

Федеральное государственное автономное образовательное
учреждение высшего образования

Университет ИТМО

Дисциплина: Информационная безопасность

Лабораторная работа Windows 1

Учетные записи и авторизация в ОС MS Windows

Вариант 12 -> 2

Работу выполнил студент группы Р34111:
Кривоносов Егор Дмитриевич

Преподаватель:
Маркина Татьяна Анатольевна

2022 г.

г. Санкт-Петербург

Содержание

| | |
|---|-----------|
| Цель работы | 3 |
| Программные и аппаратные средства, используемые при выполнении работы: | 3 |
| Основная часть | 4 |
| 1. Определить (в отчете: не надо писать определения): | 4 |
| 2. Создание пользователя | 4 |
| Вариант 2.1: | 4 |
| Вариант 2.2: | 9 |
| Вариант 2.3: | 11 |
| Вариант 2.4: | 12 |
| Вариант 2.5: | 17 |
| Возможности | 19 |
| 3. Создание администратора | 23 |
| Вариант 3.1: | 23 |
| Вариант 3.2: | 26 |
| Вариант 3.3: | 27 |
| Вариант 3.4: | 28 |
| Ограничения | 31 |
| 4. Политики UAC (User Account Control) | 34 |
| 5. Задание по варианту | 36 |
| Выполнение | 36 |
| Меры повышения надежности парольной защиты | 43 |
| Анализ реализации механизма защиты в ОС Windows 10 | 45 |
| Дополнительная часть | 47 |
| Задание 3 | 47 |
| Выполнение | 47 |
| Вывод | 49 |

Цель работы

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

Программные и аппаратные средства, используемые при выполнении работы:

Для выполнения работы было использовано ПО Oracle VM VirtualBox.
Характеристики созданной виртуальной машины:

Характеристики устройства

| | |
|-----------------------|---|
| Имя устройства | DESKTOP-DC30ER7 |
| Процессор | AMD Ryzen 5 4600H with Radeon Graphics 2.99 GHz |
| Оперативная память | 4,00 ГБ |
| Код устройства | 08343D81-55F0-4E98-8B53-80834E7D1A69 |
| Код продукта | 00330-80000-00000-AA178 |
| Тип системы | 64-разрядная операционная система, процессор x64 |
| Перо и сенсорный ввод | Для этого монитора недоступен ввод с помощью пера и сенсорный ввод |

Основная часть

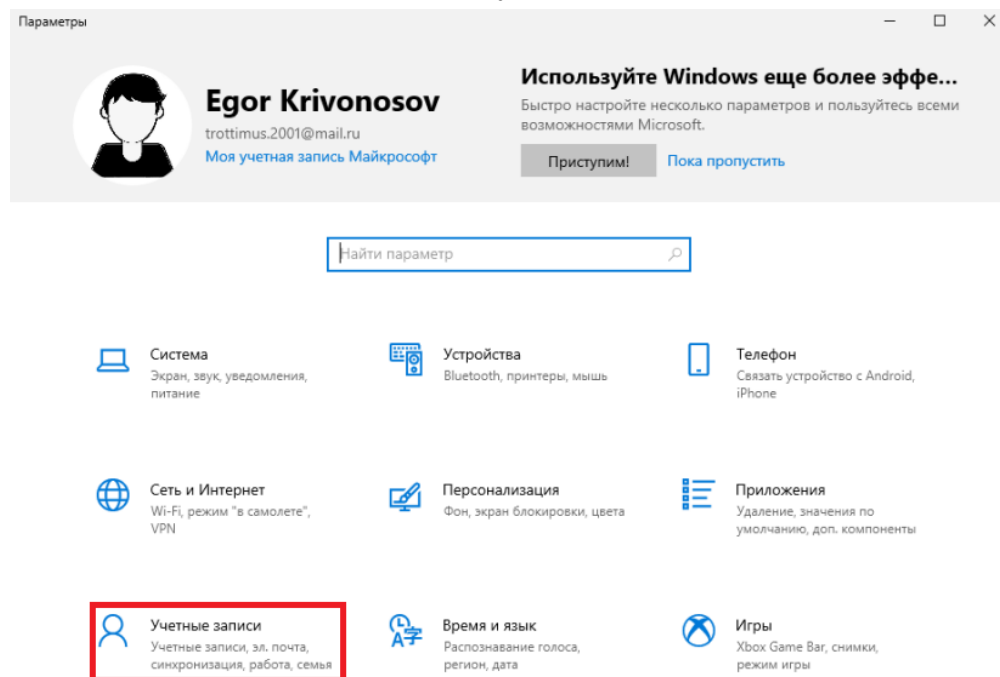
1. Определить (в отчете: не надо писать определения):

- 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),
- объект доступа,
- субъект доступа,
- олицетворение (impersonation),
- список контроля доступа (ACL - Access Control List),
- учетная запись,
- домен.

2. Создание пользователя

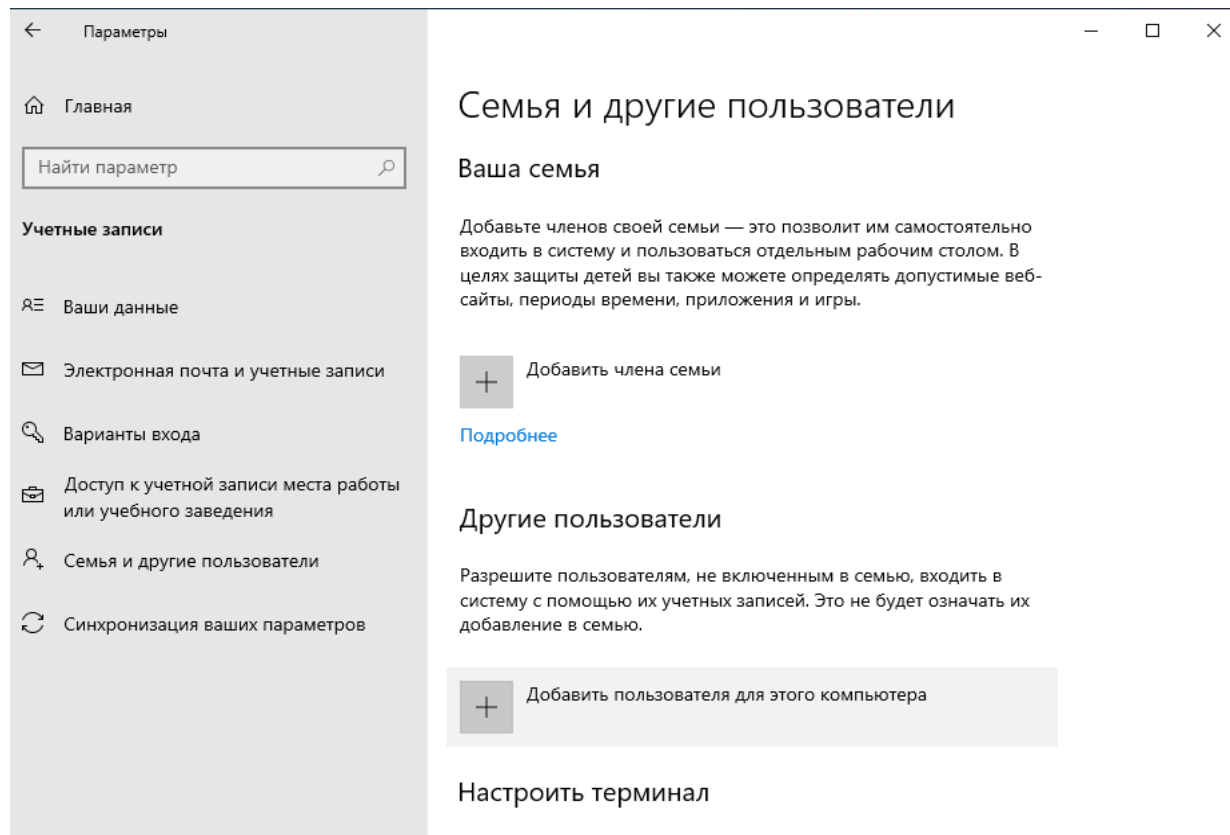
Вариант 2.1:

Откроем “**Параметры**” и выберем пункт “**Учетные записи**”



Выбрать пункт: **Семья и другие пользователи**


Выбрать пункт: **Добавить пользователя для этого компьютера**



Выбрать пункты: **У меня нет данных для входа этого человека**
Затем: **Добавить пользователя без учетной записи Майкрософт**

Учетная запись Майкрософт





Выберите способ входа пользователя в систему

Введите адрес электронной почты или номер телефона человека, которого вы хотите добавить. Если он использует Windows, Office, Outlook.com, OneDrive, Skype или Xbox, введите адрес электронной почты или номер телефона, используемый для входа.


[У меня нет данных для входа этого человека.](#)

ОтменаДалее

[Условия использования](#) [Конфиденциальность и файлы cookie](#)

Учетная запись Майкрософт





Создание учетной записи

[Использовать номер телефона](#)

[Получить новый адрес электронной почты](#)

[Добавить пользователя без учетной записи Майкрософт](#)

НазадДалее

[Условия использования](#) [Конфиденциальность и файлы cookie](#)

Затем вводим все необходимые данные для учетной записи и нажимаем: **Далее**

Учетная запись Майкрософт



Создать пользователя для этого компьютера

Если вы хотите использовать пароль - выберите что-то, что вам запомнится легко другим будет сложно угадать.

Кто будет использовать данный компьютер?

User_2

Обеспечьте безопасность.

••••

••••

В случае, если вы забыли свой пароль

В каком городе вы родились?

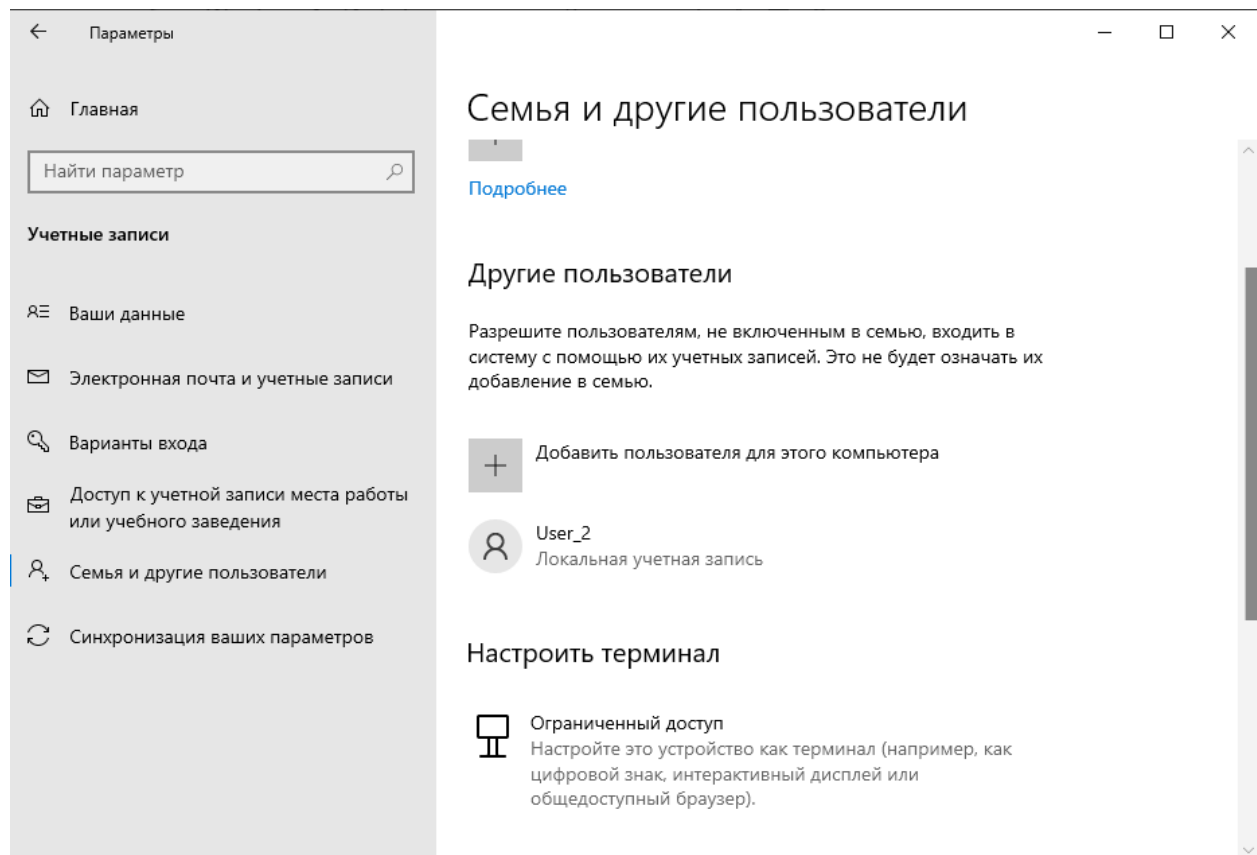


1

Далее

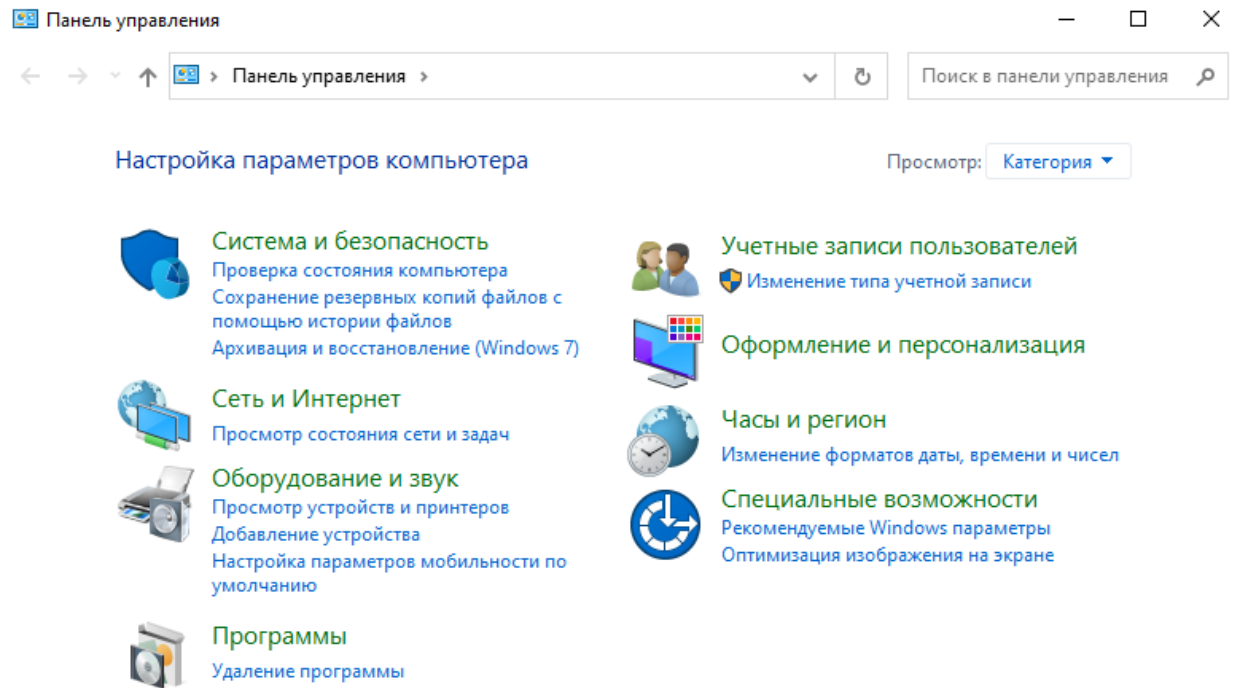
Назад

После чего создается пользователь



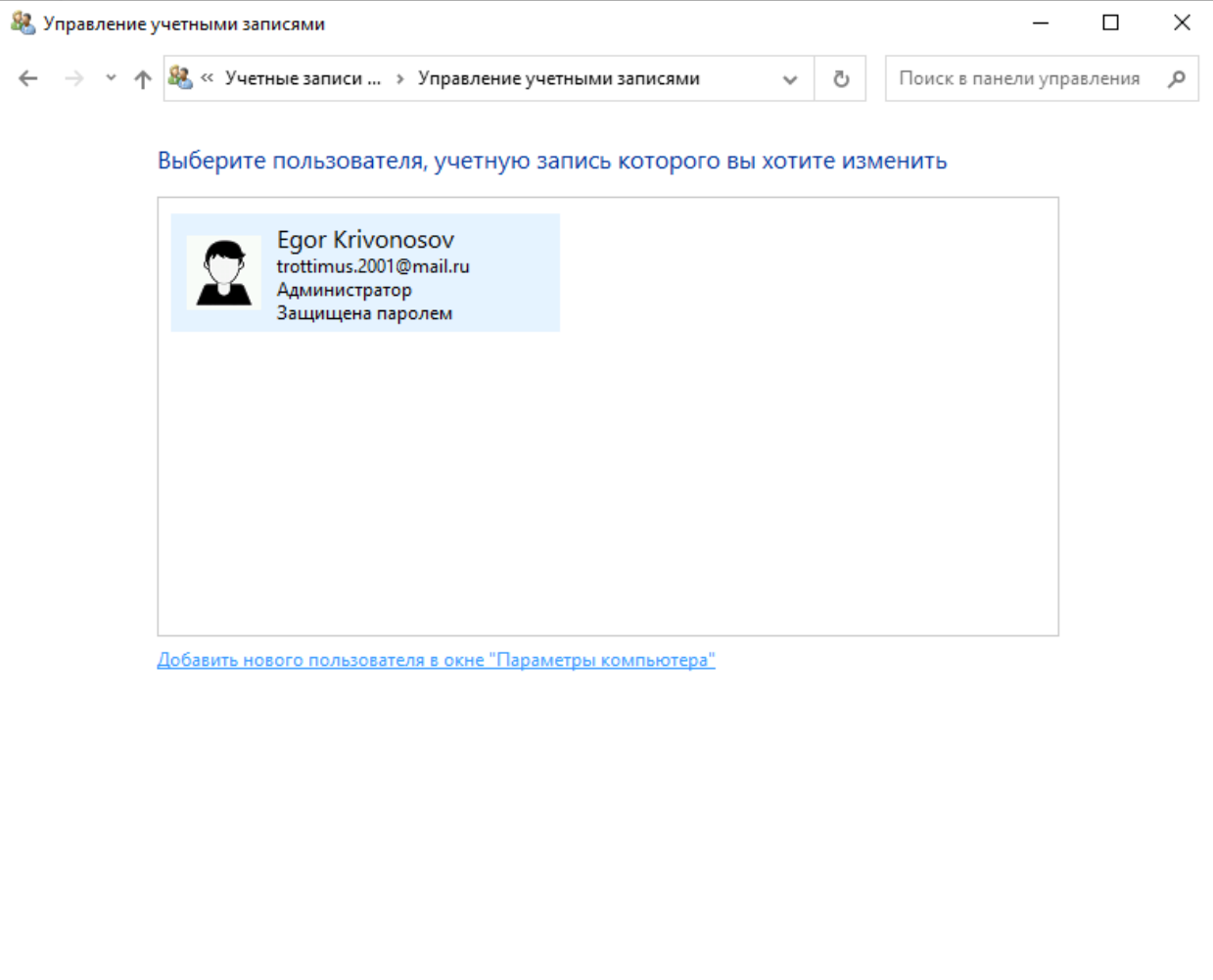
Вариант 2.2:

Открываем “Панель управления” и выбираем пункт “Изменение типа учетной записи”.



