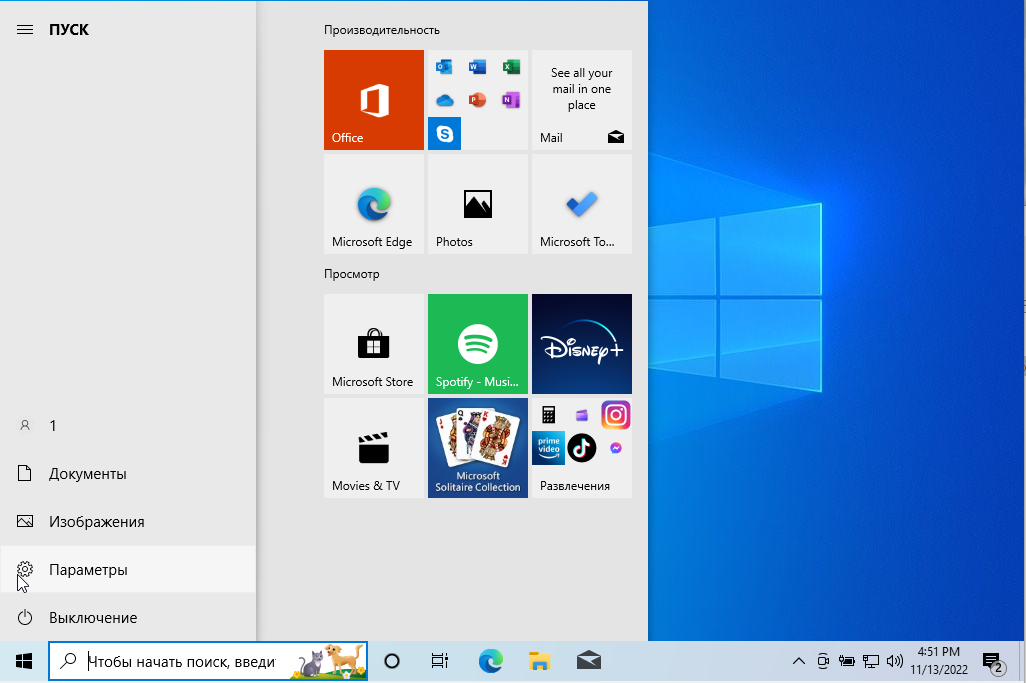


# **Основная часть**

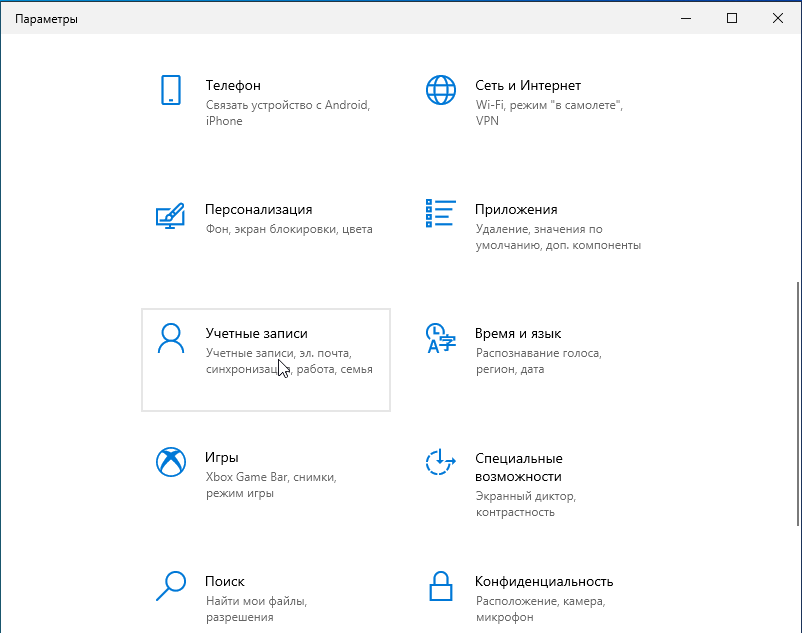
## **Создайте пользователя User\_№ варианта, входящего в группу «Пользователи». Опишите все спообы создания, а также (на примерах) возможности данного пользователя по изменению конфигурации системы (минимум 3 примера).**

### *Способ 1:*

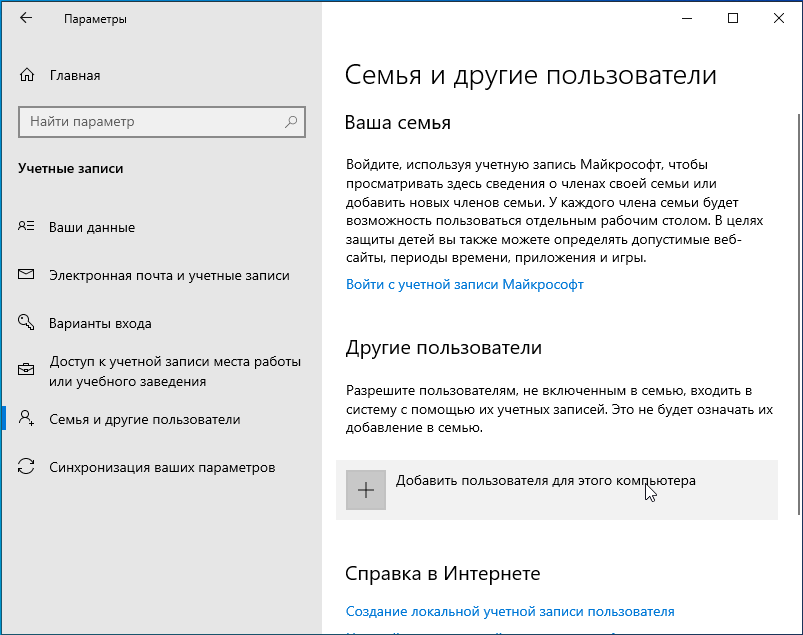
Заходим в меню “параметры”.

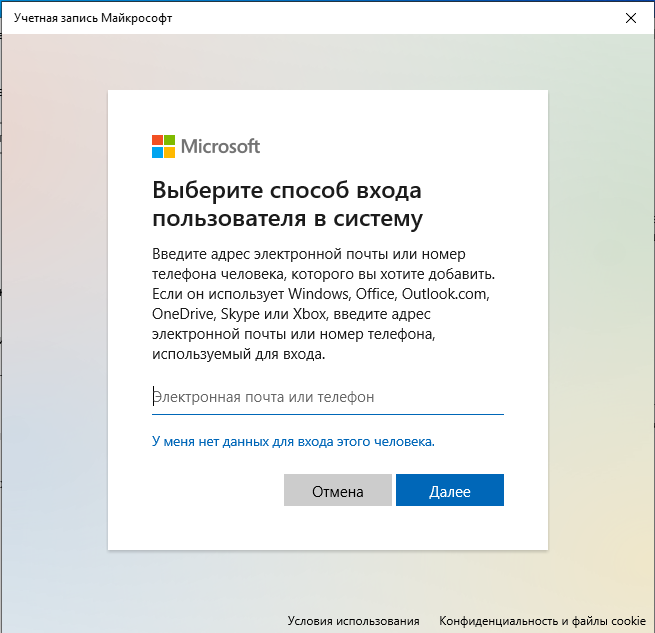


Далее выбираем “Учетные записи”, затем раздел “Семья и другие пользователи”.

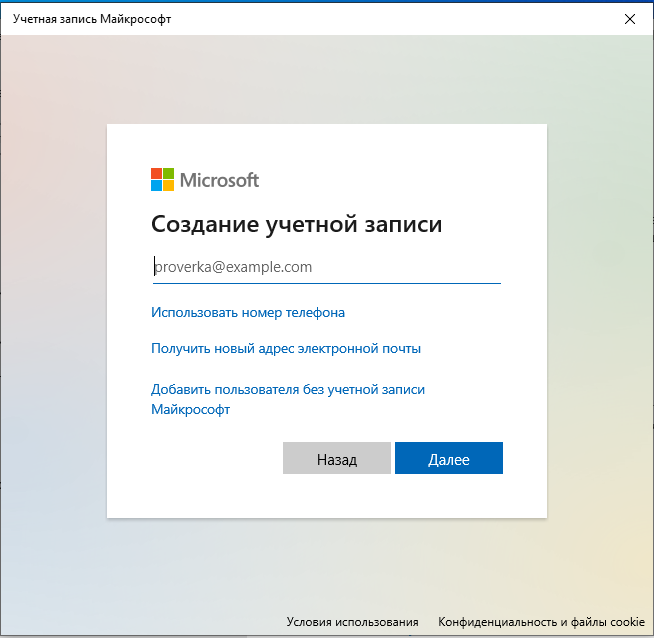


Чтобы добавить пользователя жмем на кнопку “добавить пользователя для этого компьютера”

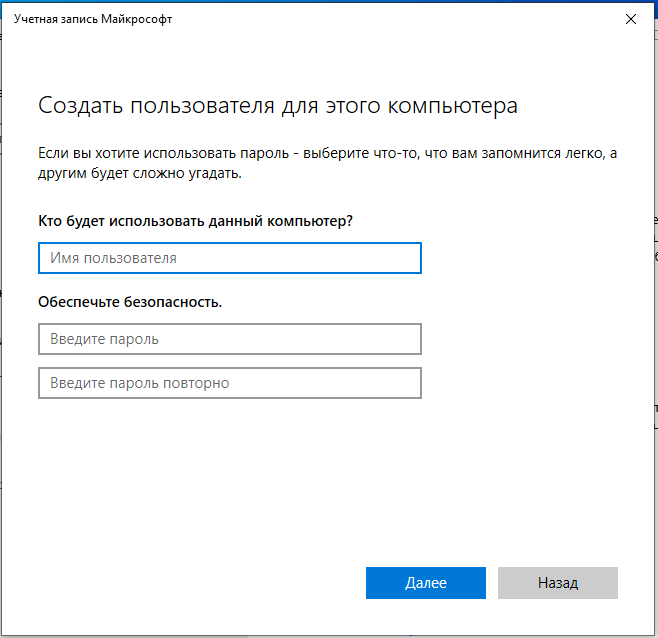
  
Есть возможность использовать учетную запись Microsoft.



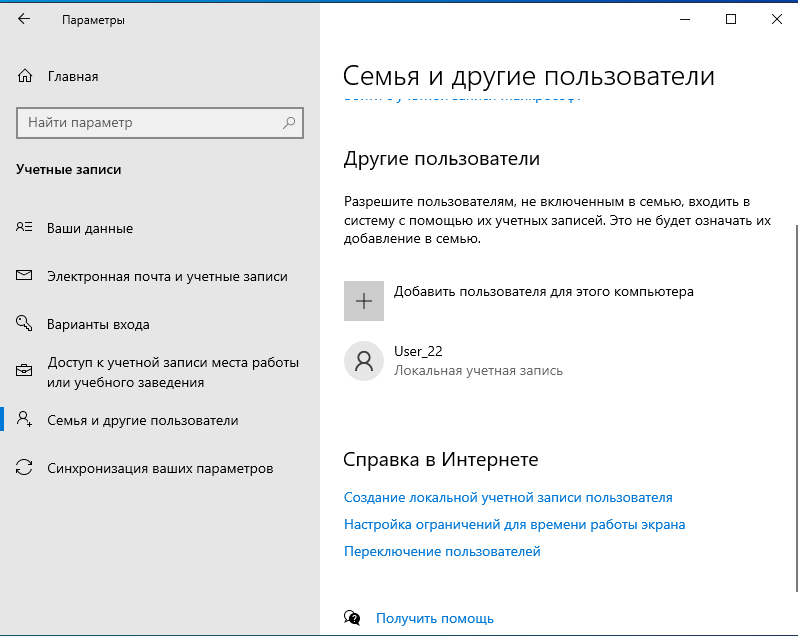
Или создать новую учетную запись



Либо создать пользователя без использования учетной записи Microsoft.

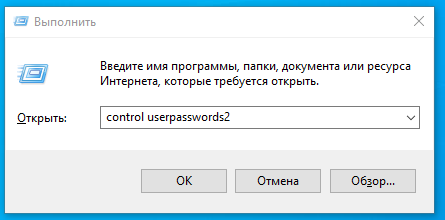


Будет создан новый пользователь

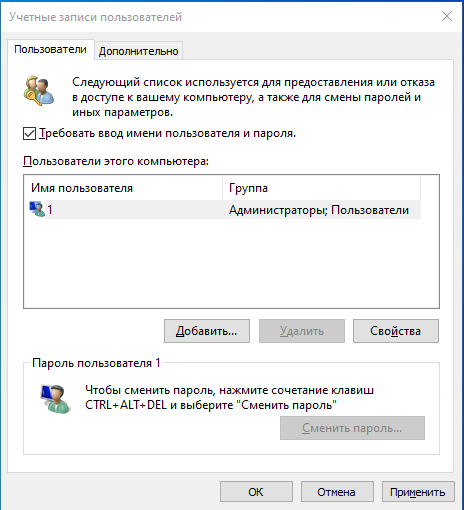


### ***Способ 2:***

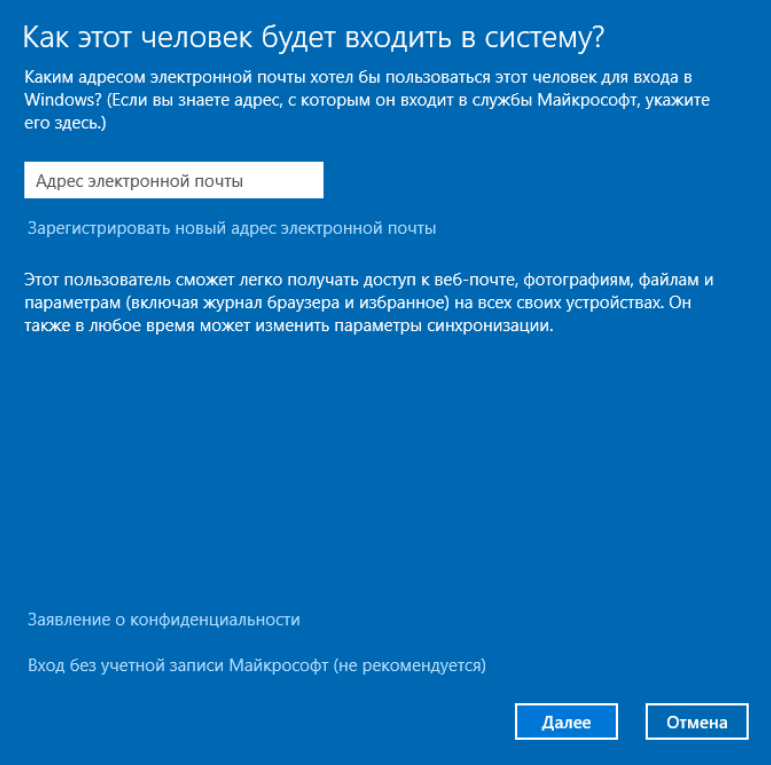
С помощью win+R открываем окно “Выполнить” и пишем:



В открывшемся окне нажимаем кнопку “Добавить”.