Выбираем пункт: **Добавить нового пользователя в окне параметры “Параметры компьютера”**

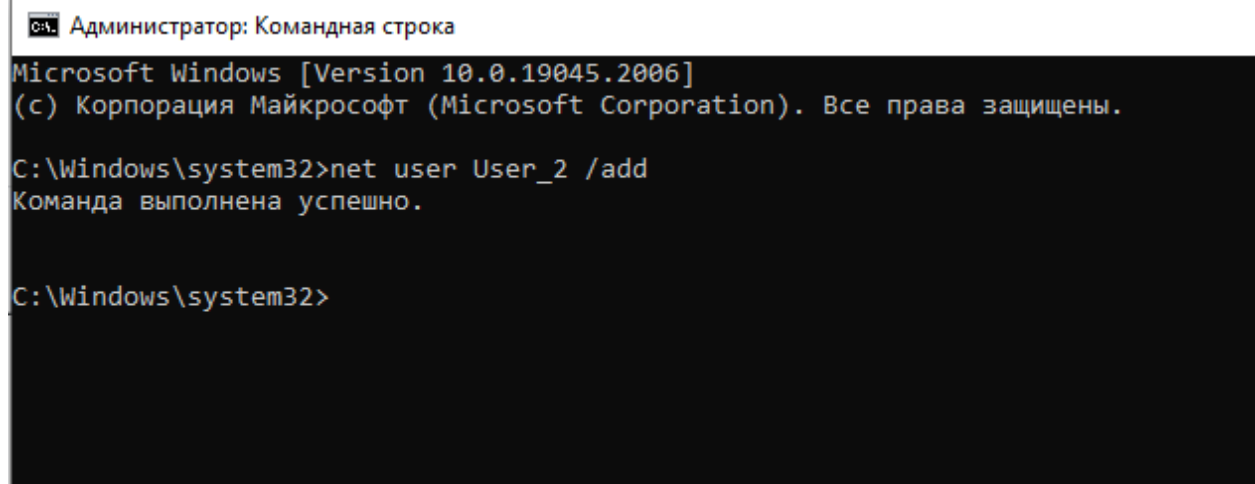
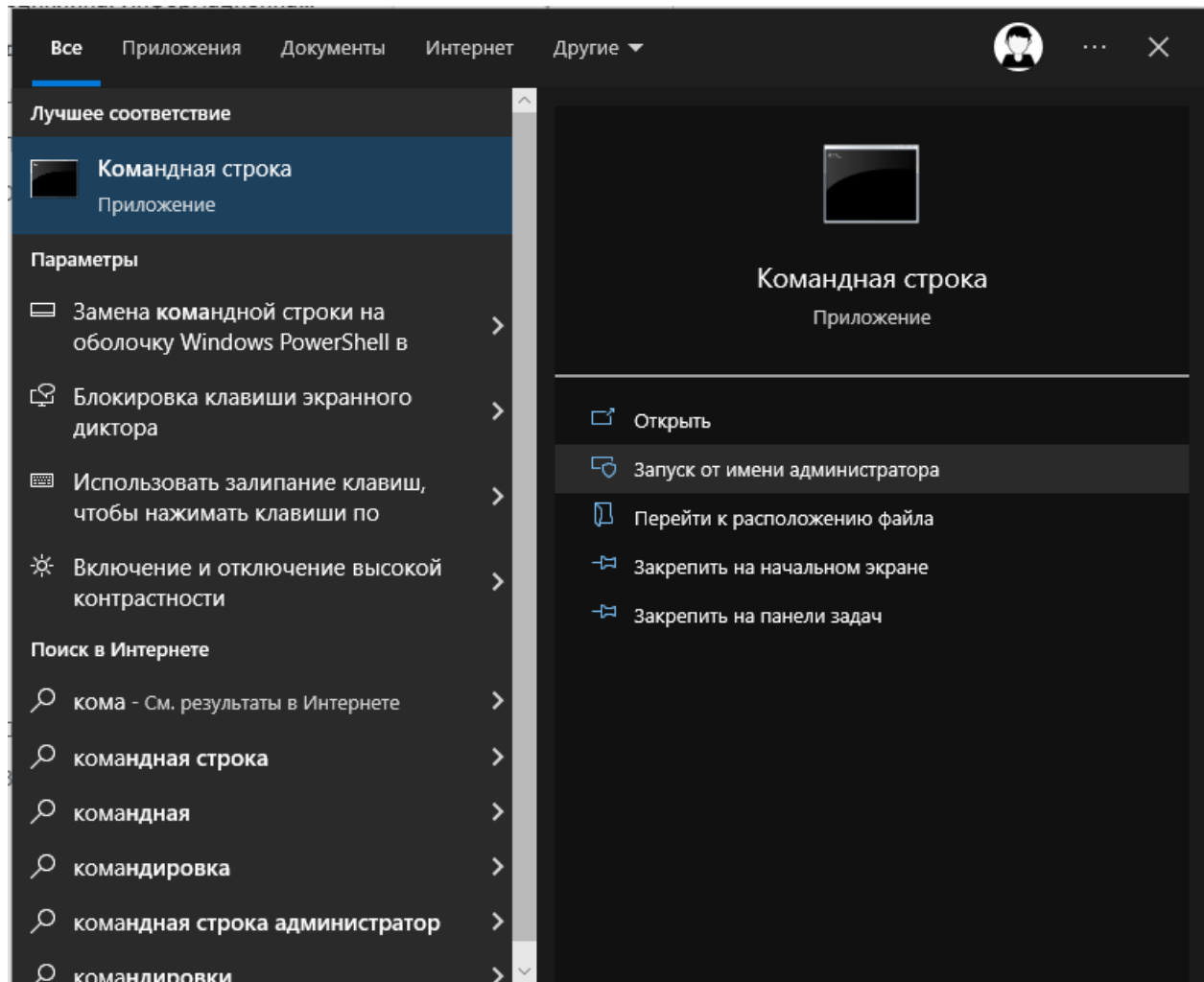
Затем повторяем те же самые действия, как и в Вариант 2.1



Вариант 2.3:

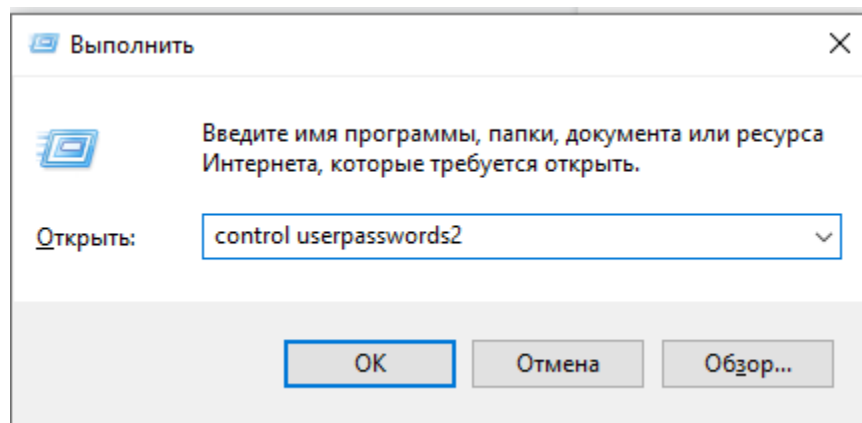
Запускаем “Командная строка” от имени администратора.

Вводим команду: `net user User_2 /add`

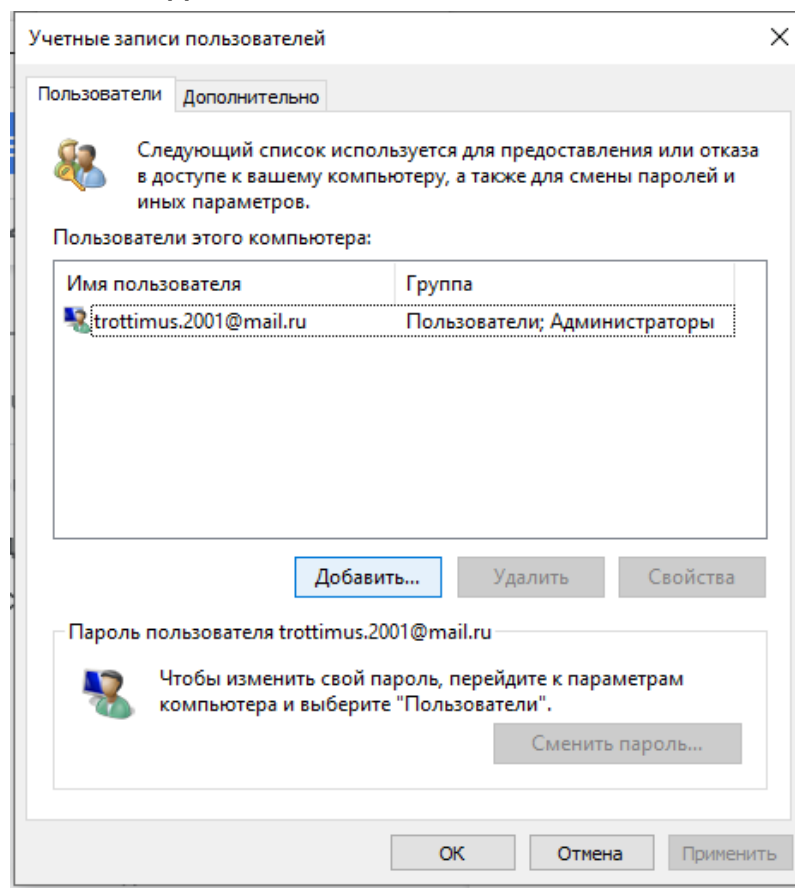


Вариант 2.4:

Открываем окно **“Выполнить”** например через сочетание клавиш: **Win + R**
Вводим в появившейся строке: **control userpasswords2**



Нажимаем: **Добавить...**



Выбираем пункт: **Вход без учетной записи Майкрософт (не рекомендуется)**

Как этот человек будет входить в систему?

Каким адресом электронной почты хотел бы пользоваться этот человек для входа в Windows? (Если вы знаете адрес, с которым он входит в службы Майкрософт, укажите его здесь.)

[Зарегистрировать новый адрес электронной почты](#)

Этот пользователь сможет легко получать доступ к веб-почте, фотографиям, файлам и параметрам (включая журнал браузера и избранное) на всех своих устройствах. Он также в любое время может изменить параметры синхронизации.

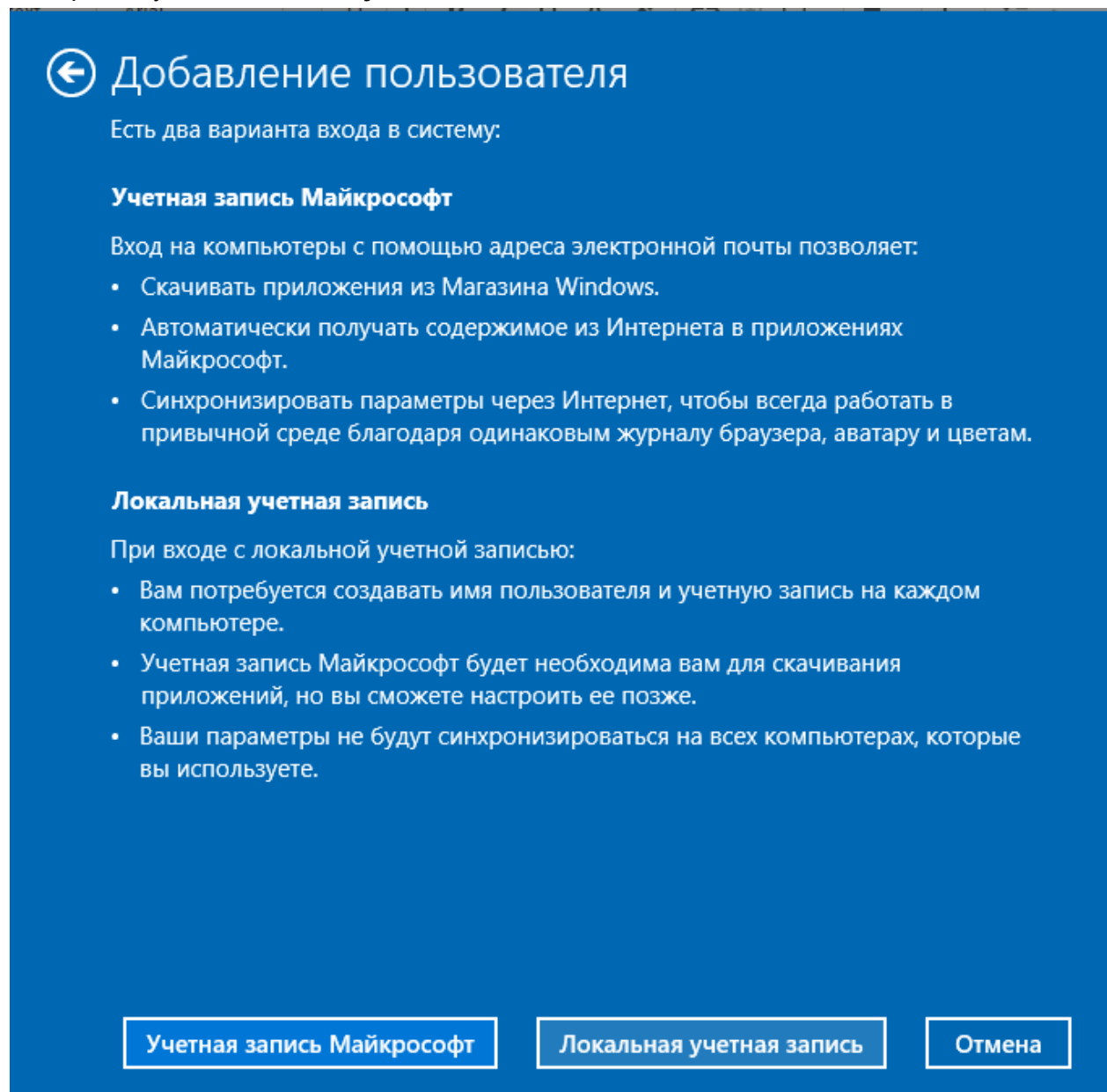
[Заявление о конфиденциальности](#)

Вход без учетной записи Майкрософт (не рекомендуется)

Далее

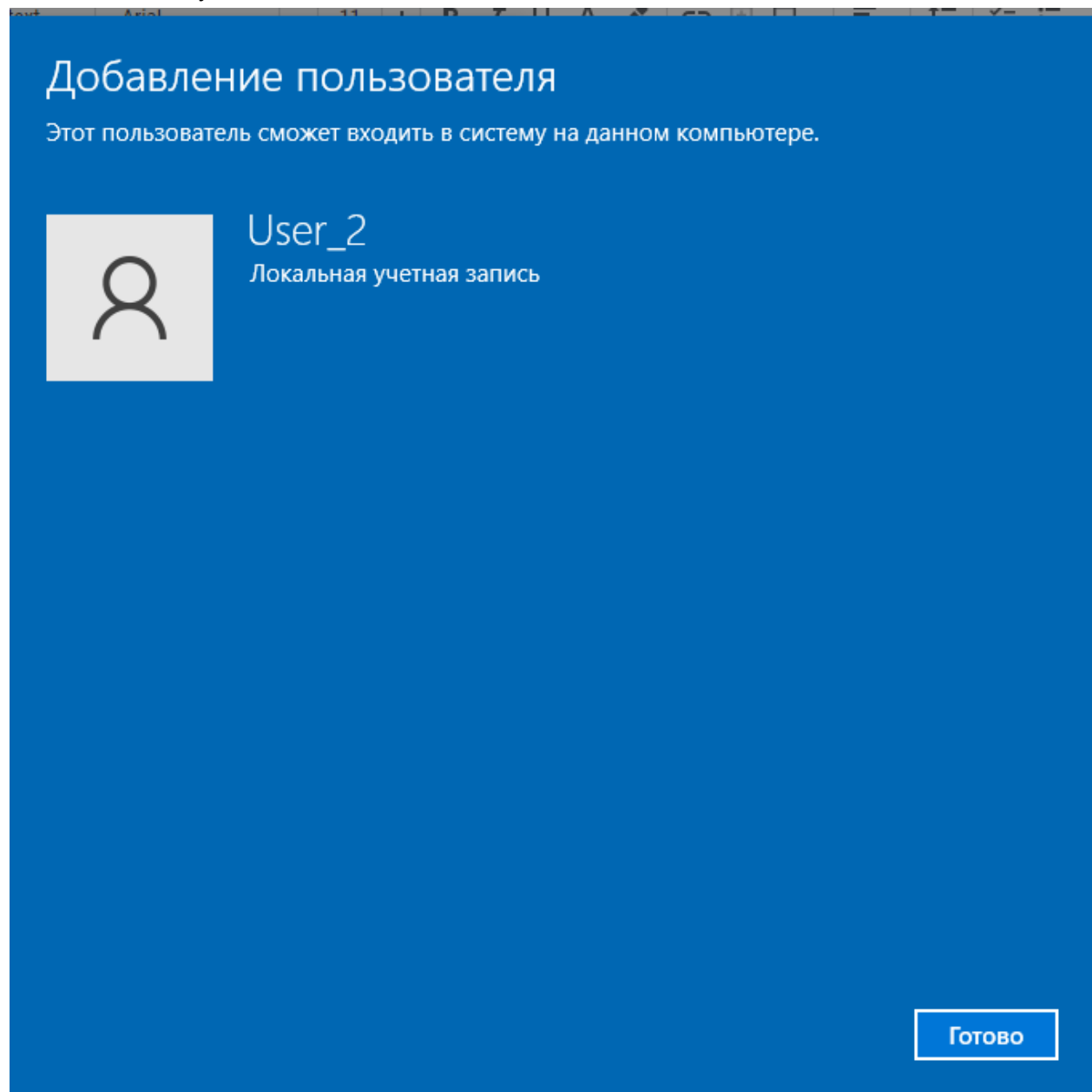
Отмена

Выбираем пункт: **Локальная учетная запись**



Вводим данные пользователя и нажимает кнопку **“Далее”**

Нажимает кнопку: **Готово**





Пользователи

Дополнительно



Следующий список используется для предоставления или отказа в доступе к вашему компьютеру, а также для смены паролей и иных параметров.