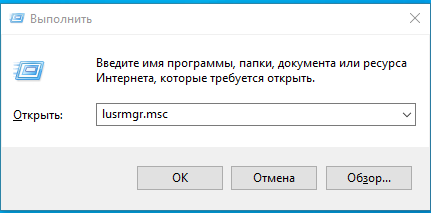


По аналогии с первый способом вводим данные нового пользователя

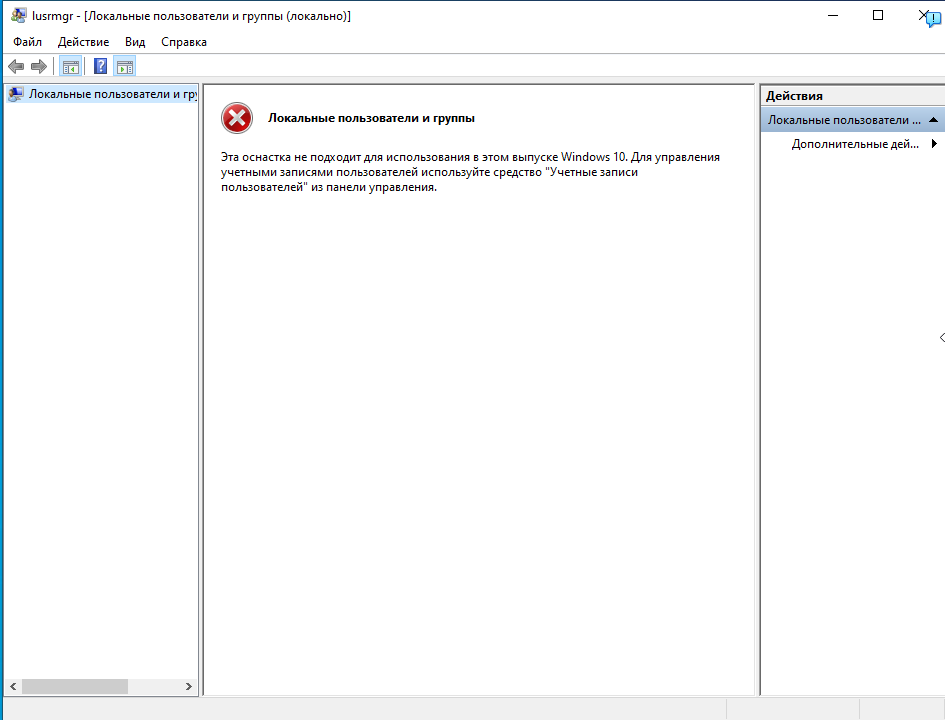


### ***Способ 3:***

С помощью win+R открываем окно “Выполнить” и пишем lusrmgr.msc , запуская от имени администратора

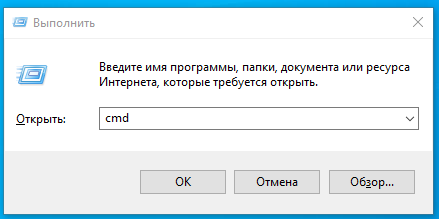


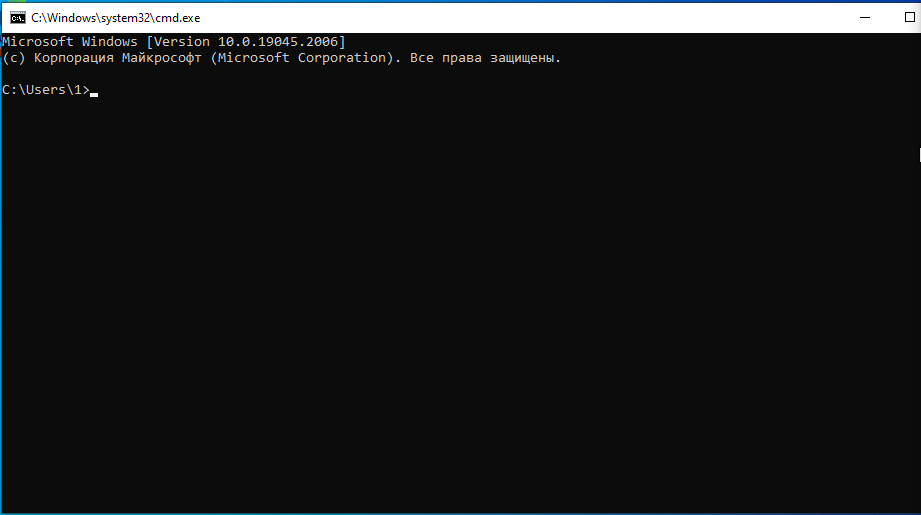
Данный способ не работает в Windows 10



### ***Способ 4:***

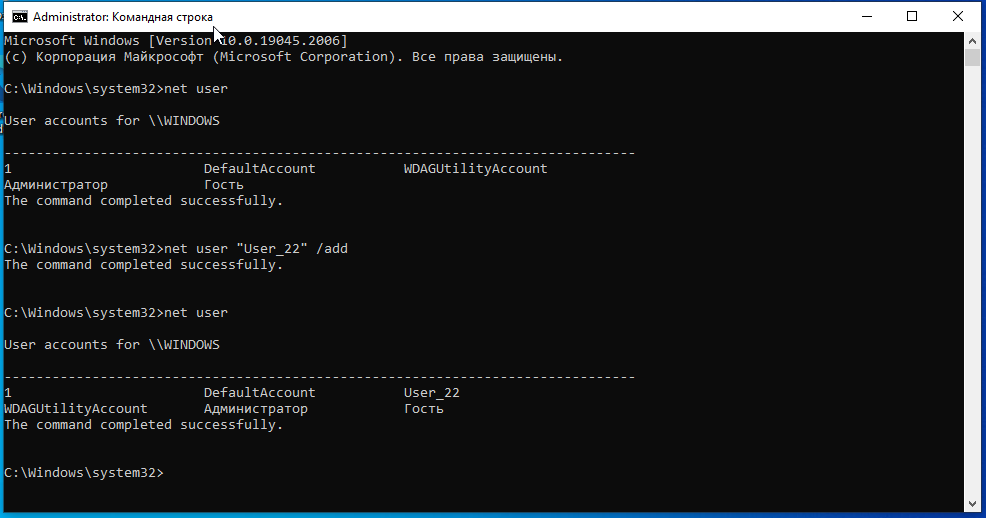
Открываем командную строку от имени администратора





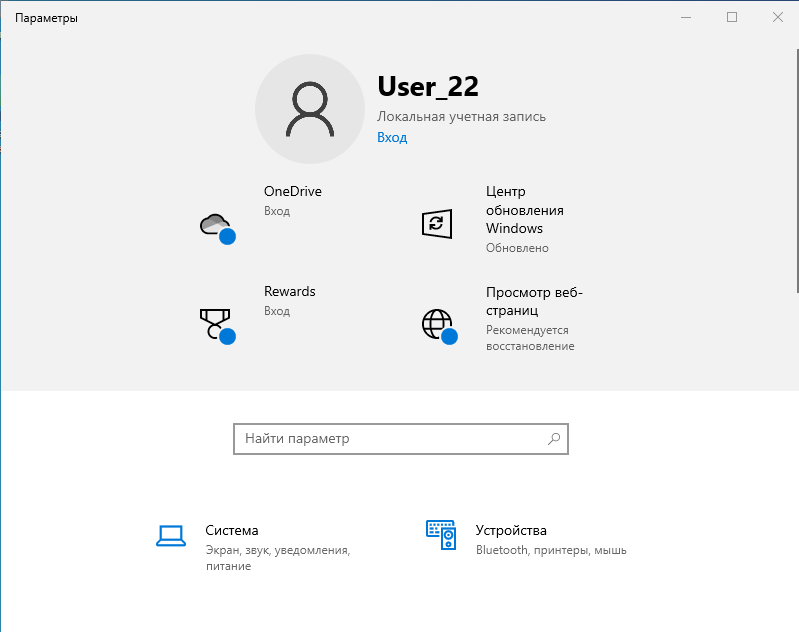
Вводим команду:

net user имя\_пользователя пароль /add

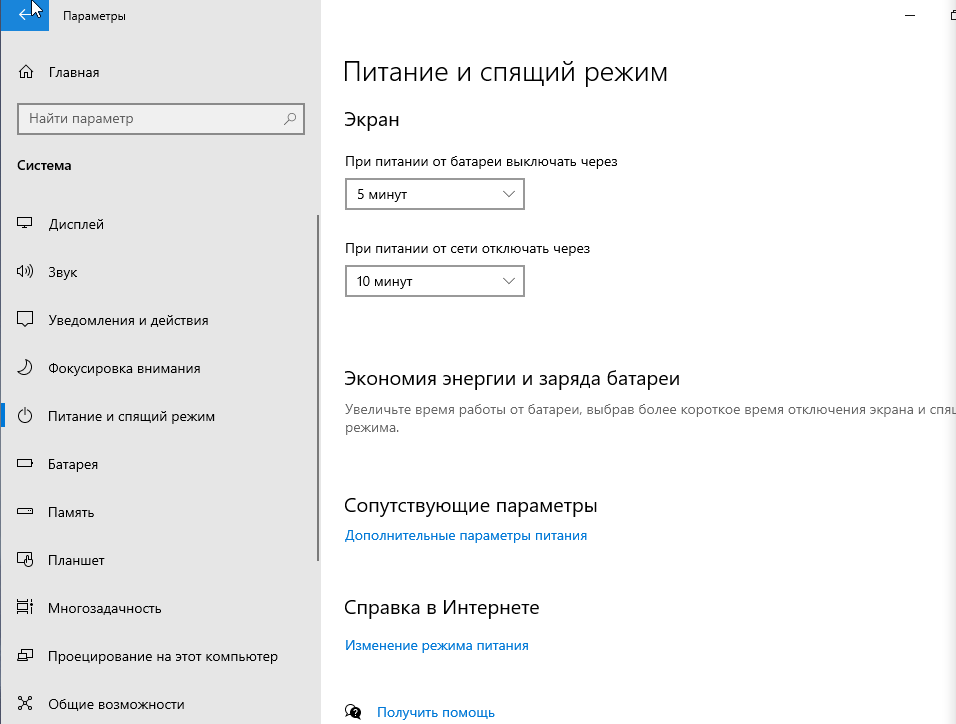


### ***Возможности данного пользователя по изменению конфигурации системы:***

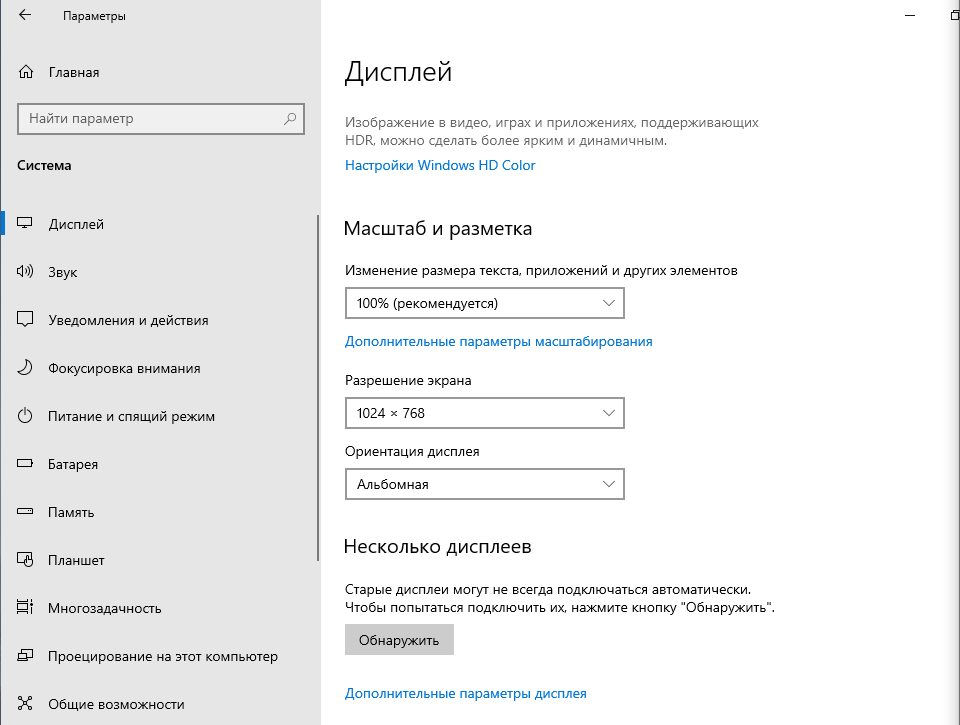
Выбираем созданного пользователя



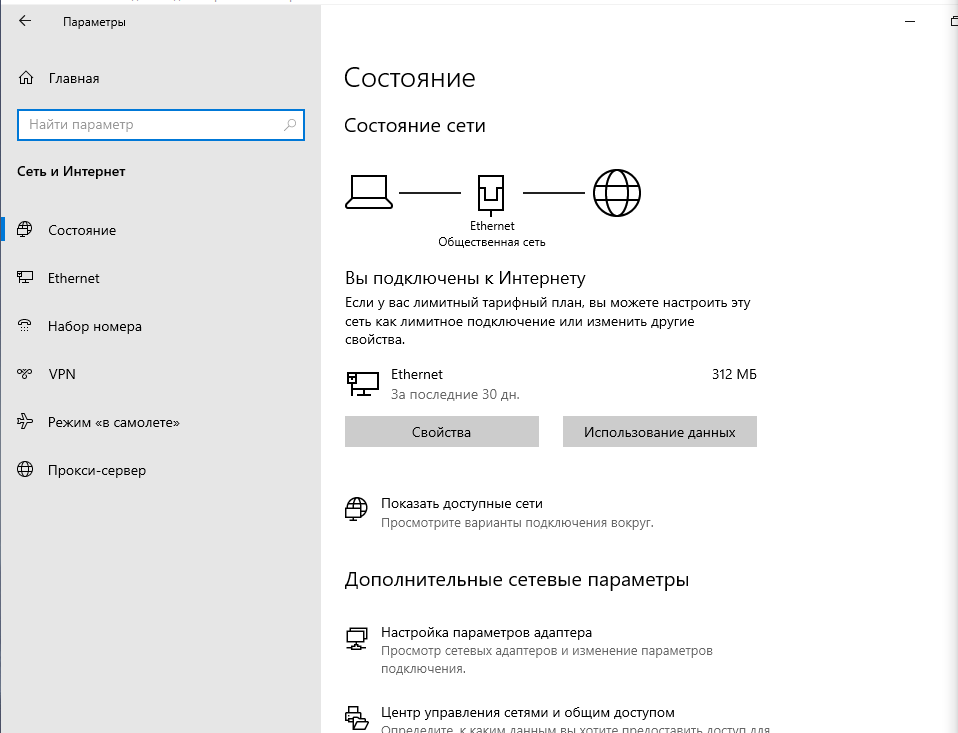
Пользователь может управлять питанием и спящим режимом



Пользователь может управлять параметрами дисплея



Пользователь может управлять подключением к сети.

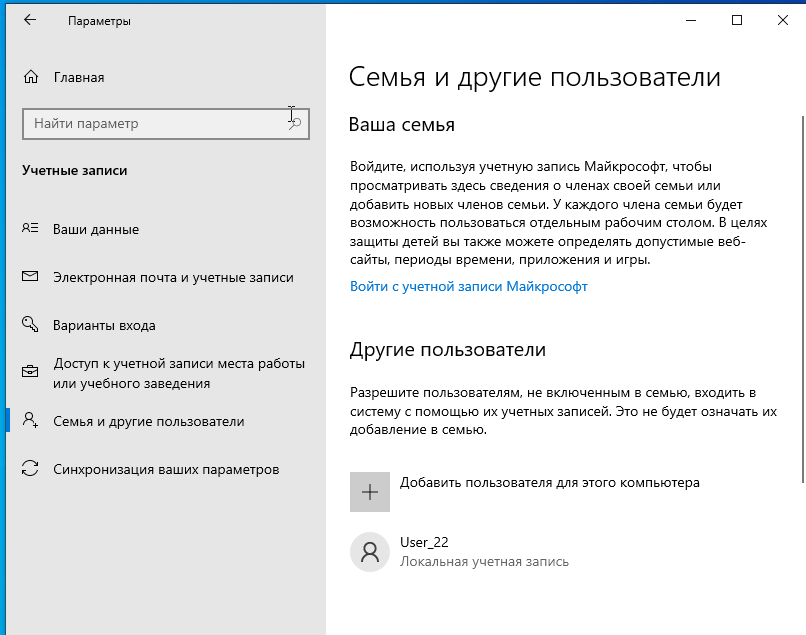


## **Создайте администратора Admin\_№ варианта, входящего в группу «Администраторы». Опишите все способы создания, а также (на примерах) ограничения данного пользователя по изменению конфигурации системы (минимум 3 примера) (в отчете: подробное описание выполнения задания со скриншотами).**