Пользователи этого компьютера:

| Имя пользователя | Группа |
|--|------------------------------|
|  trottimus.2001@mail.ru | Пользователи; Администраторы |
|  User_2 | Пользователи |

Добавить...

Удалить

Свойства

Пароль пользователя trottimus.2001@mail.ru



Чтобы изменить свой пароль, перейдите к параметрам компьютера и выберите "Пользователи".

Сменить пароль...

ОК

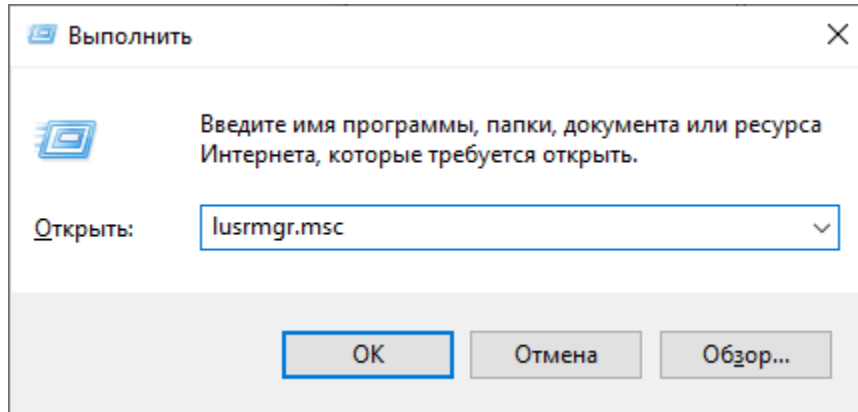
Отмена

Применить

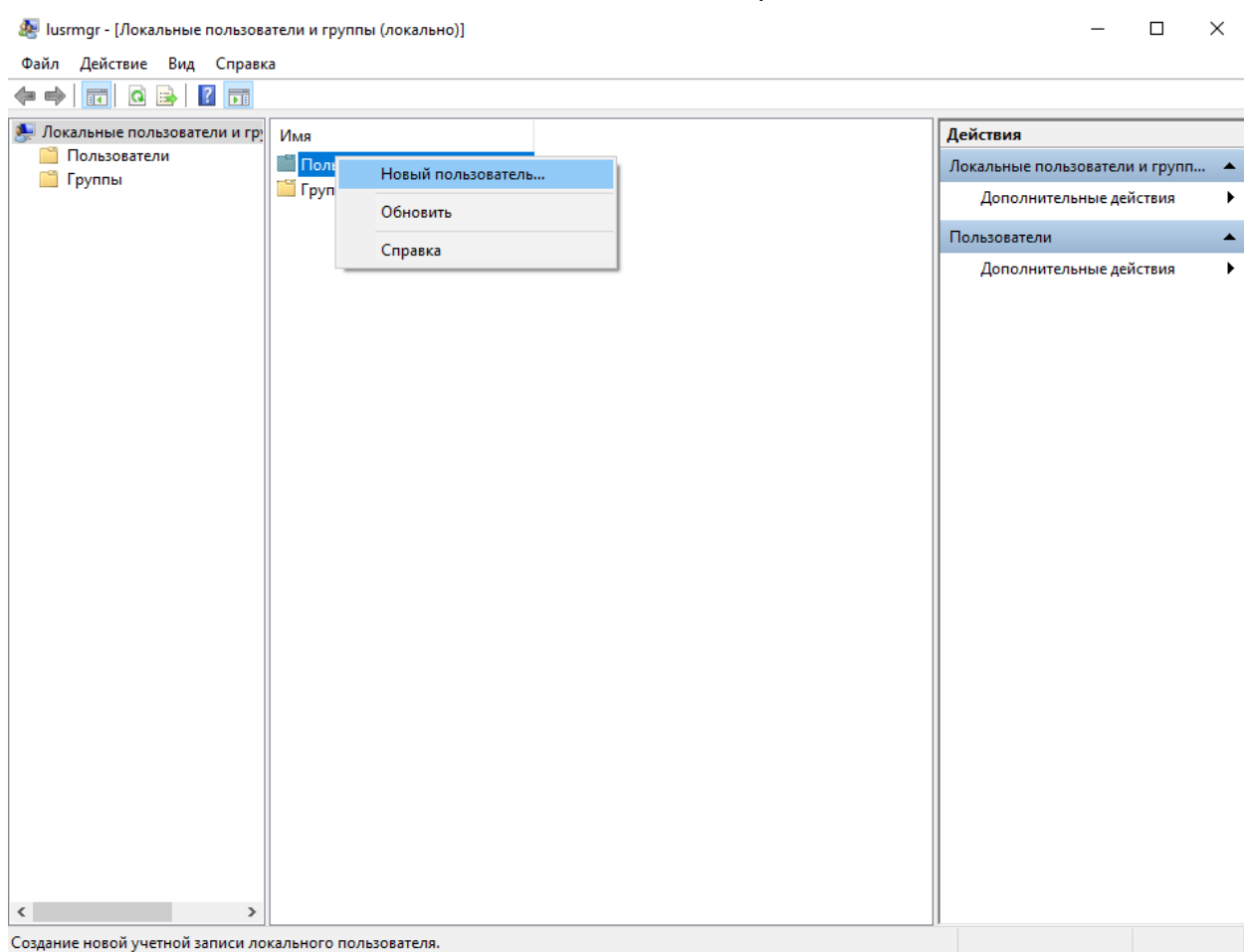
Вариант 2.5:

Открываем окно **“Выполнить”** например через сочетание клавиш: **Win + R**

Вводим в появившейся строке: **lusrmgr.msc**



Вызываем контекстное меню от **“Пользователи”** и выбрать **“Новый пользователь”**



Вводим необходимые данные и нажимаем кнопку **“Создать”**

Новый пользователь

?

×

Пользователь:

User_2

Полное имя:

Описание:

Пароль:

Подтверждение:

☐ Требуется смена пароля при следующем входе в систему

☐ Запретить смену пароля пользователем

☐ Срок действия пароля не ограничен

☐ Отключить учетную запись

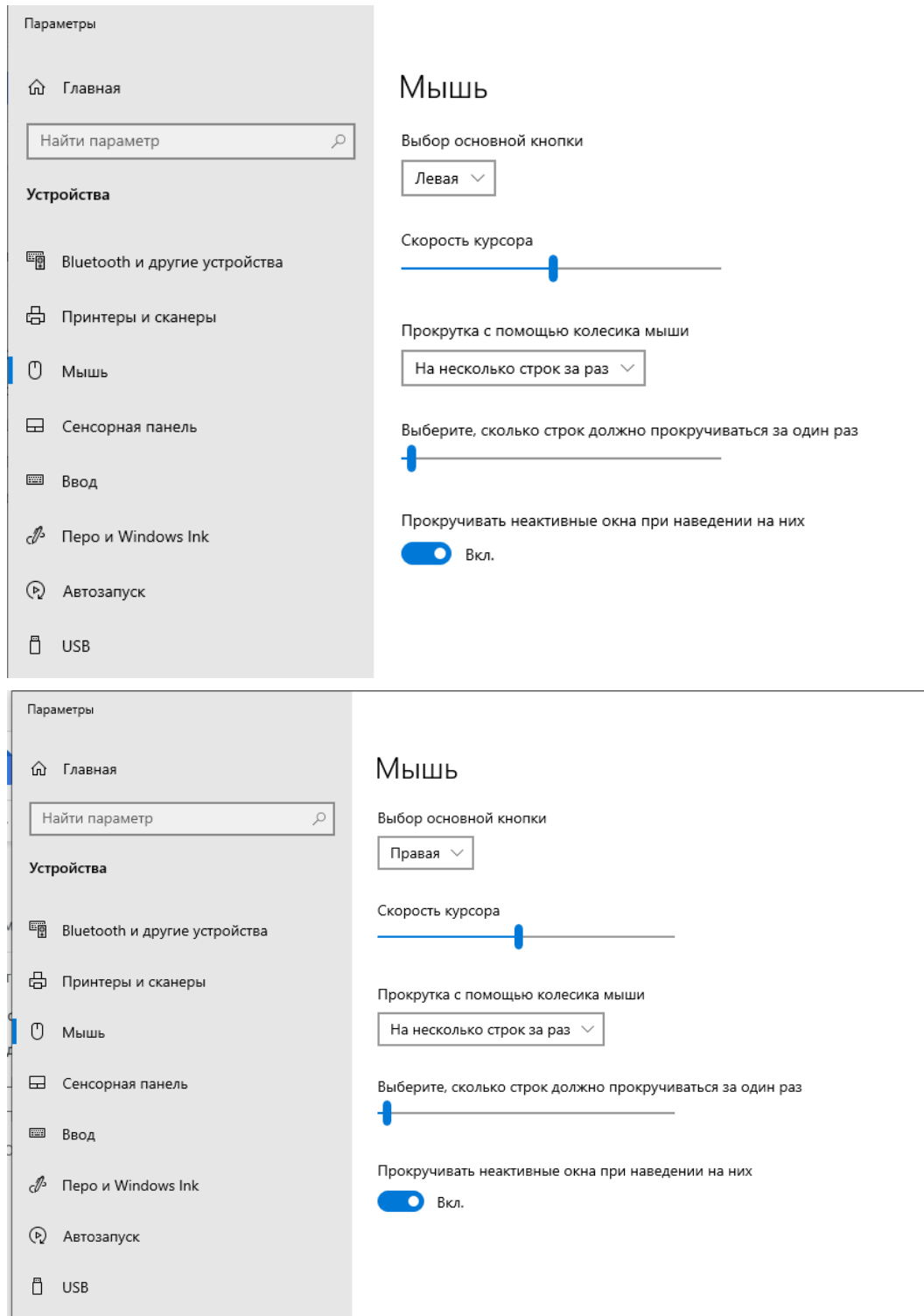
Справка

Создать

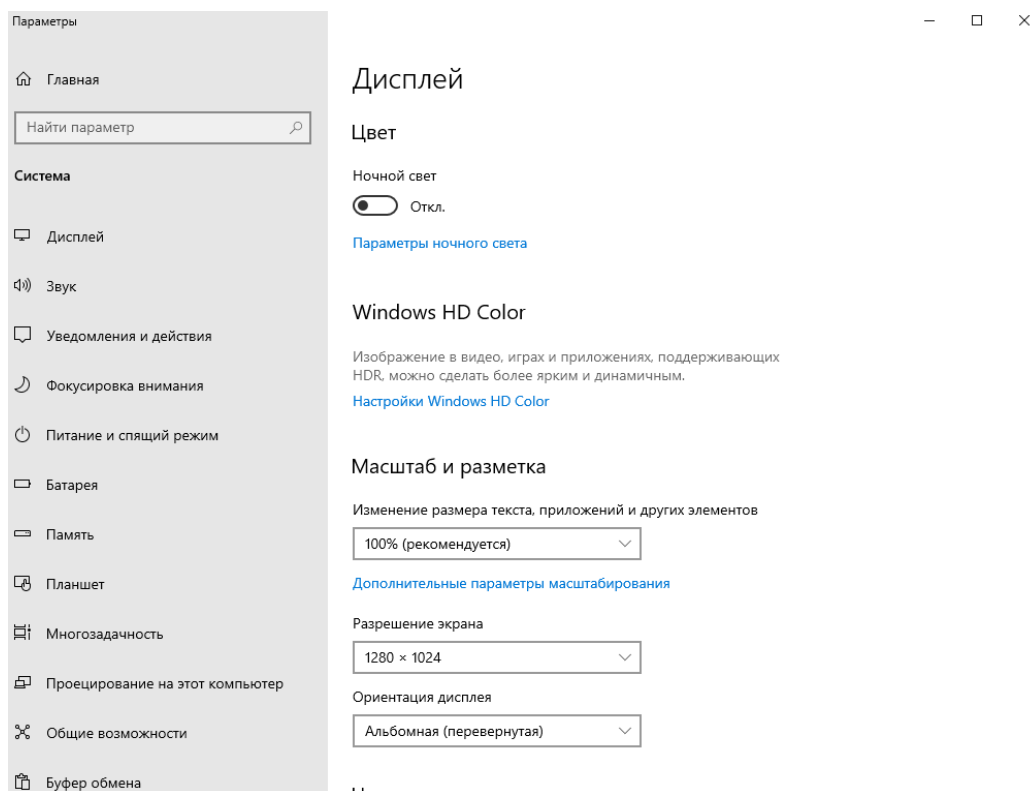
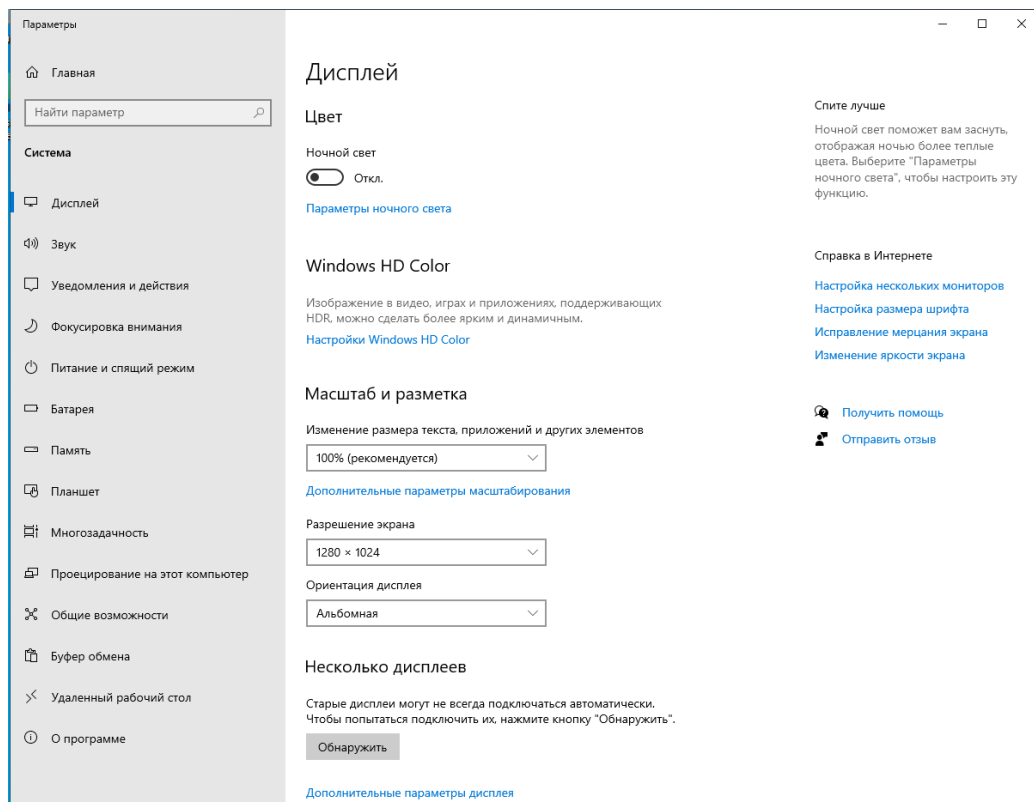
Закреть

Возможности

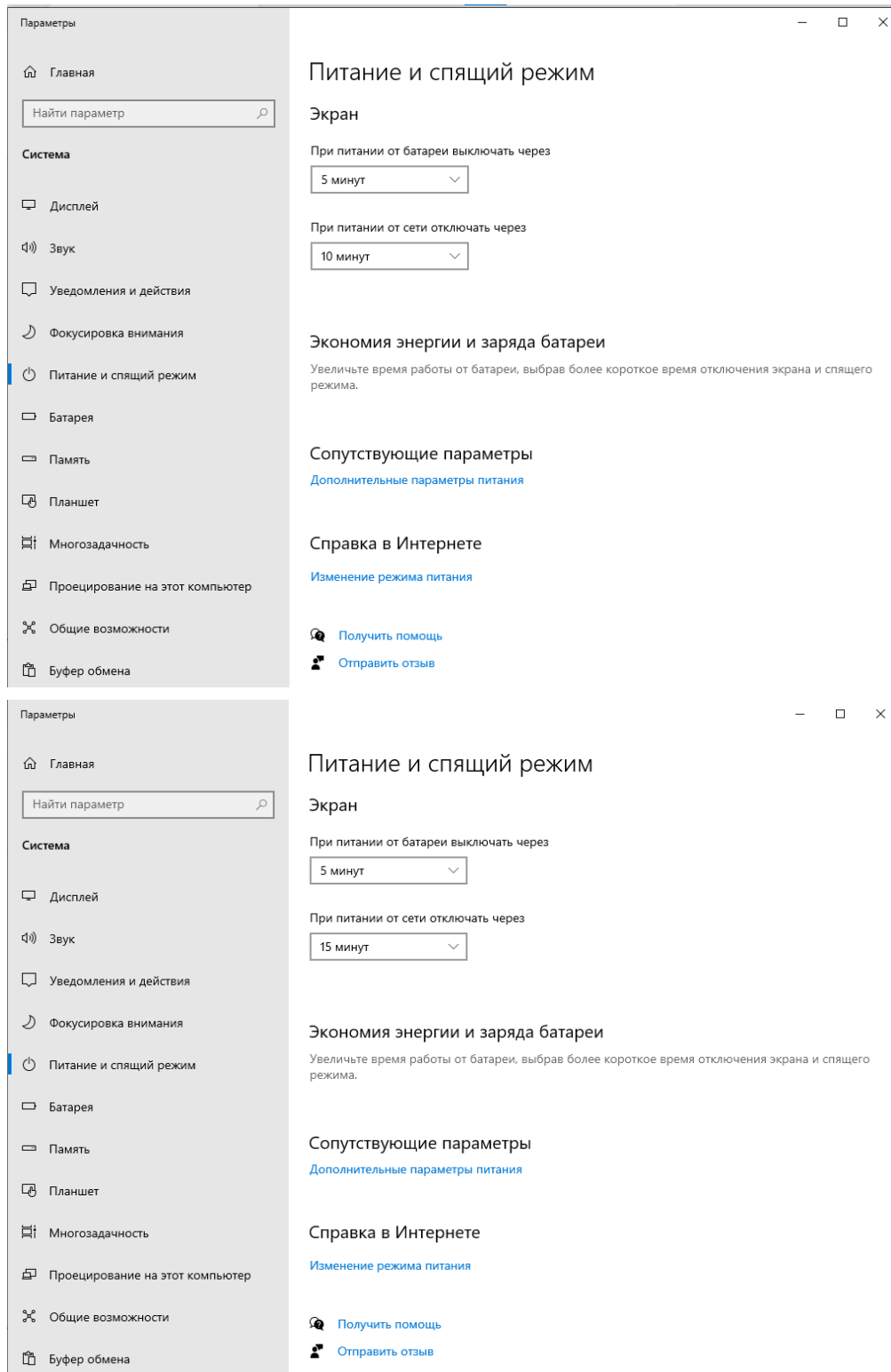
Пользователь в Параметрах может изменить конфигурацию мыши в системе. Например, изменить основную кнопку:



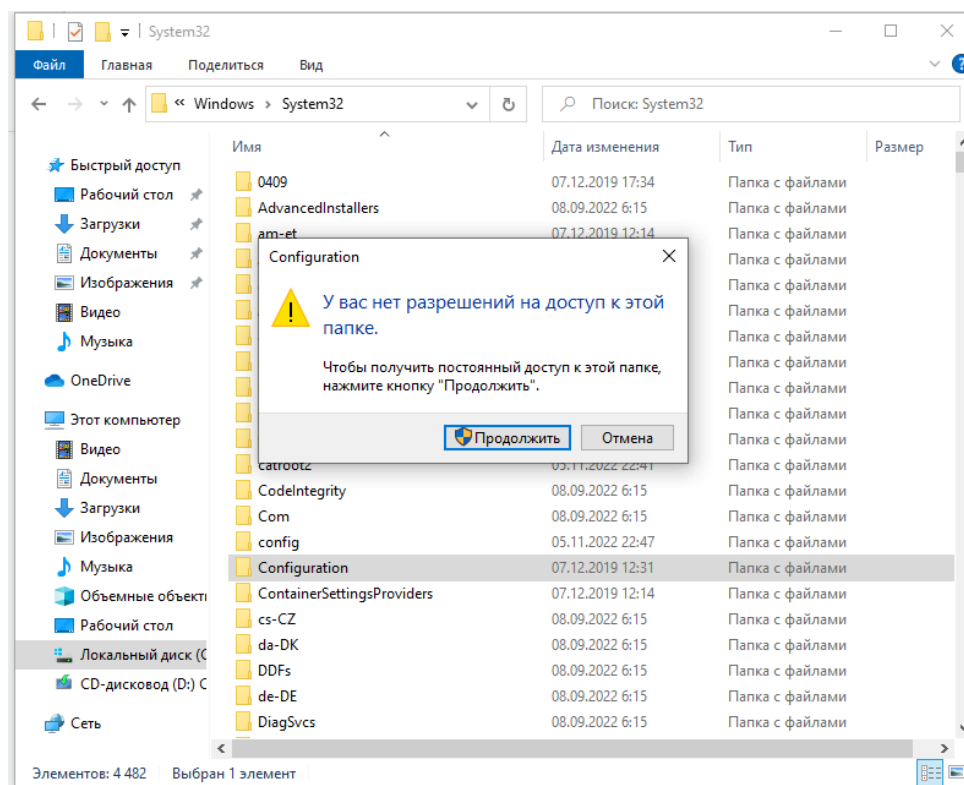
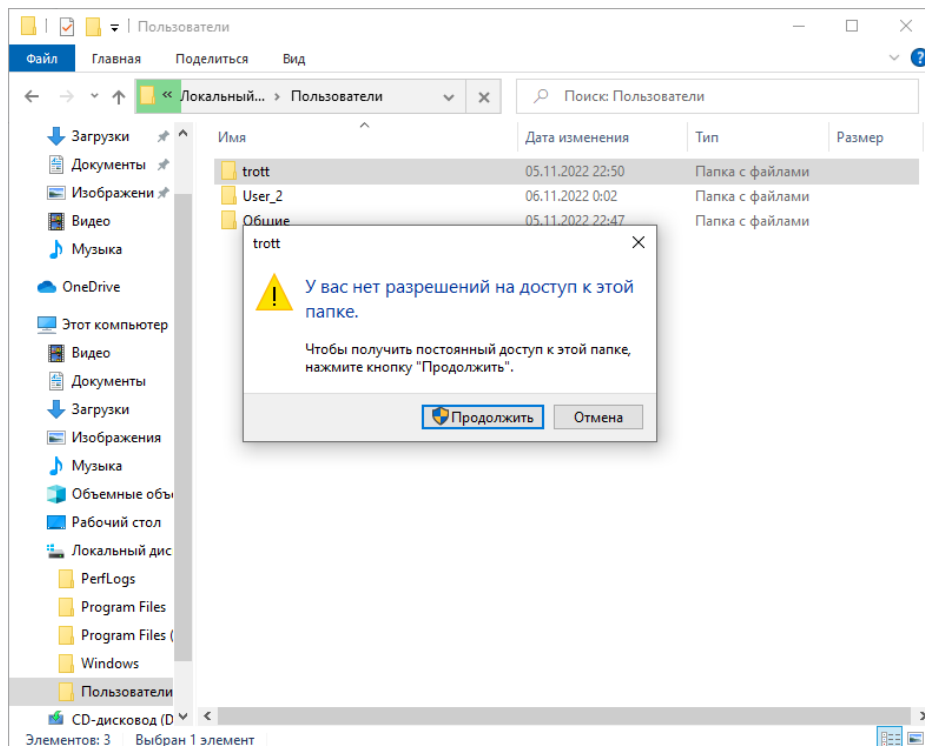
Также пользователь может изменить параметры дисплея.
Например, разрешение:



Пользователь может задать время отключения экрана:



Однако обычный пользователь не может получить доступ к папке другого пользователя или к системным папкам

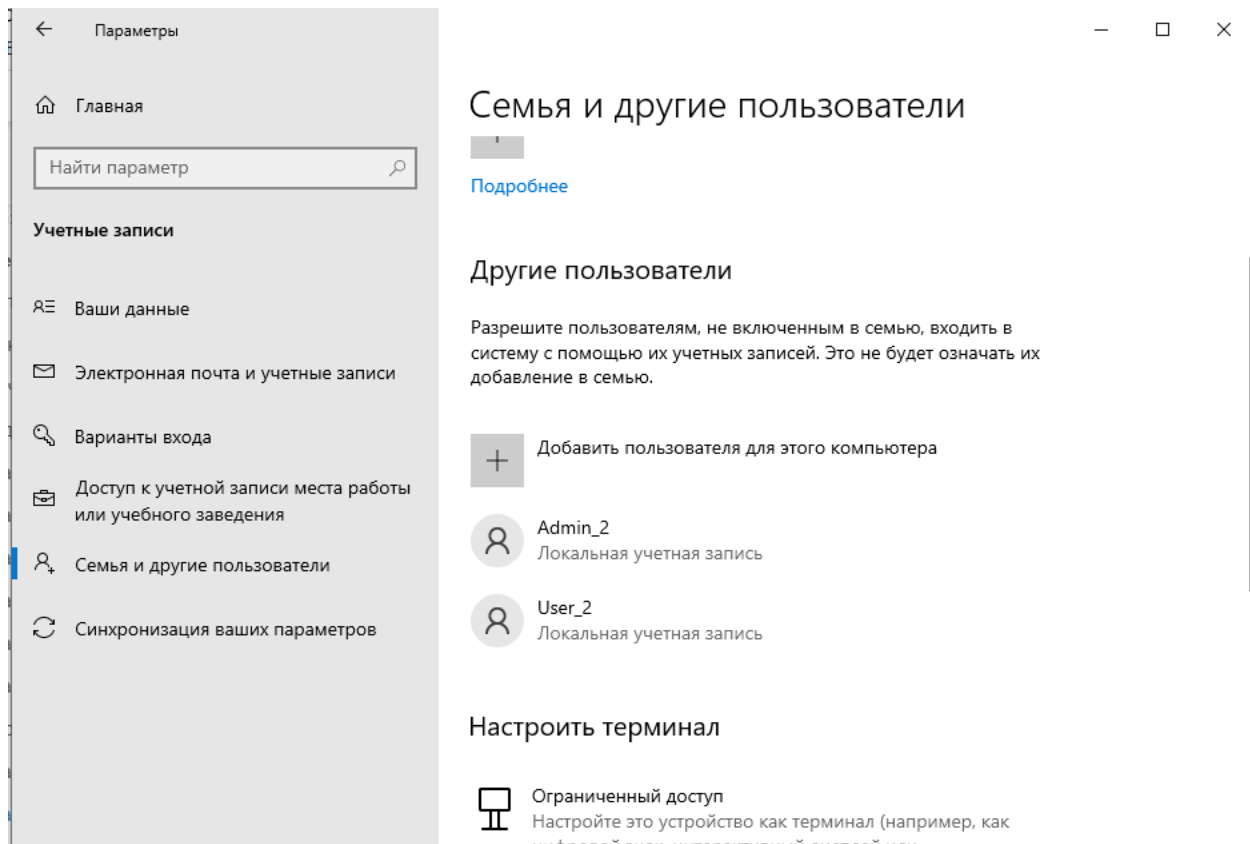


3. Создание администратора

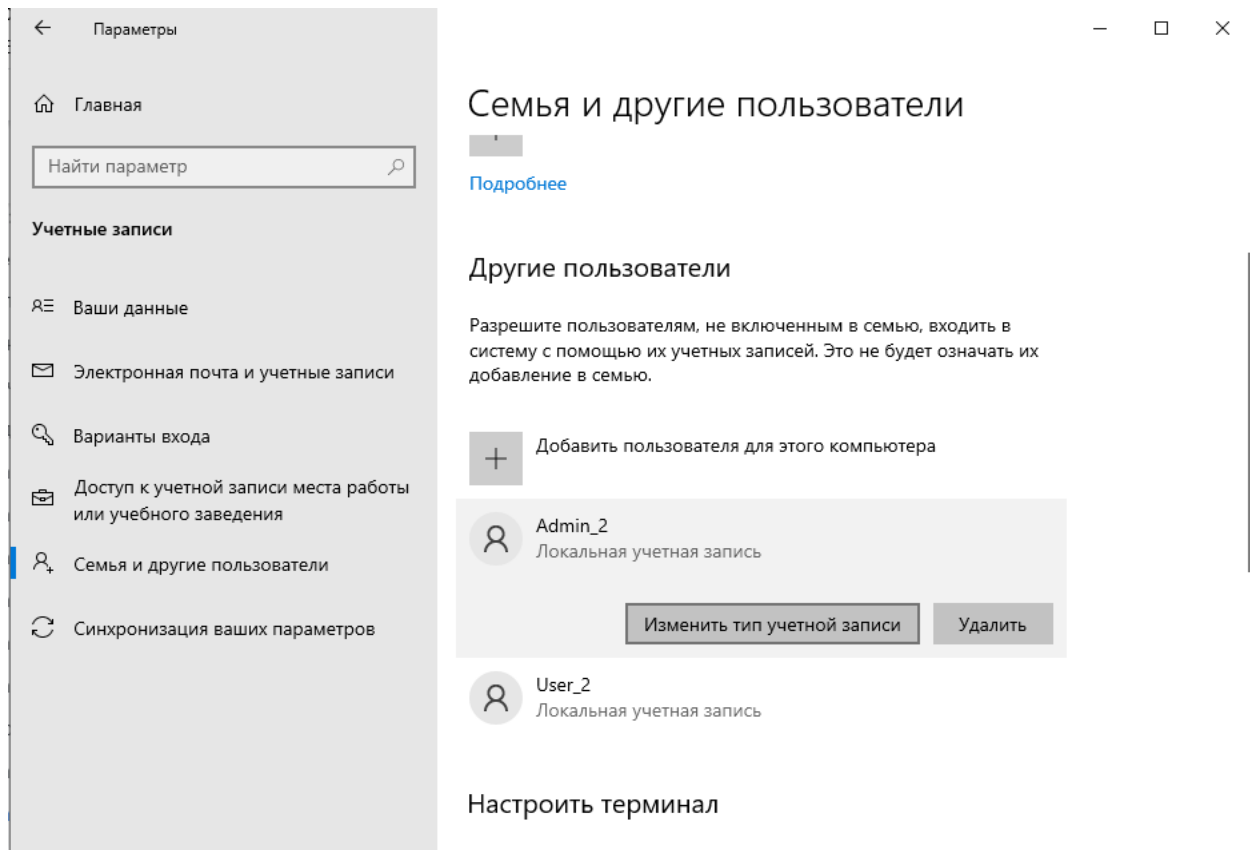
К сожалению в Windows 10 нельзя сразу создать пользователя в группе **Администраторы**, как это раньше было в Windows 7. Можно только создать пользователя в группе **Пользователи** и затем уже добавить его после этого в группу **Администраторы**.

Вариант 3.1:

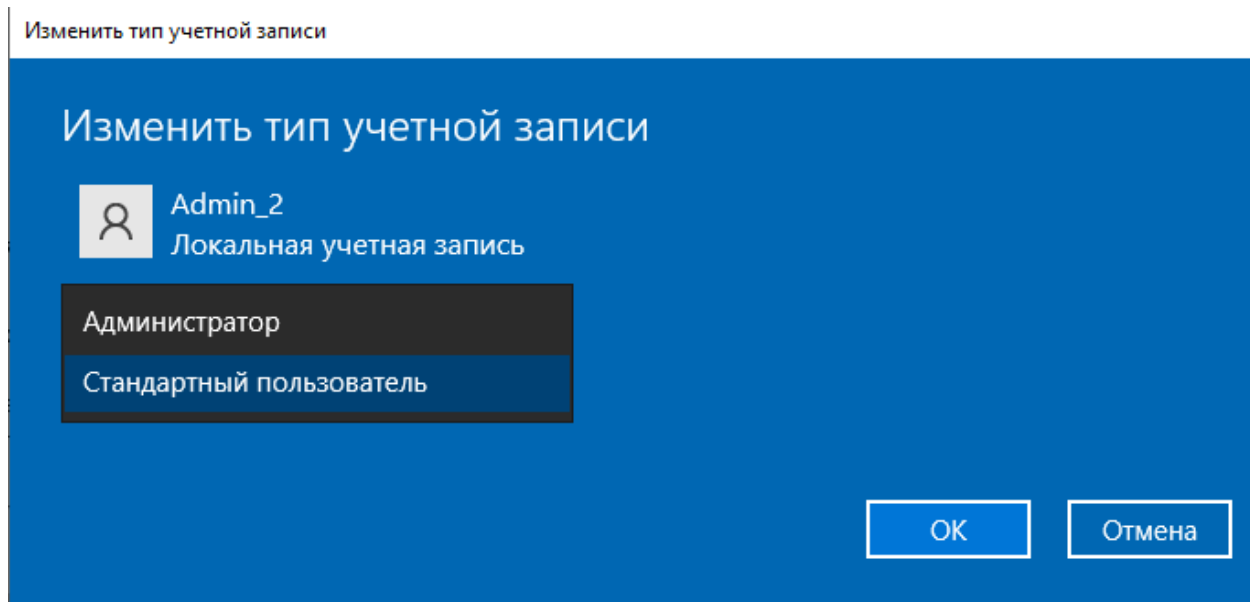
Повторим действия из пункта [Вариант 2.1:](#) и создадим пользователя **Admin_2**



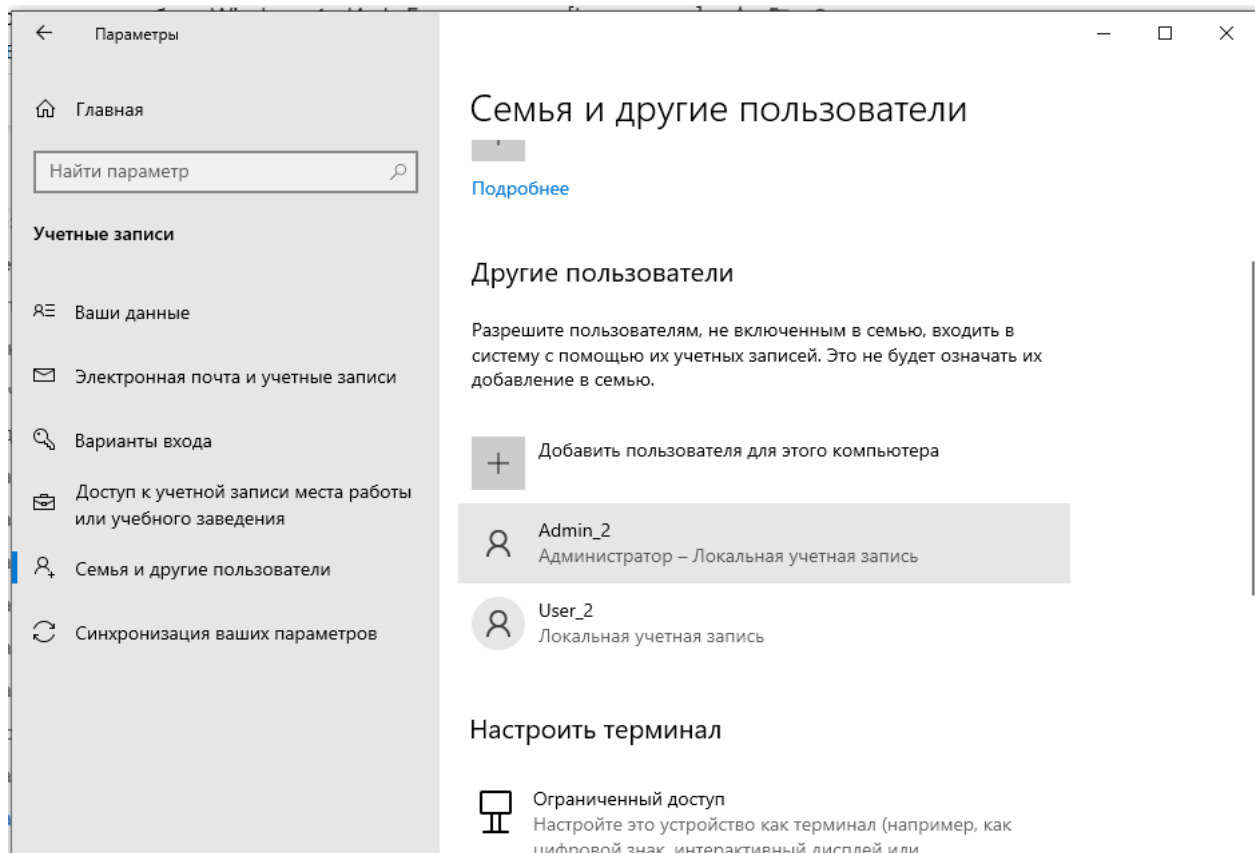
Затем нажмем на нашего пользователя **Admin_2** и нажмем на появившуюся кнопку:
Изменить тип учетной записи