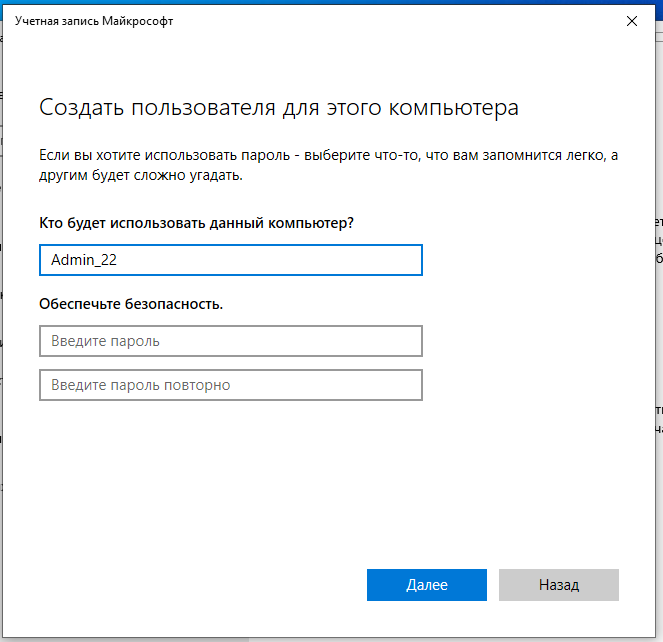
### ***Способ 1:***

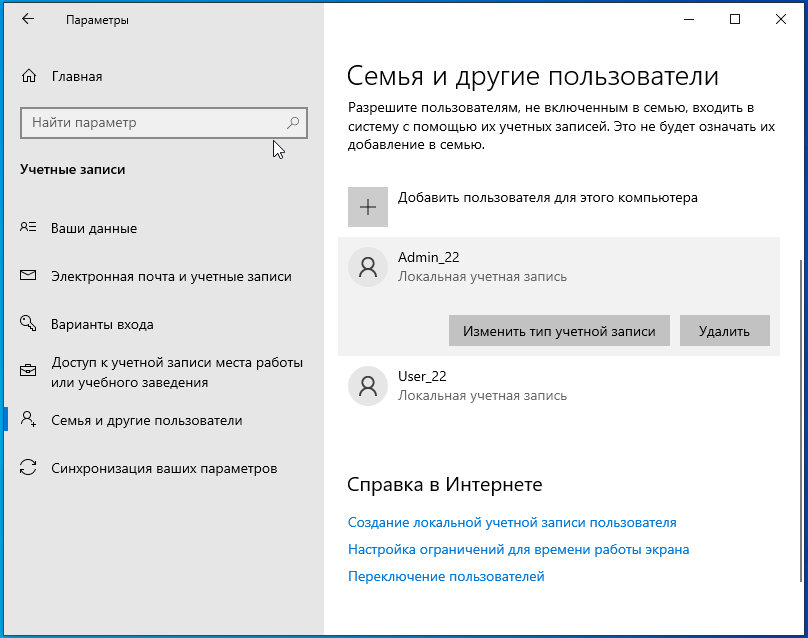
Создаем нового пользователя аналогично способу 1 пункта 2:

Заходим в параметры, далее выбираем “Учетные записи”, затем раздел “Семья и другие пользователи”.

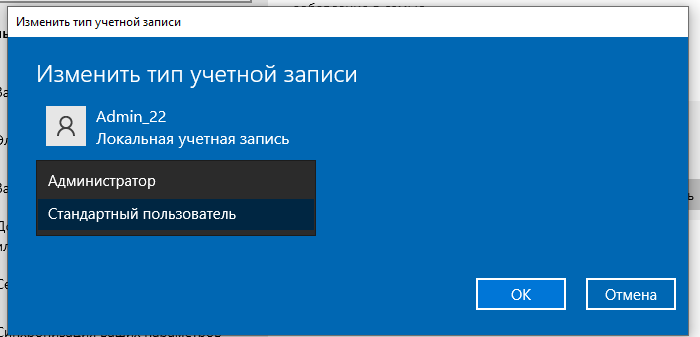


Создаем нового пользователя.

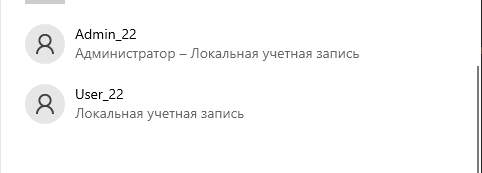


Нажимаем кнопку “Изменить тип учетной записи”  


Меняем тип учетной записи на «Администратор»

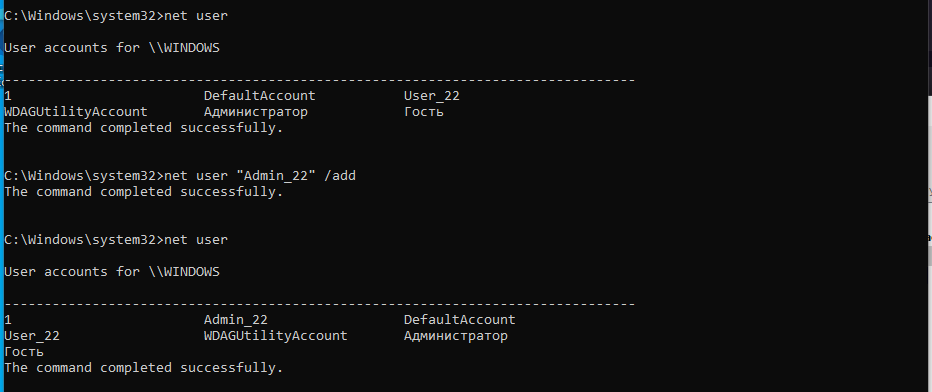


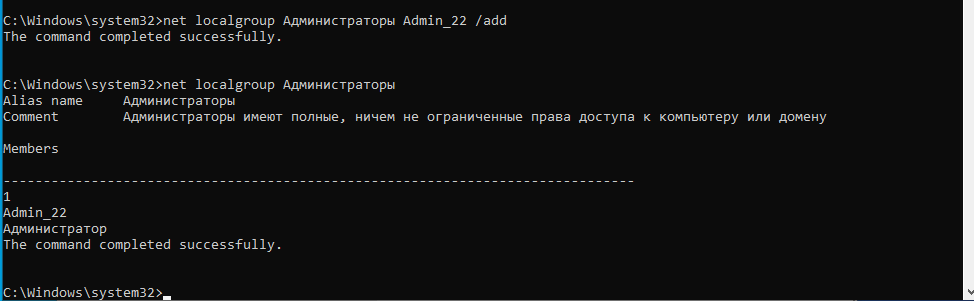
Результат



### ***Способ 2:***

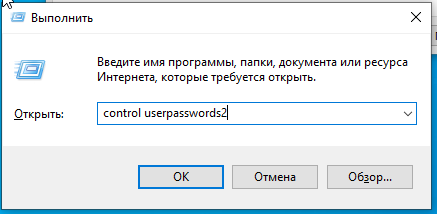
С помощью командной строки создаем пользователя

  
А затем добавляем пользователя в группу “Администраторы”.