В появившемся окне меняем тип учетной записи с “**Стандартный пользователь**” на “**Администратор**” и нажимаем кнопку “**ОК**”



Затем смотрим изменения:



Вариант 3.2:

Повторим действия из пункта [Вариант 2.3:](#) и создадим пользователя **Admin_2**

А затем добавляем его в группу “**Администраторы**” с помощью команды: **net localgroup "Администраторы" Admin_2 /add**

Чтобы узнать в какие группы мы можем добавлять пользователя мы можем ввести команду: **net localgroup**

```
Администратор: Командная строка
Microsoft Windows [Version 10.0.19045.2006]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Windows\system32>net user Admin_2 /add
Команда выполнена успешно.

C:\Windows\system32>net localgroup "Администраторы" Admin_2 /add
Команда выполнена успешно.

C:\Windows\system32>
```

```
Администратор: Командная строка

C:\Windows\system32>net localgroup

Псевдонимы для \\DESKTOP-DC30ER7
-----
*IIS_IUSRS
*Администраторы
*Администраторы Hyper-V
*Владельцы устройства
*Гости
*Криптографические операторы
*Операторы архива
*Операторы настройки сети
*Операторы помощи по контролю учетных записей
*Опытные пользователи
*Пользователи
*Пользователи DCOM
*Пользователи журналов производительности
*Пользователи системного монитора
*Пользователи удаленного рабочего стола
*Пользователи удаленного управления
*Репликатор
*Управляемая системой группа учетных записей
*Читатели журнала событий
Команда выполнена успешно.
```

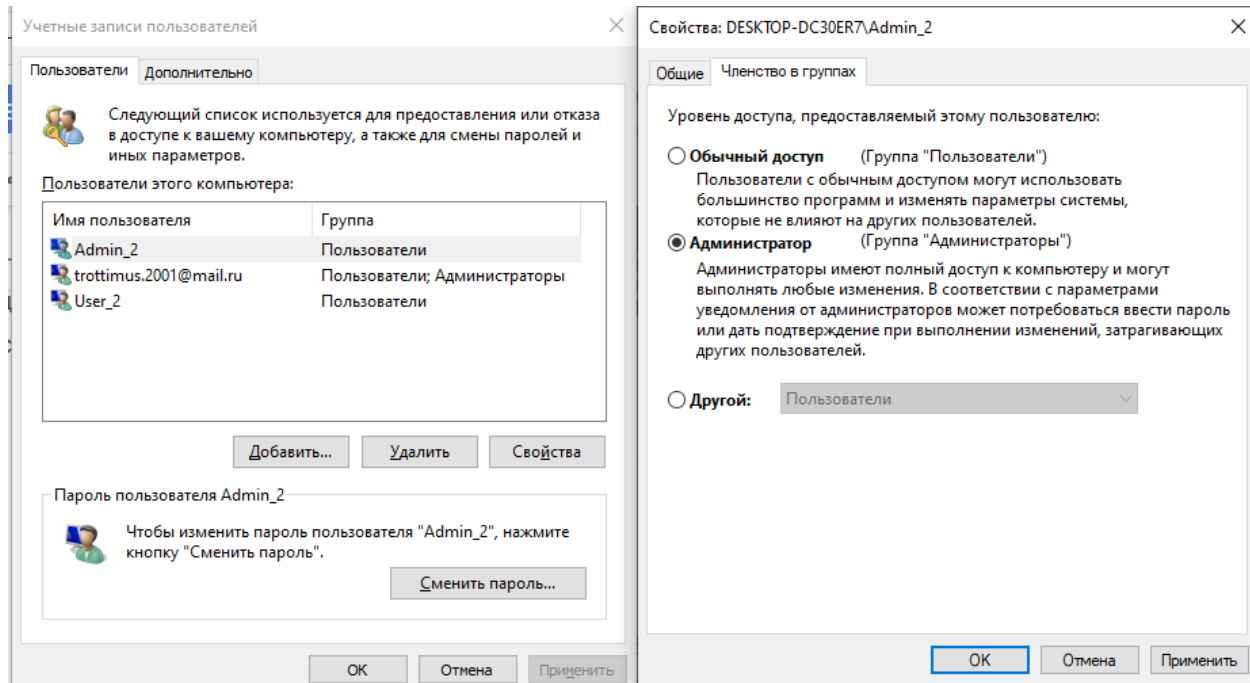
Вариант 3.3:

Повторим действия из пункта [Вариант 2.4](#): и создадим пользователя **Admin_2**

Затем выбираем **Admin_2** и нажимаем кнопку **“Свойства”**.

В правом окне меняем во вкладке **“Членство в группах”** на **“Администратор”**.

Затем нажимаем кнопку **“Применить”**, после нажимаем **“ОК”**

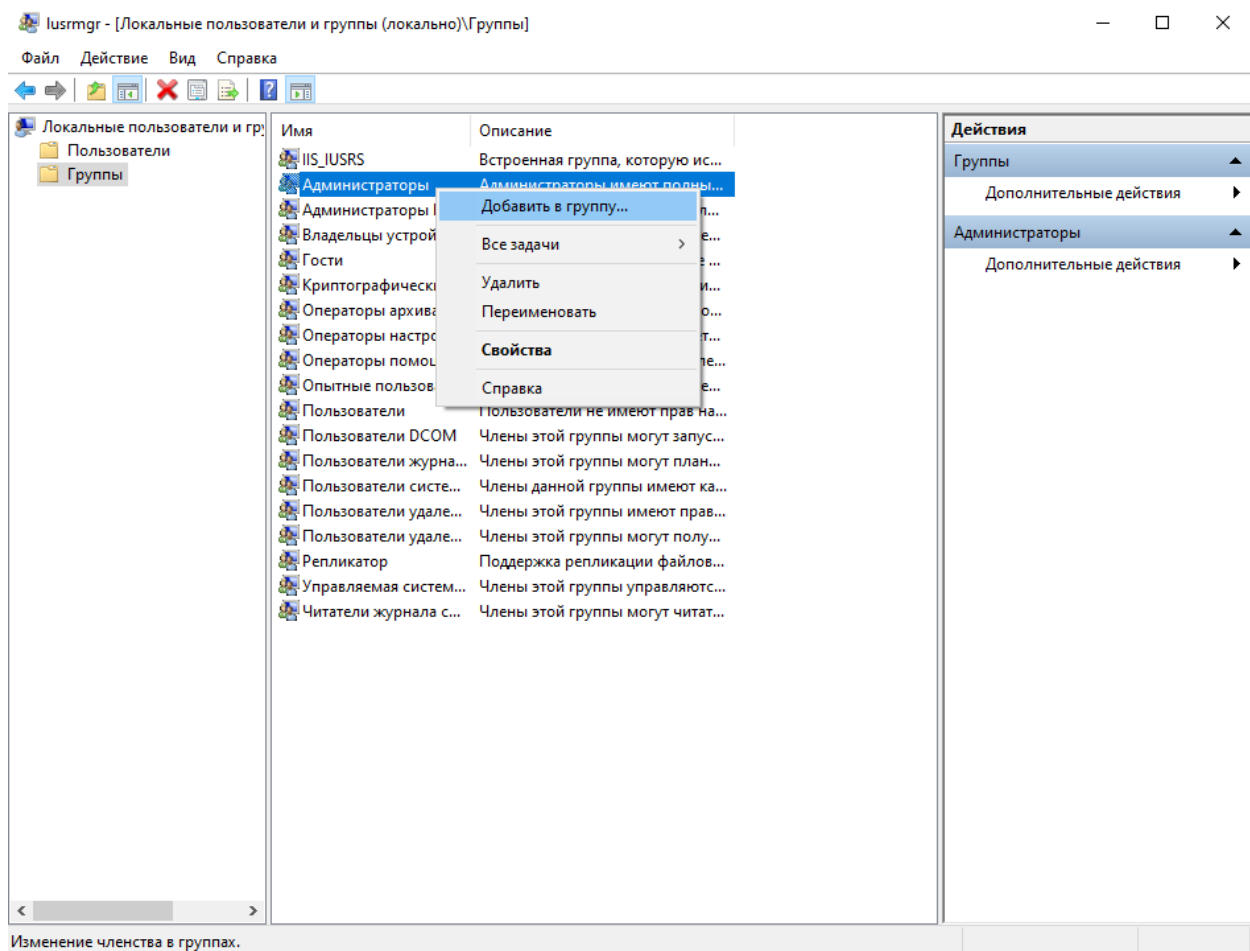


Вариант 3.4:

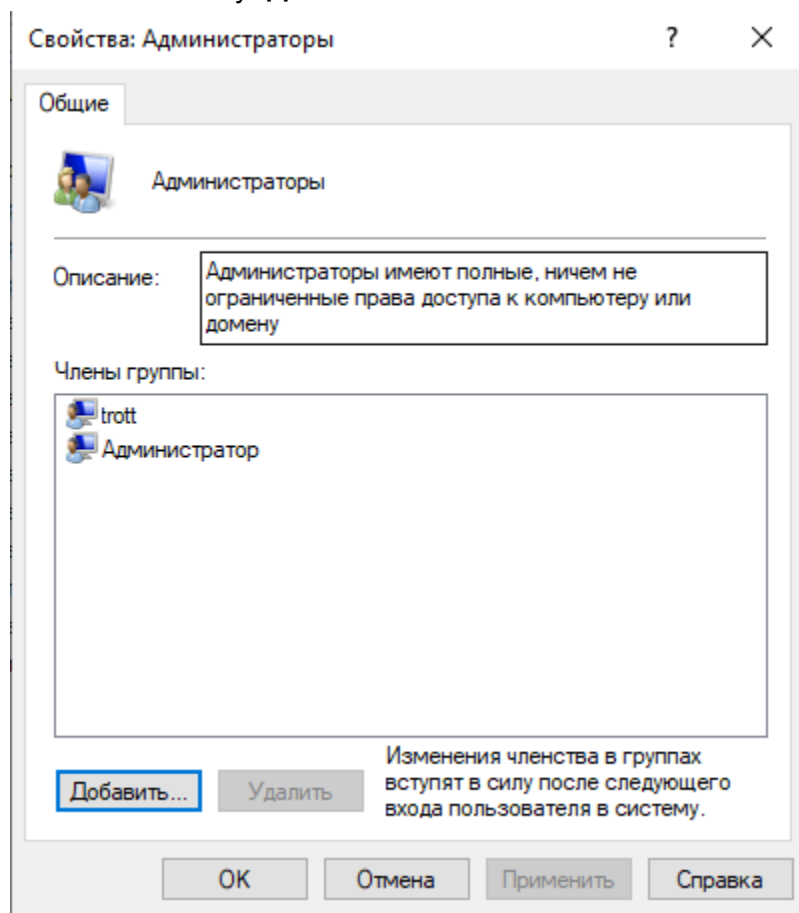
Повторим действия из пункта [Вариант 2.5](#): и создадим пользователя **Admin_2**

Затем переходим в раздел “Группы” и нажимаем правой кнопкой мыши по “Администраторы”.

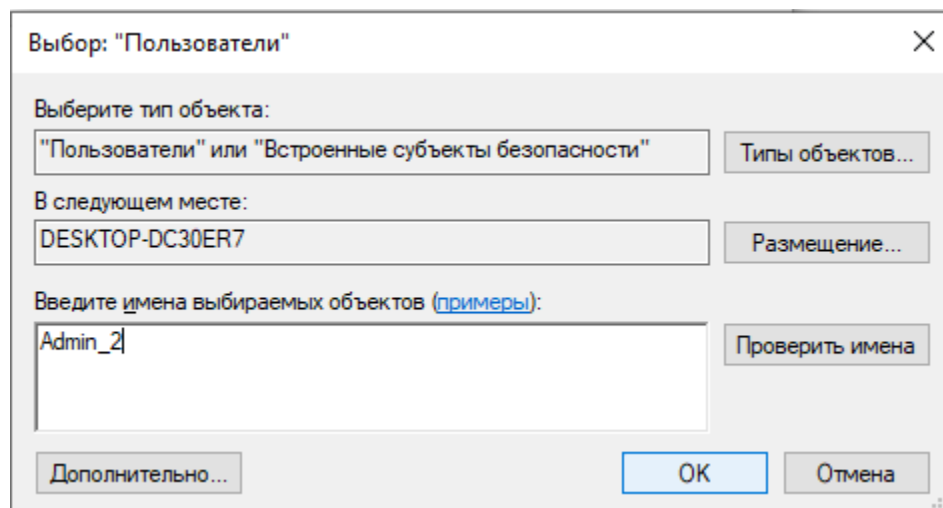
В появившемся выпадающем списке выбираем “Добавить в группу...”



Нажимаем кнопку **“Добавить...”**



Вводим имя пользователя в поле **“Введите имена выбираемых объектов (примеры)”** и нажимаем **ОК**



Затем нажимаем кнопку **“Применить”**, после нажимаем **“ОК”**

Свойства: Администраторы



Общие



Администраторы

Описание:

Администраторы имеют полные, ничем не ограниченные права доступа к компьютеру или домену

Члены группы:



Admin_2



trott



Администратор

Добавить...

Удалить

Изменения членства в группах вступят в силу после следующего входа пользователя в систему.

ОК

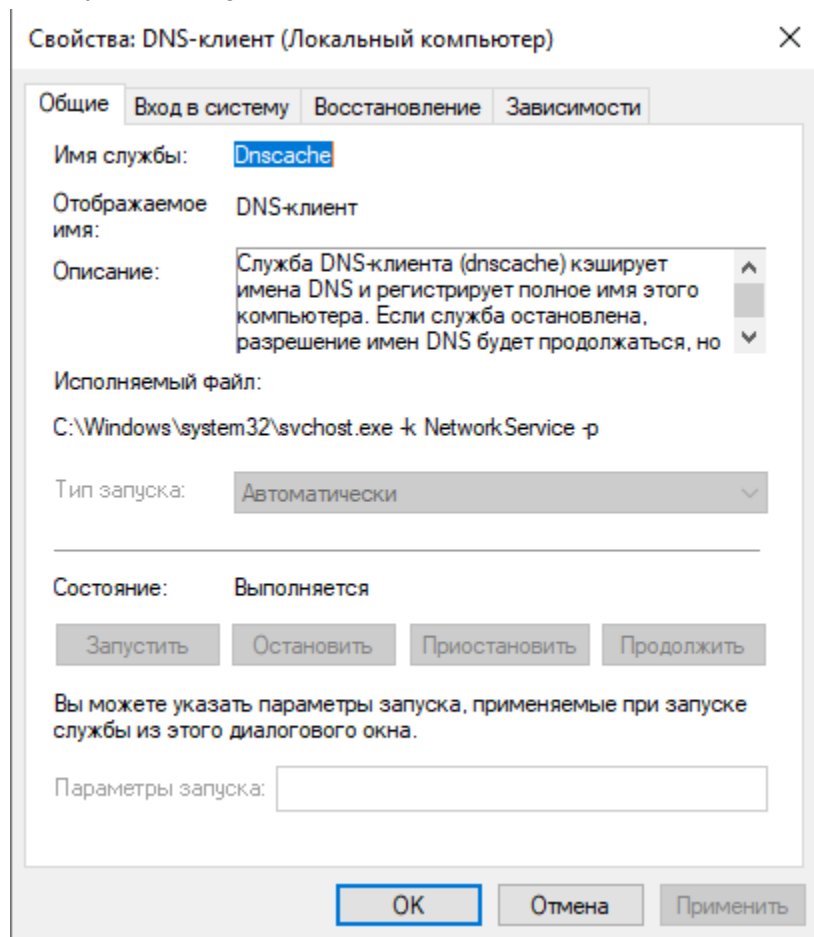
Отмена

Применить

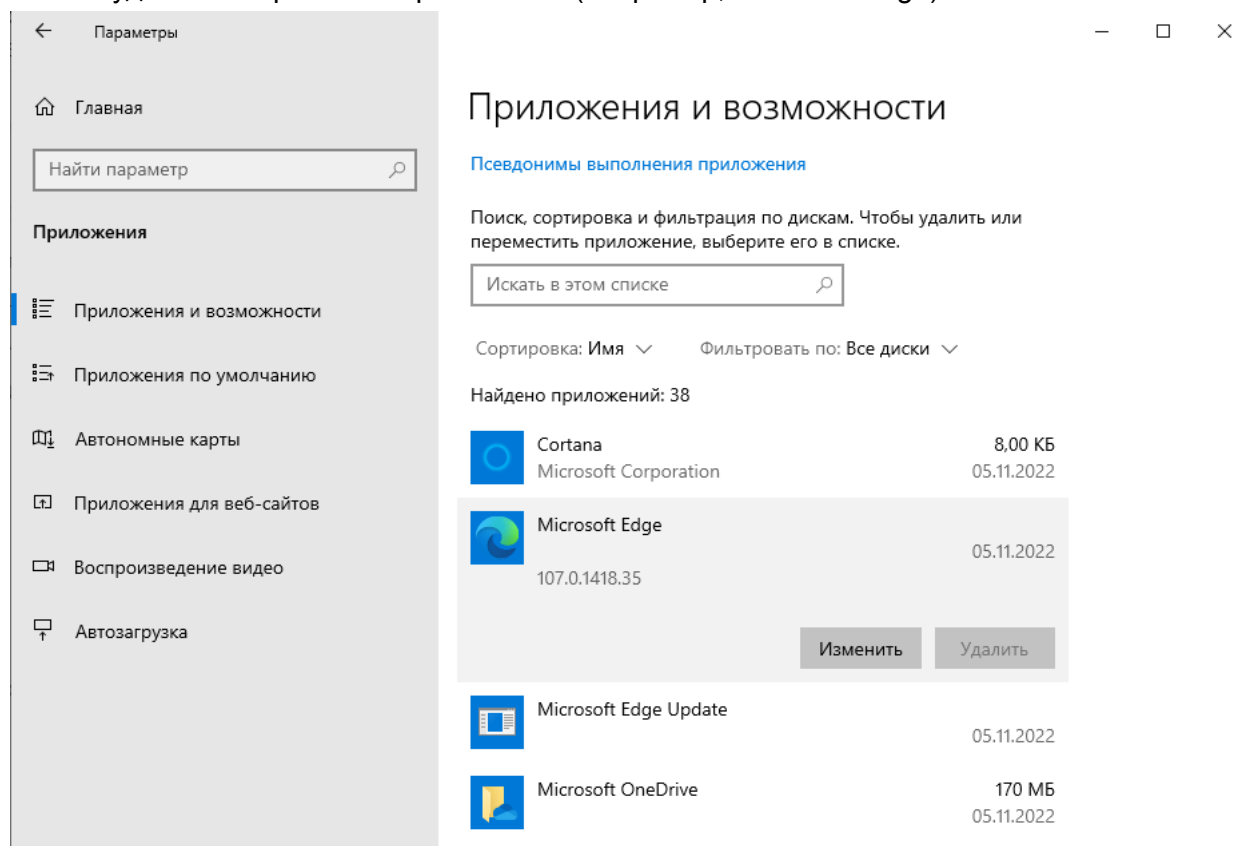
Справка

Ограничения

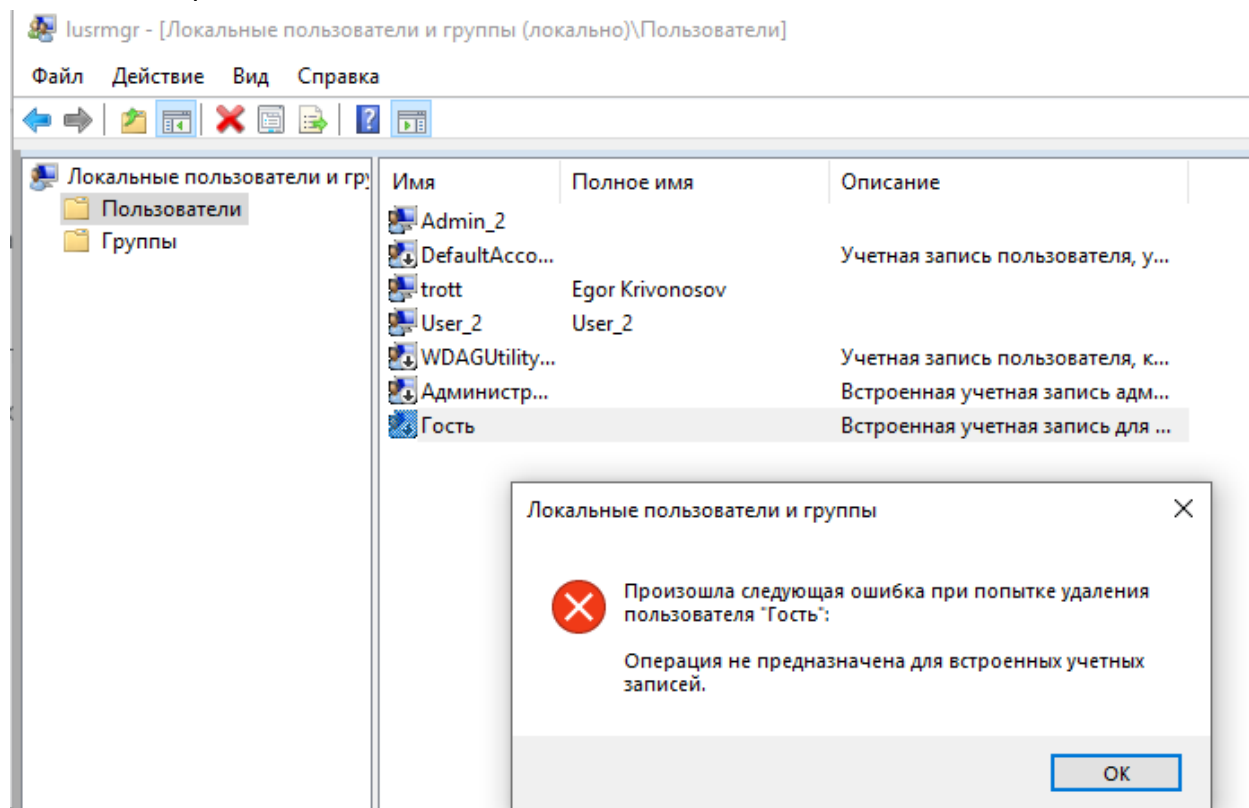
Нельзя отключить автозапуск службы например: **Dnscache**
Кнопку “**Тип запуска**” неактивна.



Нельзя удалить встроенные приложения (например, Microsoft Edge):

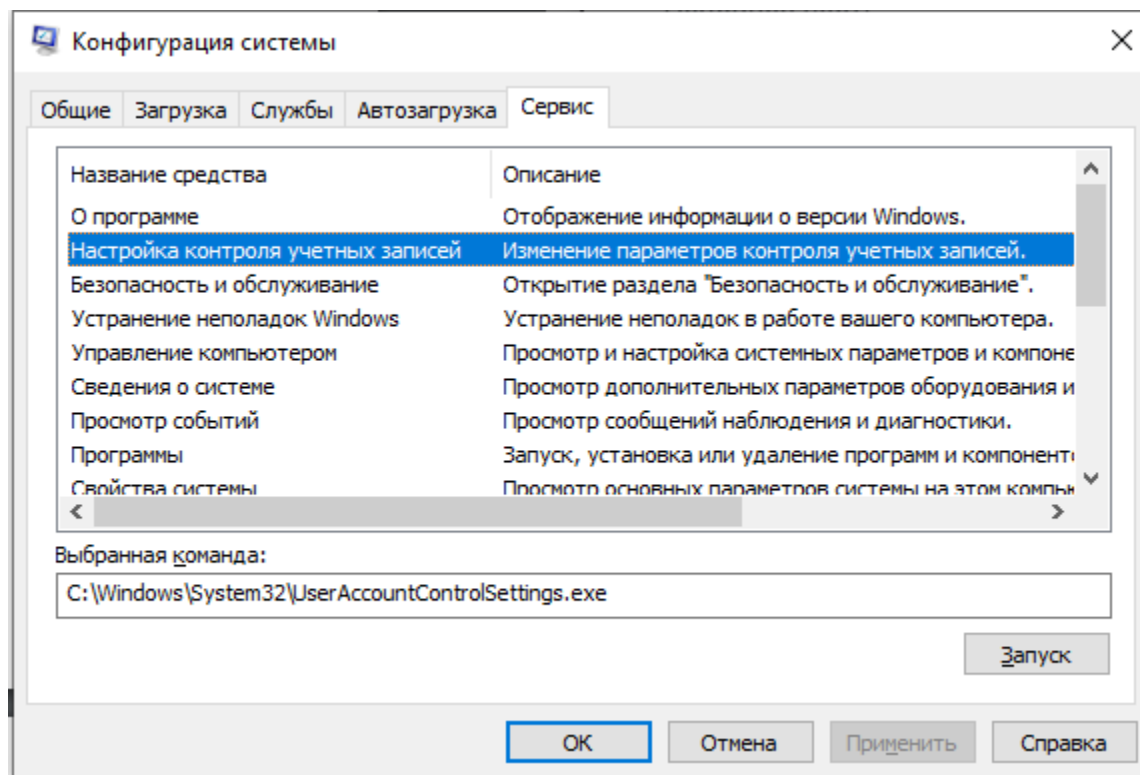
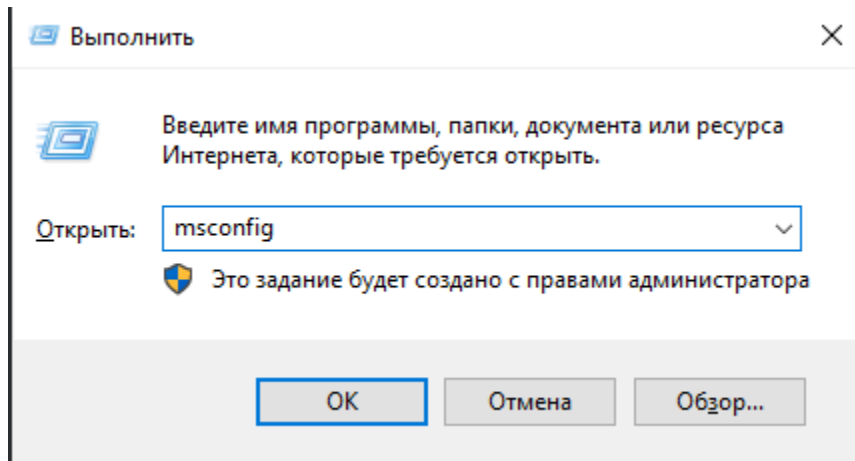


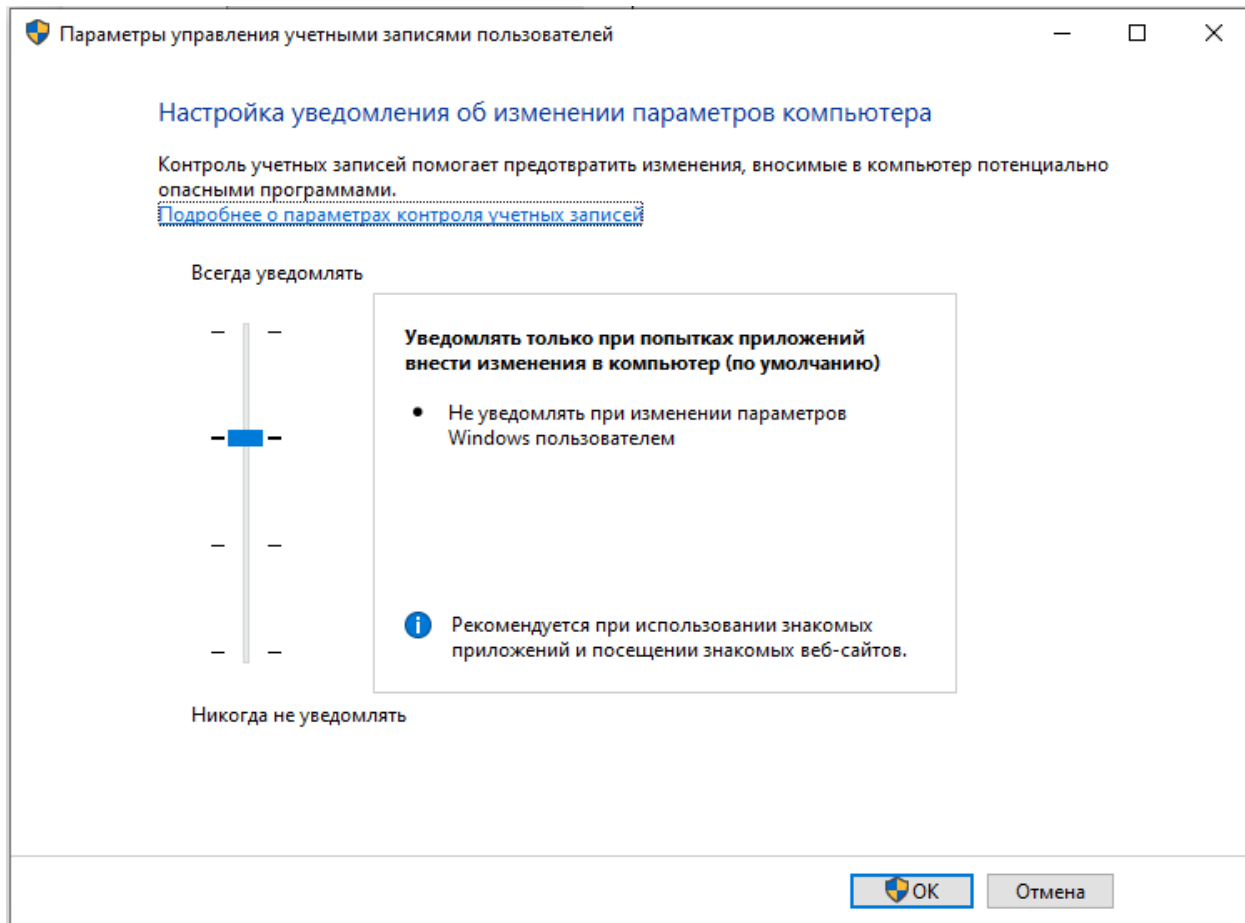
Администратор не может удалять встроенные аккаунты **Администратор** и **Гость**, которые не являются фактическими пользователями.



4. Политики UAC (User Account Control)

Контроль учётных записей пользователей - это компонент операционных систем Microsoft Windows, впервые появившийся в Windows Vista. Этот компонент запрашивает подтверждение действий, требующих прав администратора, в целях защиты от несанкционированного использования компьютера





Существует 4 уровня:

1. Уведомлять всегда, когда приложения пытаются установить программное обеспечение или изменить параметры компьютера; когда пользователь изменяет параметры Windows.
Самый рекомендуемый вариант при частом посещении незнакомых веб-сайтов или частой установке приложений.
2. Уведомлять только при попытках приложений внести изменения в компьютер, но не уведомлять при изменении параметров Windows пользователем.
Рекомендуется при нечастом посещении незнакомых веб-сайтов или не частой установке приложений.
3. Уведомлять только при попытках приложений внести изменения в компьютер (не затемнять рабочий стол), но не уведомлять при изменении параметров Windows пользователем.
Не рекомендуется, но используется, если затемнение рабочего стола отнимает много времени.
4. Не уведомлять, когда приложения пытаются установить программное обеспечение или изменить параметры компьютера; когда пользователь изменяет параметры Windows.
Не рекомендуется по соображениям безопасности.

5. Задание по варианту

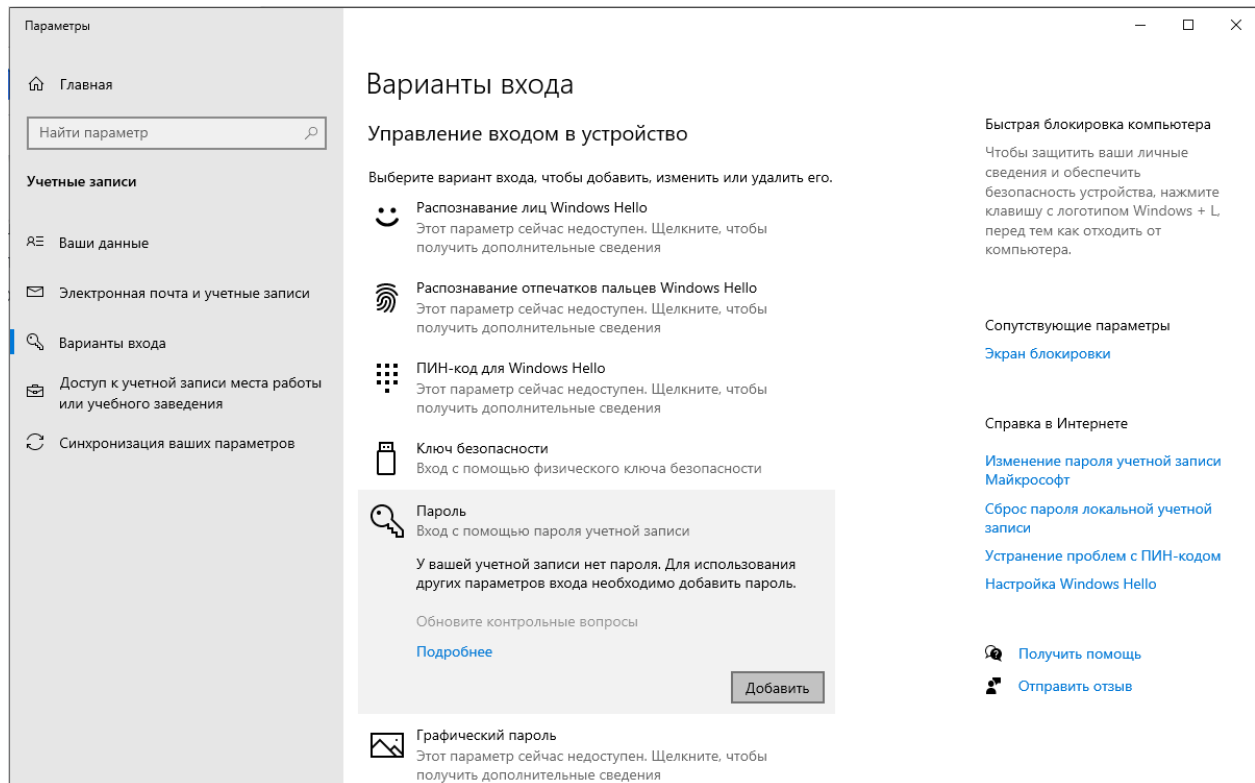
Настроить вход пользователя в систему в безопасном режиме по паролю. Рассмотреть и реализовать возможные способы усиления парольной защиты.

Выполнение


Для начала установим пароль для пользователя **User_2**.

Для этого перейдем в **Параметры**, выберем **Учетные записи**, **Варианты входа**.

Нажмем на **Пароль**, затем нажмем на кнопку **Добавить**.



Заполним поля и подтвердим добавление пароля.

 Изменение пароля


Новый пароль

••••

Подтверждение пароля


••••

Подсказка для пароля


кто не я? 

Далее

Отмена

 Создание пароля

При следующем входе в систему используйте свой новый пароль.