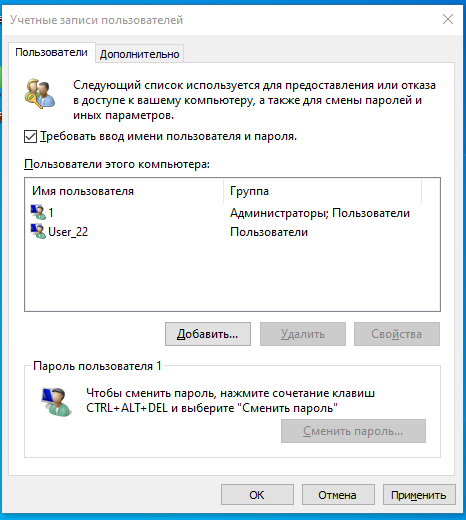


### ***Способ 3:***

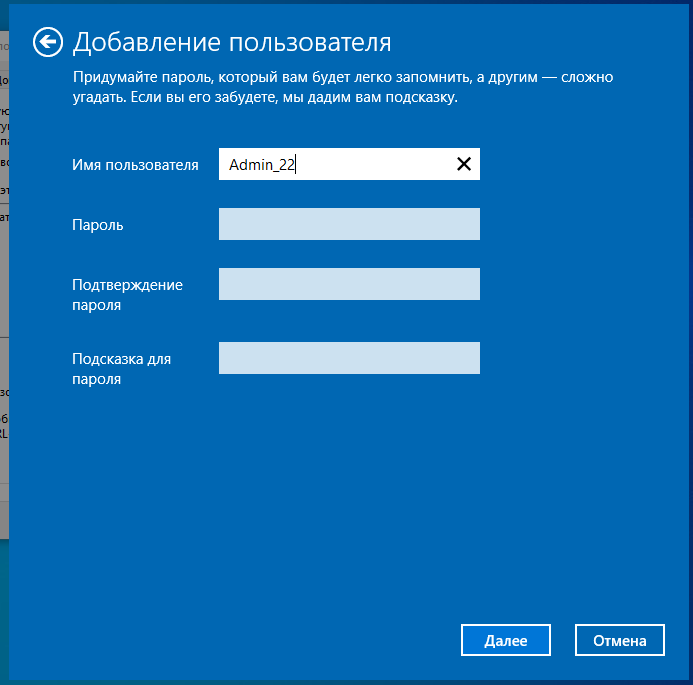
С помощью комбинации Win+R открываем окно “Выполнить” и пишем



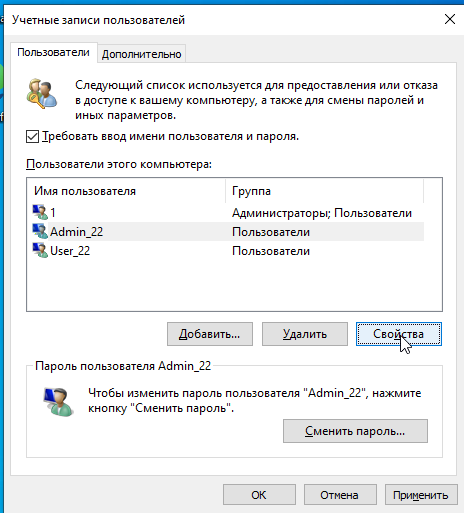
Открывается окно “Учетные записи пользователей”



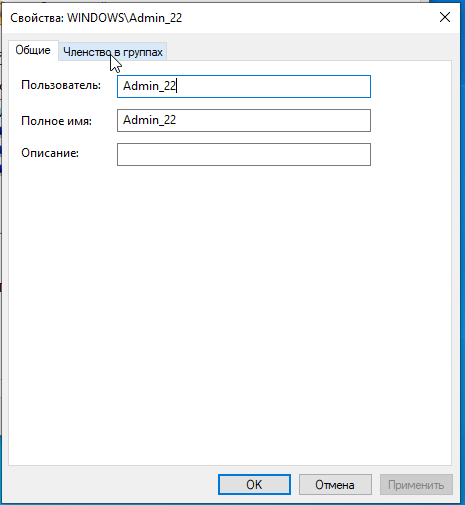
Добавляем нового пользователя.



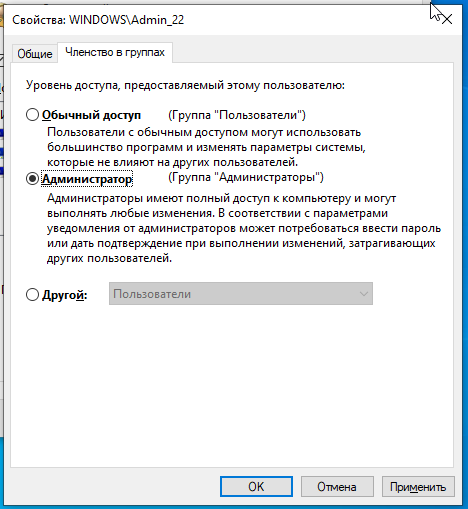
Выбираем пользователя “Admin\_22” и жмем на кнопку “Свойства”



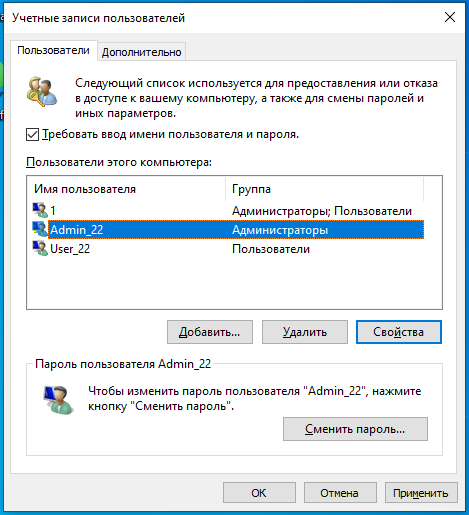
В открывшемся окне выбираем вкладку “Членство в группах



Далее выбираем пункт “администратор” и жмем “Применить”.

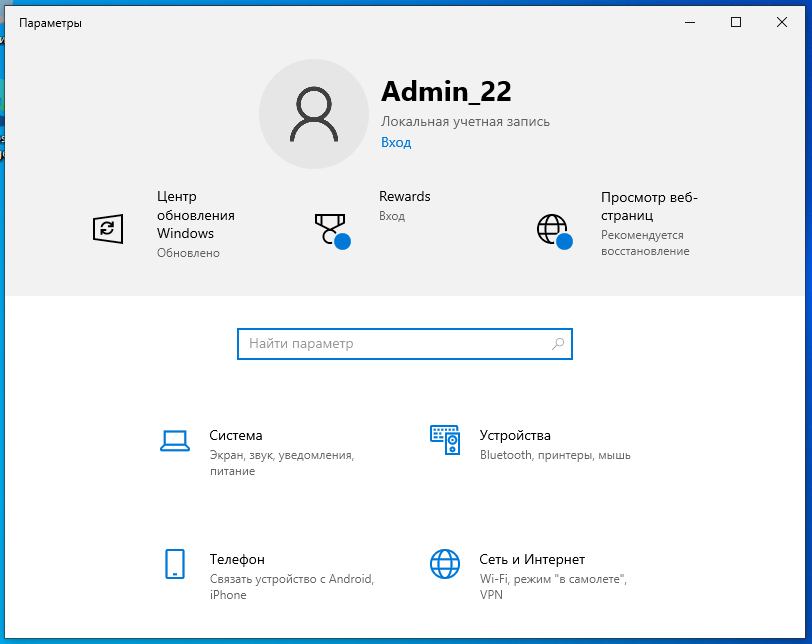


Результат:

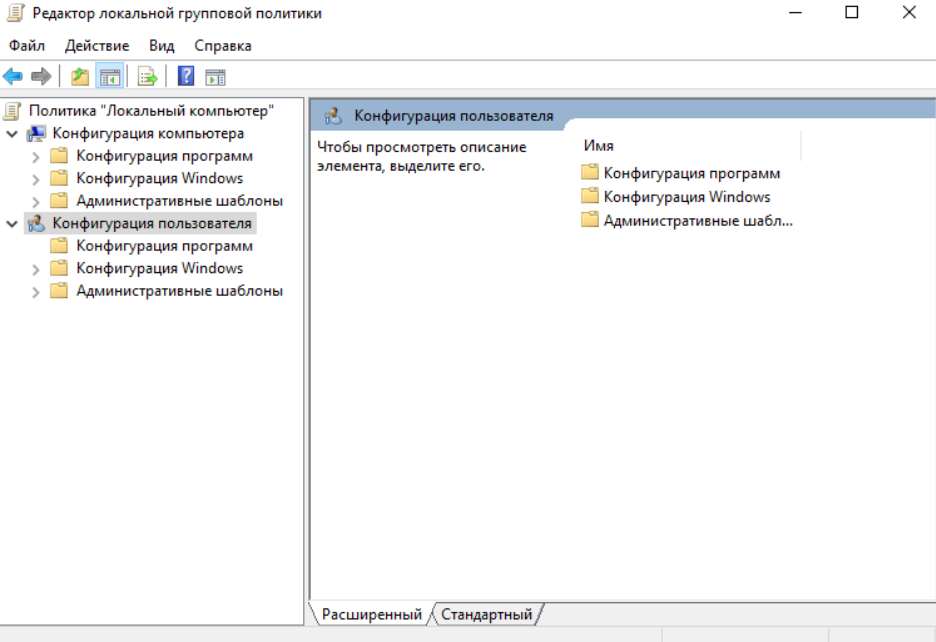


### ***Возможности данного пользователя по изменению конфигурации системы:***

Чтобы посмотреть возможности по изменению конфигурации системы заходим в учетную запись созданного администратора.



У администратора нет ограничений на изменение конфигурации системы, однако их можно добавить через редактор групповых политик.



## **Опишите параметры контроля учетных записей пользователей (UAC) (в отчете: перечислить параметры и дать им определение).**

* Не уведомлять меня - UAC отключен и не уведомляет о каких-либо изменениях в параметрах компьютера, инициированных вами или программами.
* Уведомлять только при попытках приложений внести изменения в компьютер (не затемнять рабочий стол) - отличие от предыдущего пункта в том, что рабочий стол не затемняется и не блокируется, что в некоторых случаях (вирусы, трояны) может быть угрозой безопасности.
* Уведомлять только при попытках приложений внести изменения в компьютер - этот параметр означает, что контролируются только действия программ, но не действия пользователя. Установлен по умолчанию.
* Всегда уведомлять, когда приложения пытаются установить программное обеспечение или при изменении параметров компьютера - при любом своем действии, которое может что-то изменить, а также при действиях сторонних программ пользователь будет получать уведомление об этом.

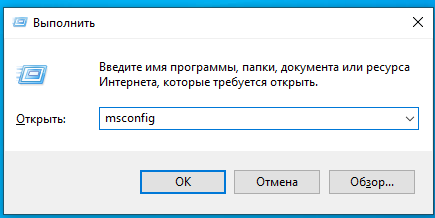
## **Выполните настройки механизмов защиты ОС Windows в соответствии с вариантом. Проанализируйте выполненные Вами настройки механизма защиты в части выполнения ими требований руководящих документов в области защиты информации. Сформулируйте, в чем не выполняются данные требования. Проанализируйте реализацию в ОС Windows механизма защиты в целом (не конкретно для Вашего примера) (в отчете: подробное описание выполнения задания со скриншотами, анализ выполненных настроек, ответ на вопрос о невыполнении требований, анализ реализации в ОС).**

**Вариант:**

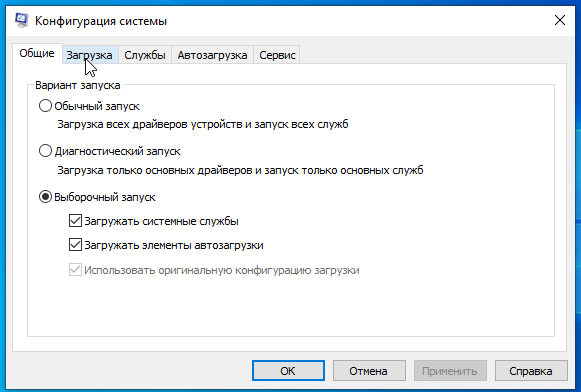
Номер варианта 22

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

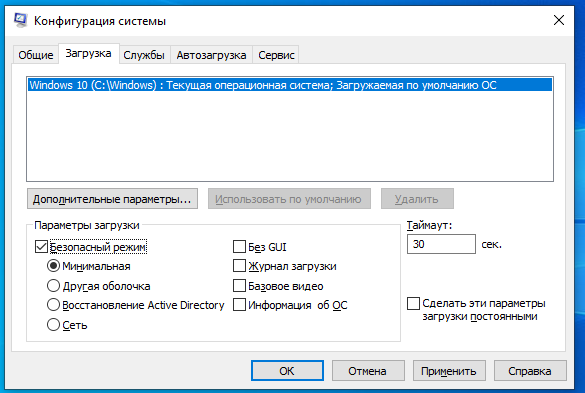
С помощью комбинации Win+R открываем окно “Выполнить” и пишем

****

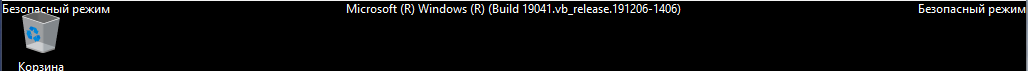
В открывавшемся окне «Конфигурация системы» перейдите на вкладку «Загрузка»

****

Выбираем ту ОС, которая должна запускаться в безопасном режиме и отмечаем пункт **«Безопасный режим»**

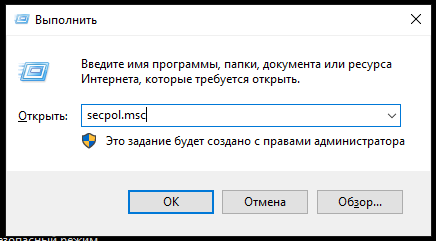
****

Нажимаем «Ок» и перезагрузите компьютер

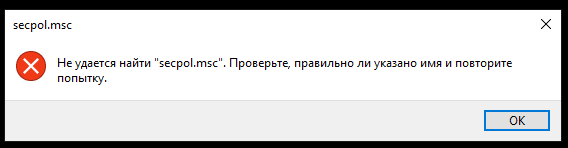
****

### ***Возможные способы парольной защиты:***

С помощью комбинации Win+R открываем окно “Выполнить” и пишем

****

Данный способ не работает в Windows 10 Home

****

Теоретически возможно выставление следующих параметров:

*Enforce password history* - хранить n предыдущих паролей чтобы запретить их повторное использование

*Maximum password age* - время  действия пароля - m дней

*Minimum password age* - минимальное время существования пароля, прежде чем пользователь сможет его изменить - x дней

*Minimum password length* - минимальная длина пароля 10 символов

*Password must meet complexity requirement* - требовать проходить проверку пароля на сложность (Не включать в пароль имя пользователя или части полного имени пользователя, включать в себя большие и маленькие буквы латинского алфавита, цифры, спецсимволы)