User_2
Локальная учетная запись

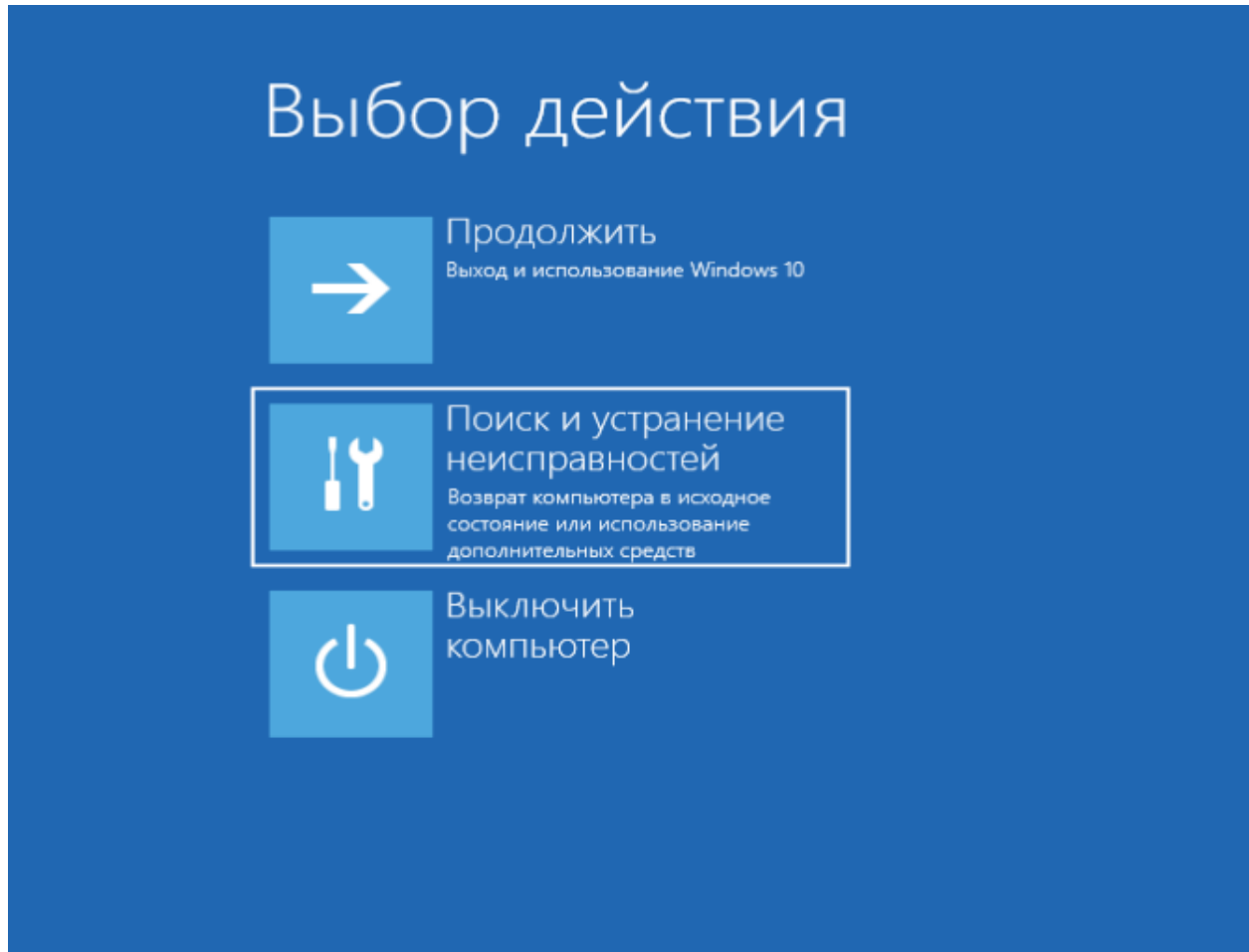
Готово

Отмена

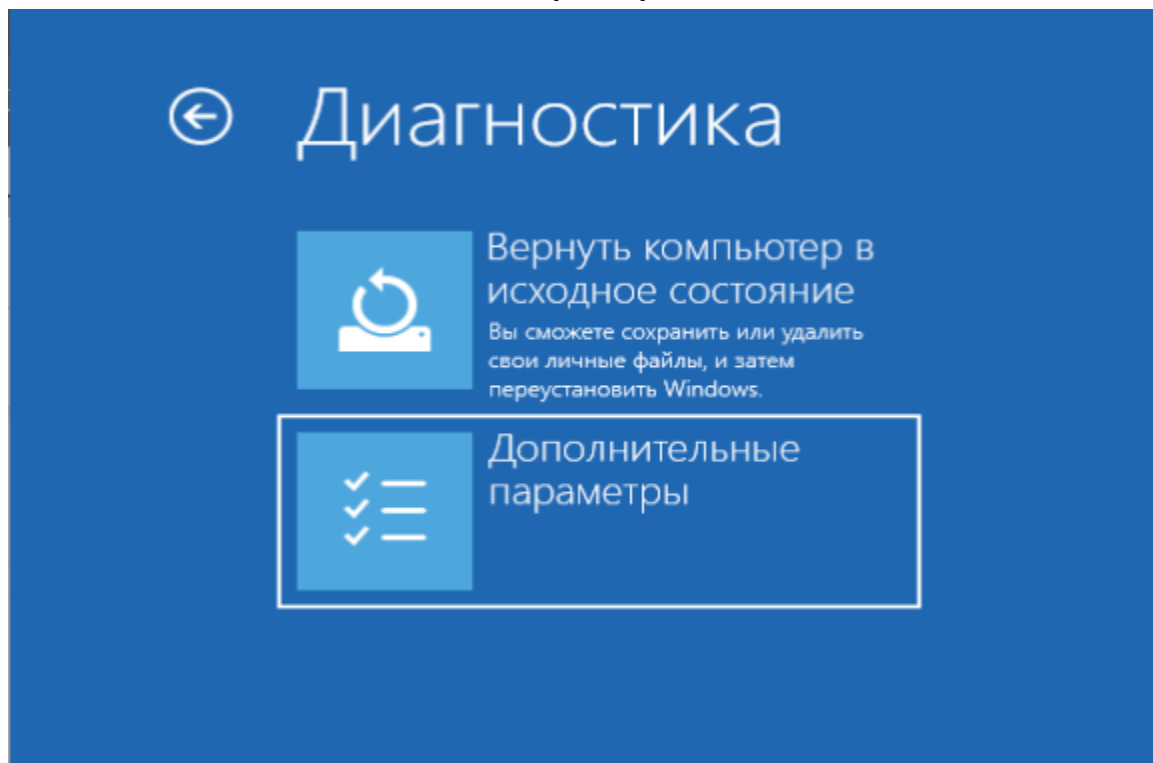
Затем есть 2 способа как попасть в безопасный режим.

Первый способ это **Перезагрузить** систему с **нажатой кнопкой Shift**.

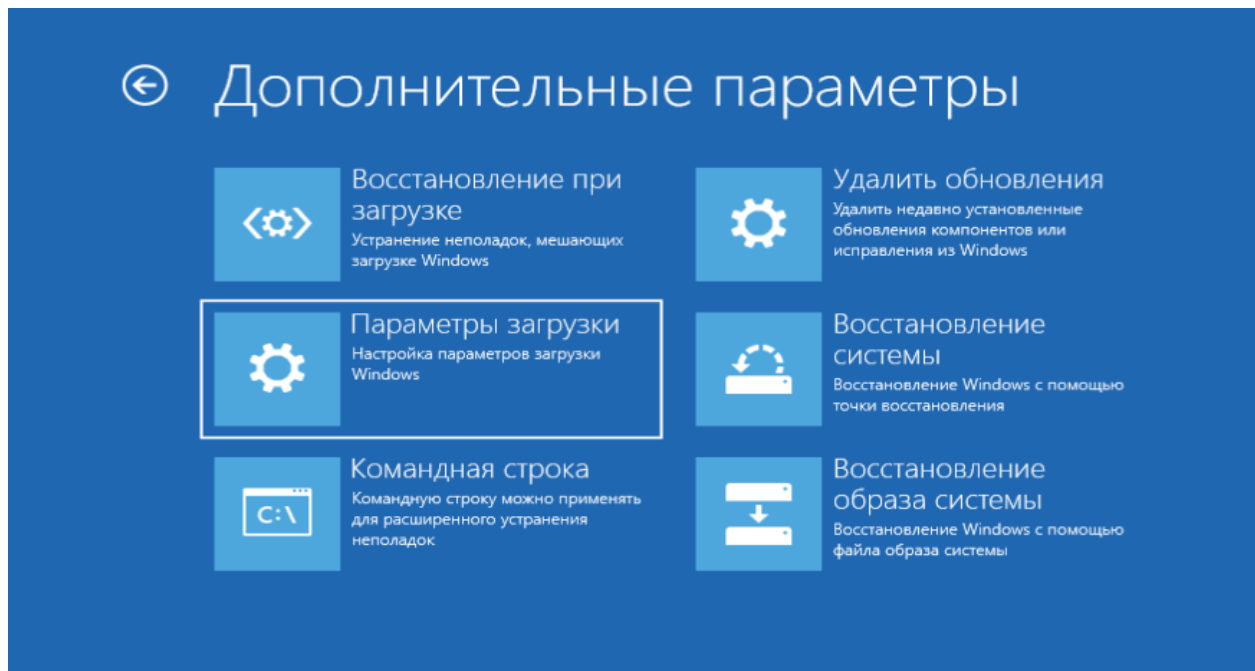
После перезагрузки появится вот такое окно и здесь мы выбираем: **Поиск и устранение неисправностей**.



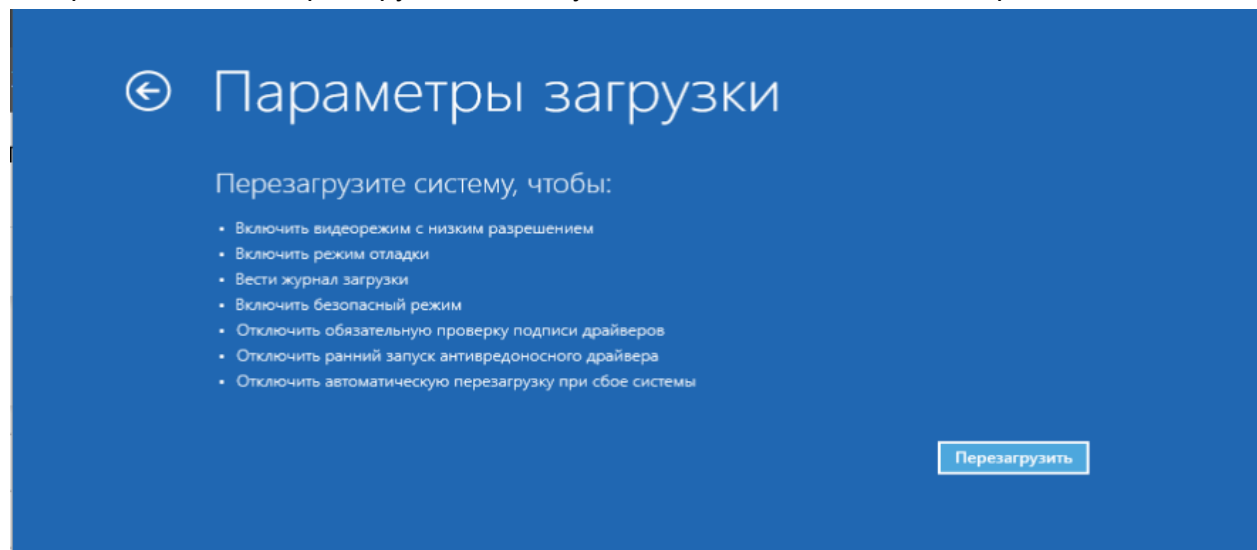
Далее нажимаем: **Дополнительные параметры**



Затем нажимает: **Параметры загрузки**

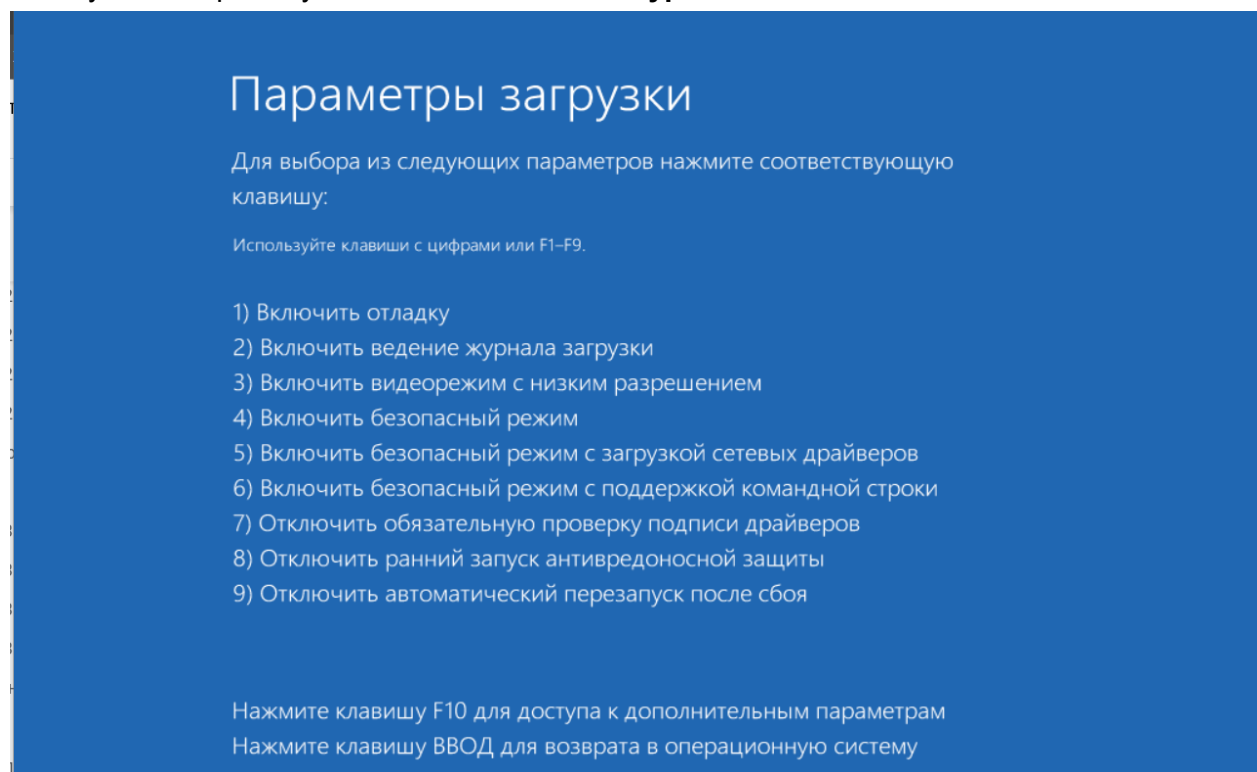


Теперь мы должны перезагрузить систему, чтобы включить безопасный режим.

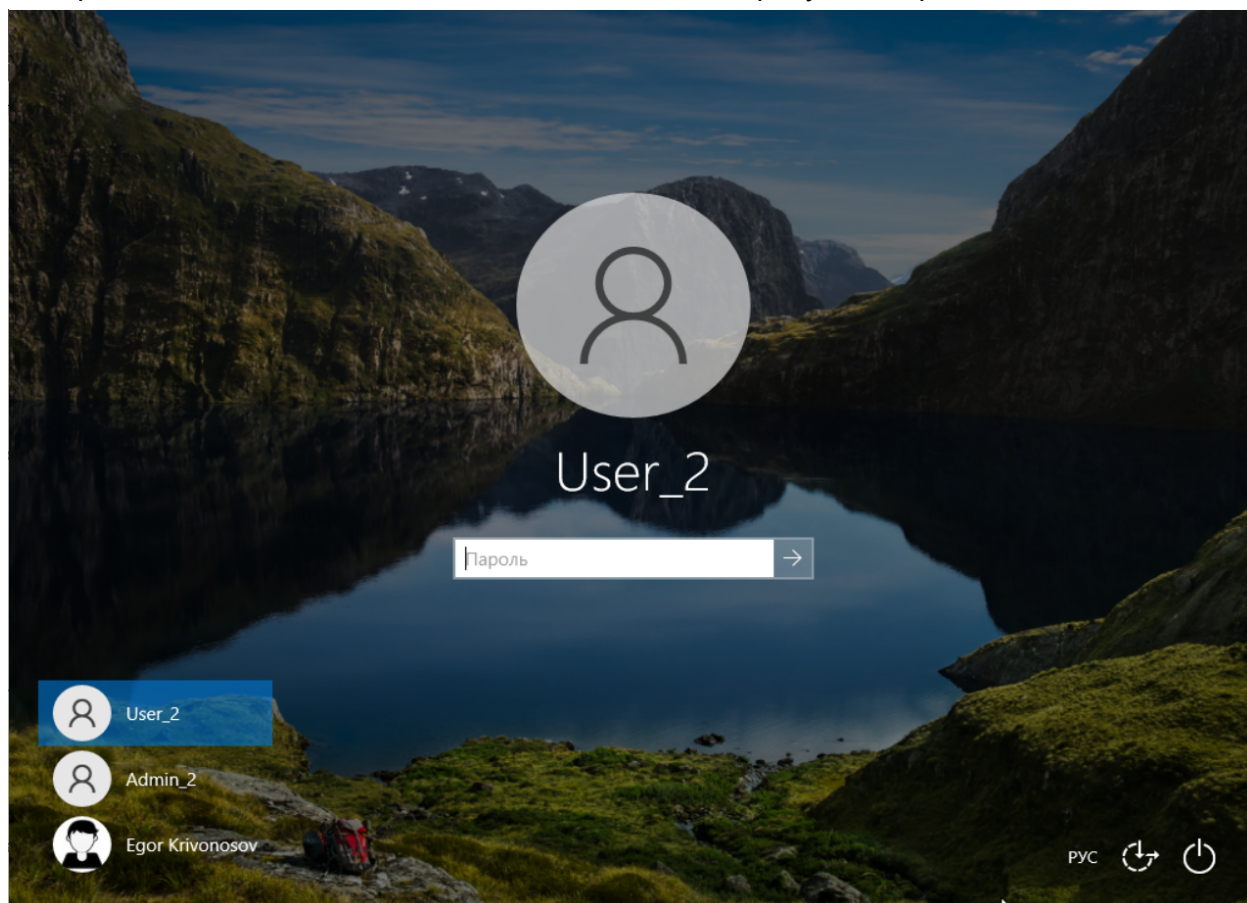


После перезагрузки у нас появится выбор режима загрузки.