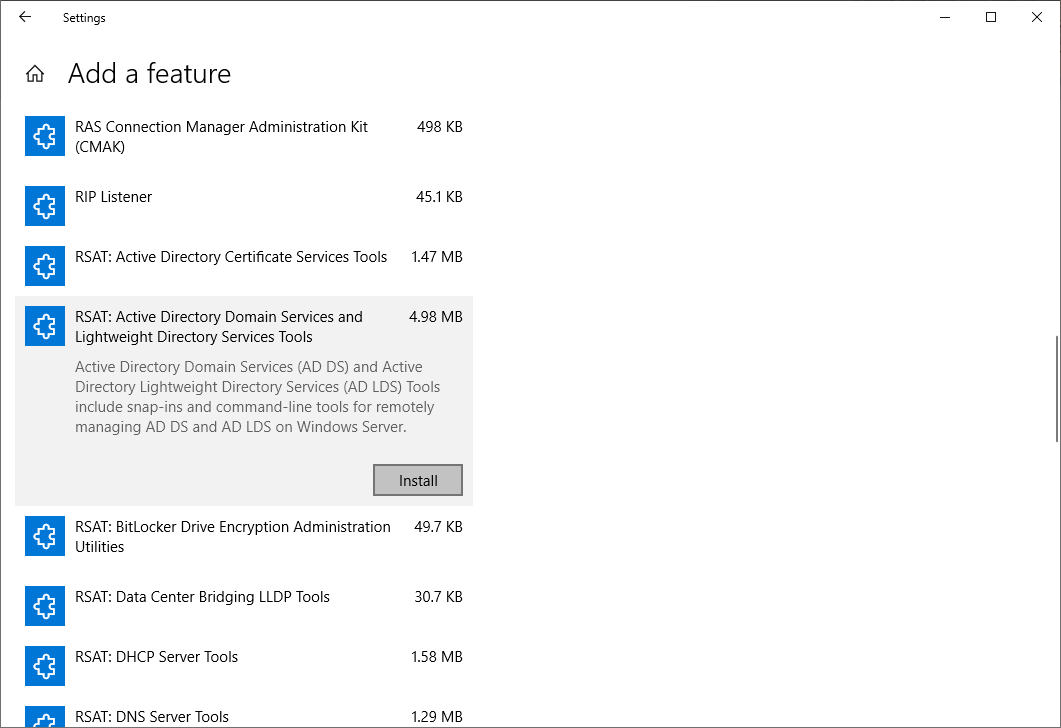
Store passwords using reversible encryption - описывает рекомендации, расположение, значения и рекомендации по безопасности для параметра политики безопасности **"Хранение паролей с использованием обратимого шифрования**"

# **Дополнительная часть**

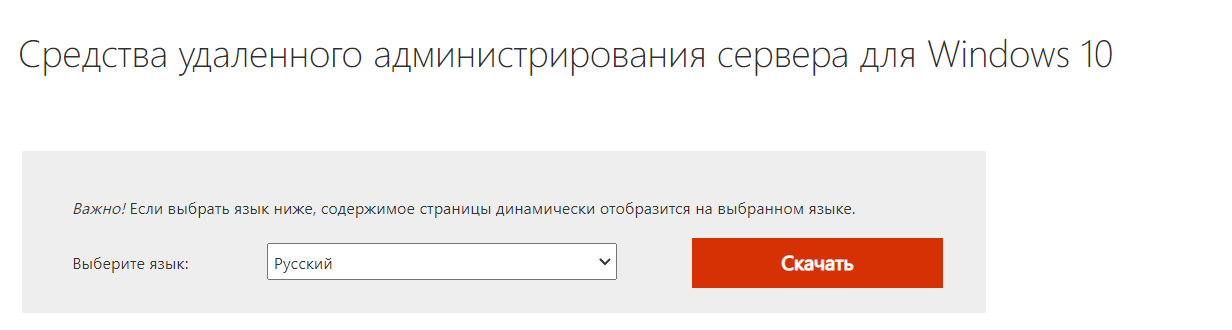
## **Опишите создание профиля пользователя и его копирование (на основе Windows Server) (в отчете: подробное описание выполнения задания со скриншотами).**

## **Опишите настройку и работу со смарт-картами (локально и в домене) (в отчете: подробное описание выполнения задания со скриншотами).**

* Получить certificate chain от CA (certification authority). Он должен быть в формате Base64 Encoded X.509.
* Добавить CA в доверенные источники в Active Directory Group Policy object. Для этого требуется скачать RSAT (Начиная с обновления Windows 10 за октябрь 2018 года, RSAT включен в комплект "Компоненты по запросу" в самой ОС Windows 10). Это средство удалённого администрирования.



В случае отсутствия можно скачать данный пакет в магазине Microsoft.



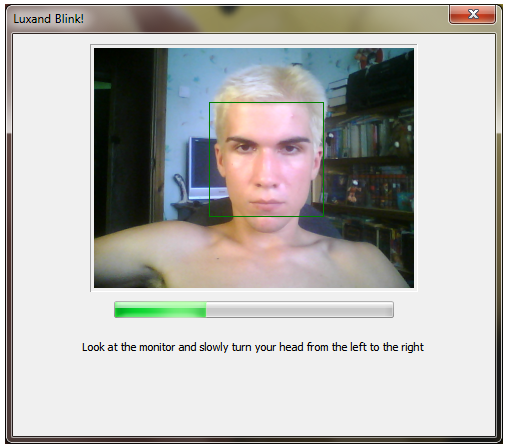
## **Опишите отличия компонентов биометрической службы Windows 10 от предыдущих версий ОС (в отчете: подробное описание выполнения задания со скриншотами).**

В Windows 10 компания Microsoft перешла на новую технологию Windows Hello. В предыдущих версиях был использован Windows Biometric Framework (WBF).

Различие между версиями:

* **Встроенная поддержка распознавания лиц**

В более ранних версиях ОС данная функция была реализована через использование сторонних программ. Например, Blink от компании Luxand для Windows Vista.

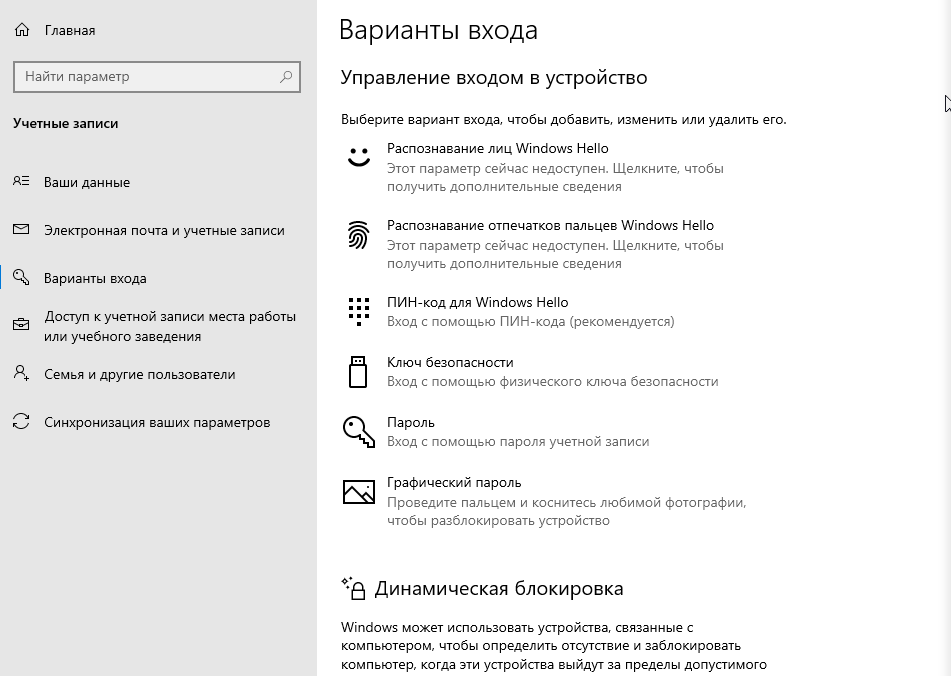


* **Объединение двухфакторной аутентификации и биометрического распознавания в одном модуле**

В первоначальной версии Windows Hello данной интеграции не было, однако её переместили позже в один модуль для удобства.

* **Процесс настройки и предустановленные пакеты**

В Windows 10 биометрические функции вынесены в раздел настройки конкретных пользователей.



В то время как настройка в предыдущих версиях была вынесена в раздел настройки конкретных устройств, требующих отдельной настройки драйверов.

Изображение выглядит как текст

Автоматически созданное описание

# **Вывод:**

В процессе выполнения данной лабораторной работы я познакомился со основами системного администрирования, используя операционную систему Windows 10. Я научился создавать учётные записи, задавая им пароль и присваивая им определенный уровень доступа (Стандартный пользователь или Администратор). Также познакомился с 4 уровнями предупреждения для пользователей.

<https://habr.com/ru/post/101692/>