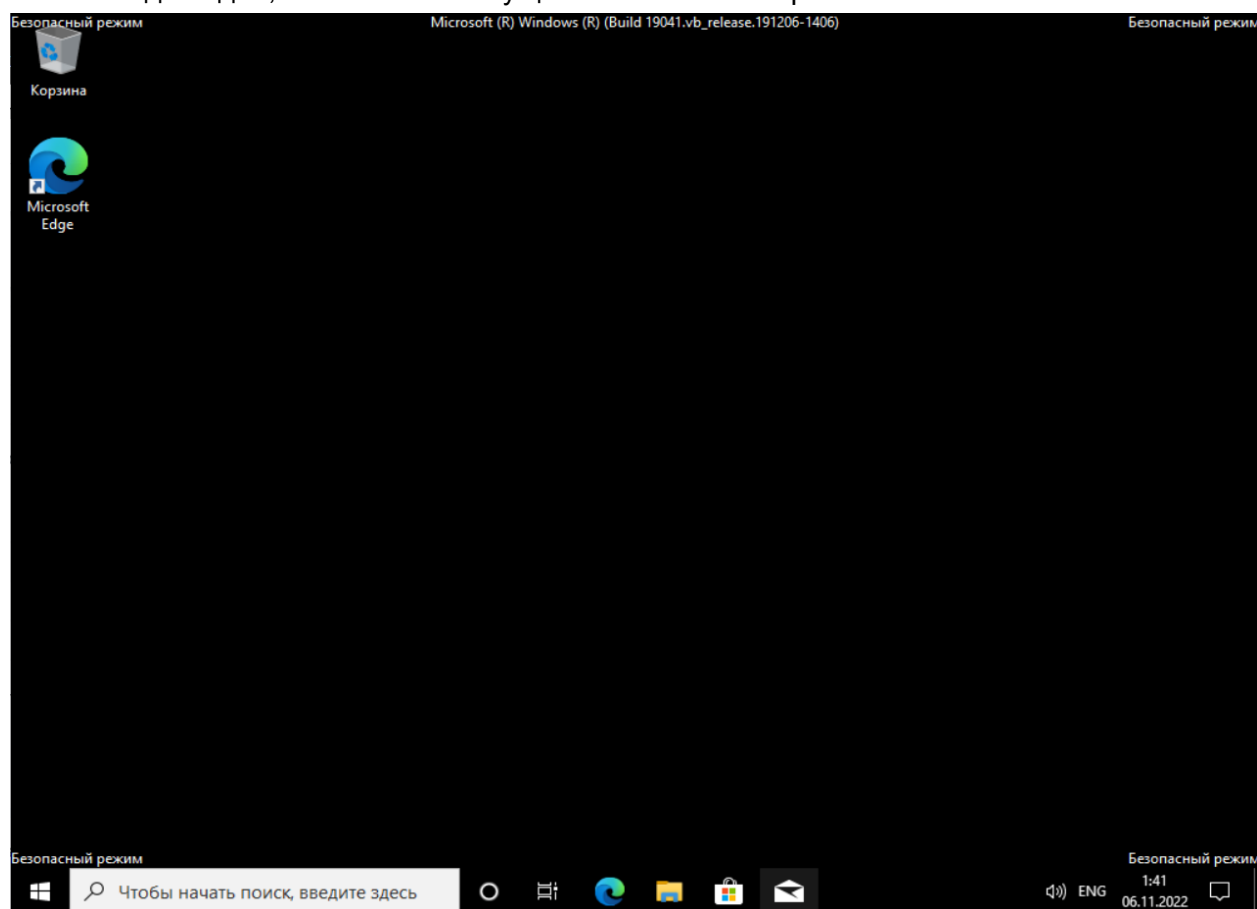
Нам нужно выбрать пункт 4 **нажав на клавиатуре F4**



На экране входа видно, что нет подключения к сети и требуется пароль для входа.



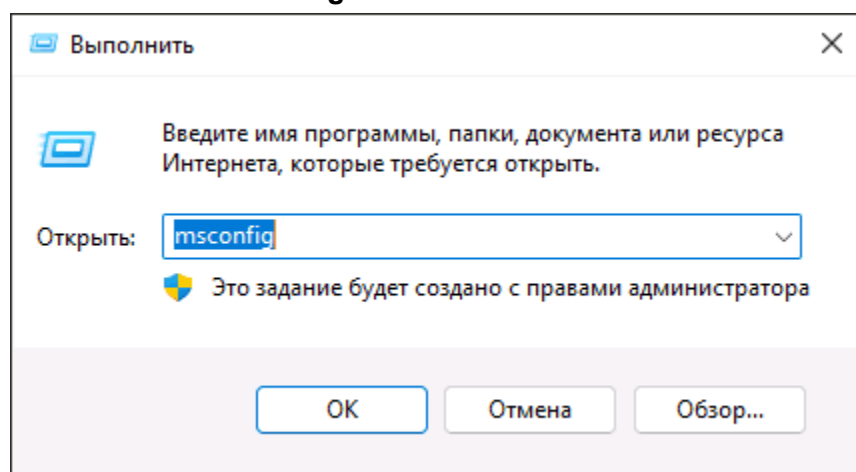
После входа видно, что система запущена в безопасном режиме.



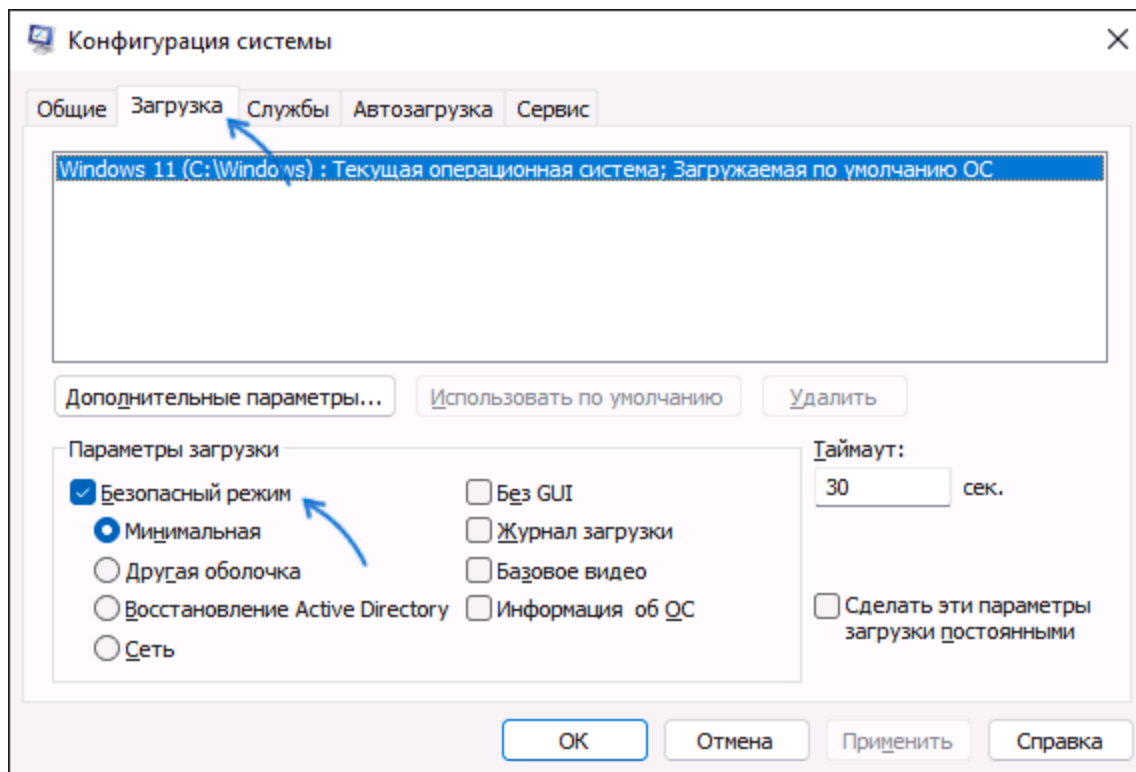
Второй способ попасть в безопасный режим:

Нажать сочетание клавиш **Win + R**

Ввести в поле: **msconfig**



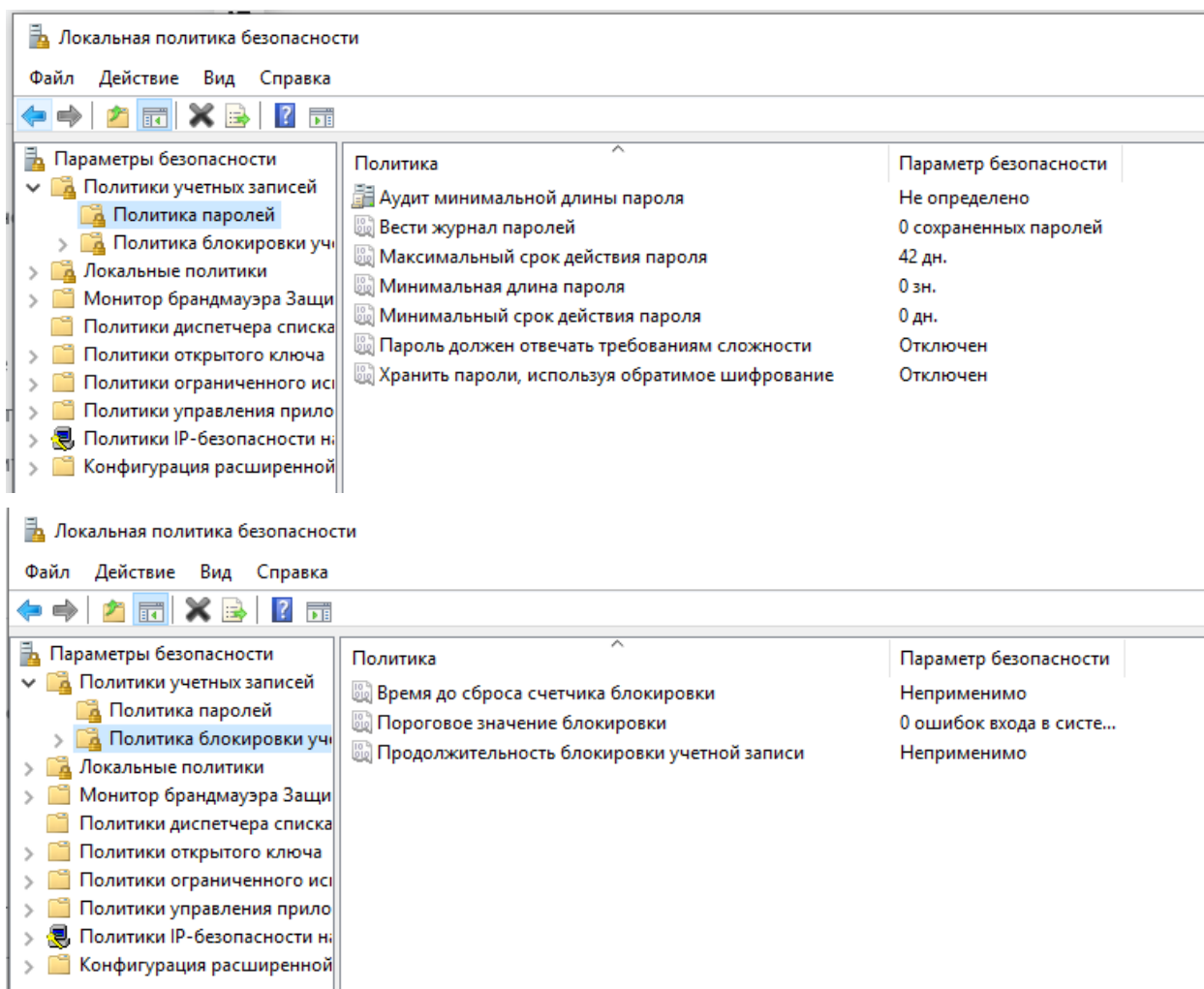
И установить галочку, после чего подтвердить и перезагрузить систему:



Меры повышения надежности парольной защиты

1. наложение технических ограничений (длина, увеличение алфавита (символы разных языков, спецсимволы))
2. управление сроком действия паролей, их периодическая смена;
3. ограничение доступа к файлу паролей
4. ограничение числа неудачных попыток входа в систему, чтобы исключить bruteforce
5. обучение и воспитание пользователей (запрет разглашения)
6. использование программных и аппаратных генераторов паролей
7. ограничение повторяемости паролей (история паролей)

Часть из данных мер можно установить в политике безопасности системы

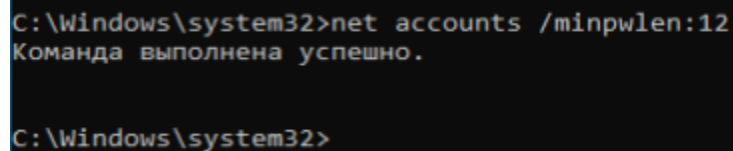


Аналогично, что и выше можно сделать через **Командную строку** используя команды **NET ACCOUNTS**:

- **forcelogoff** - время ожидания в минутах перед отключением пользователя от сервера в случае, если период действия пользовательского имени закончился или истекло время, выделенное для подключения.
- **/minpwlen**- минимальная длина пользовательского пароля.
- **/maxpwage** - период времени в днях, в течение которого будет действовать пароль пользователя.
- **/minpwage** - минимальное количество дней, которые должны пройти перед сменой пароля пользователем.
- **/uniquepw** - запрет на повторное использование заданного числа последних паролей.

Пример команды:

net accounts /forceloff:30 /minpwlen:0



```
C:\Windows\system32>net accounts /minpwlen:12
Команда выполнена успешно.

C:\Windows\system32>
```

Запуск системы в безопасном режиме и использование парольной защиты увеличивают защищенность системы. Даже зная пароль, злоумышленник получит доступ к ограниченному безопасным режимом набору служб. Однако он может перезапустить систему в обычном режиме.

Выполненные мной настройки механизма защиты в виде установки пароля для пользователя не удовлетворяют множеству требований из списка в руководящих документах: требованиям “Очистка памяти”, “Дискреционный принцип контроля доступа”, “Руководство для пользователя” и т.д, так как это - функциональность непосредственно ОС Windows 10. Настройка входа по паролю направлена выполнение требования об идентификации и аутентификации.

Анализ реализации механизма защиты в ОС Windows 10

Операционная система Windows 10 не имеет сертификата ФСТЭК (Федеральная служба по техническому и экспортному контролю) от НСД (Несанкционированного доступа), но имеет сертификат №4369, устанавливающий 6 уровень доверия к системе по документу «Требования по безопасности 26 информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020). Уровень доверия к системе достаточно низкий, из чего можно сделать вывод, что механизм защиты в системе Windows 10 недостаточно надежный для использования системы в значимых объектах. В то же время можно утверждать, что для использования системы на большинстве персональных компьютерах уровень надежности является достаточным.

С точки зрения руководящего документа “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.” Windows 10 относится к классу систем 1Г (так как является многопользовательской, в которой одновременно хранится/обрабатывается информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации). Она удовлетворяет следующим требованиям:

- **Идентификация, проверка подлинности и контроль доступа субъектов**
В рамках данного требования пользователь должен иметь возможность идентификации и аутентификации, система должна иметь средства проверки

подлинности пользователя, а также должна препятствовать доступу к защищаемым ресурсам от неидентифицированных пользователей, что реализовано с помощью ввода логина и пароля или входа по биометрическим данным и т.д.

- **Регистрация и учет**

В рамках данного требования система должна осуществлять регистрацию входа (выхода) субъектов доступа в систему (из системы) и прочие действия пользователя. Реализовано внутри ОС Windows 10.

- **Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей**

Данное требование определяет поведение системы при завершении работы конкретных процессов, выполняемых алгоритмов. В Windows 10 отсутствует шифрование конфиденциальной информации и использование сертифицированных криптографических средств, что не позволяет отнести ее к более высокому классу

- **Обеспечение целостности**

Наличие средств восстановления - система защиты информации от несанкционированного доступа

С точки зрения руководящего документа “Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации” Windows 10 относится к шестому классу защищенности: рассмотрим следующие требования:

- **Дискреционный принцип контроля доступа**

В рамках данного требования необходимо контролировать доступ наименованных субъектов (пользователей) к наименованным объектам, а это реализовано с помощью ассоциирования пользователя с группой.

- **Идентификация и аутентификация**

В рамках данного требования пользователь должен иметь возможность идентификации и аутентификации, система должна иметь средства проверки подлинности пользователя, а также должна препятствовать доступу к защищаемым ресурсам от неидентифицированных пользователей, что реализовано с помощью ввода логина и пароля или входа по биометрическим данным и т.д.

- **Руководство для пользователя**

В рамках данного требования система должна иметь документацию, содержащую краткое руководство для пользователя с описанием способов использования. Это реализовано путем наличия справки внутри Windows 10.

- **Обеспечение целостности программных средств и обрабатываемой информации**

Данное требование соблюдено не полностью, так как существуют урезанные сборки Windows 10, запускающиеся без определённых системных служб, системных приложений и параметров реестра. При этом можно самостоятельно вызывать утилиты и нарушить целостность системы. Из-за несоблюдения данного требования система не может быть причислена к пятому классу защищенности.

Дополнительная часть

Задание 3

Опишите отличия компонентов биометрической службы Windows 10 от предыдущих версий ОС

Выполнение

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

Основные отличия между версиями:

- **Встроенная поддержка распознавания лиц**

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

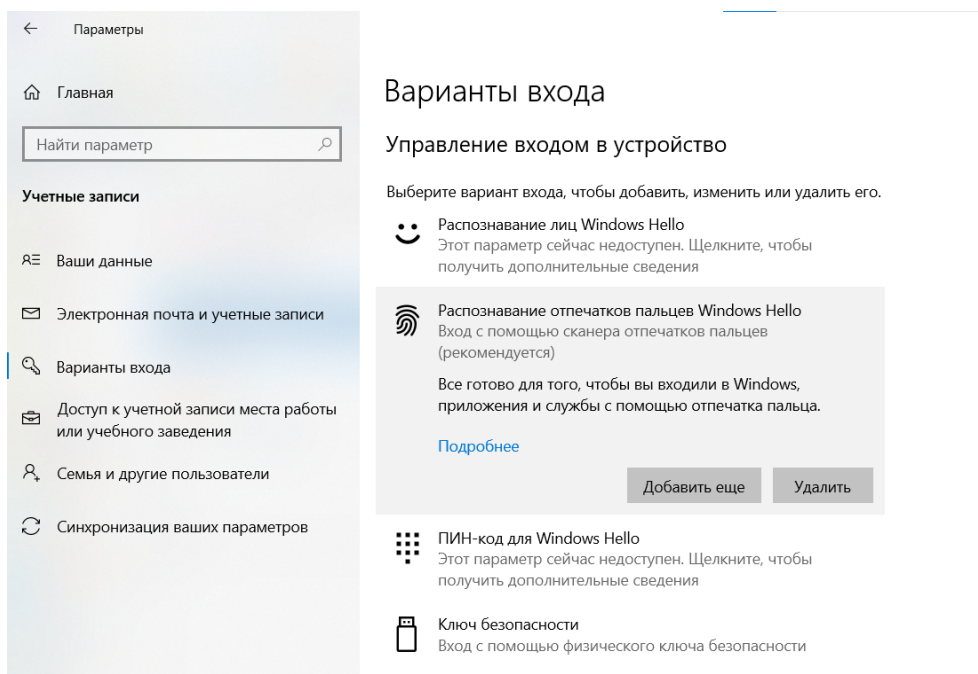


- **Объединение двухфакторной аутентификации и биометрического распознавания в одном модуле**

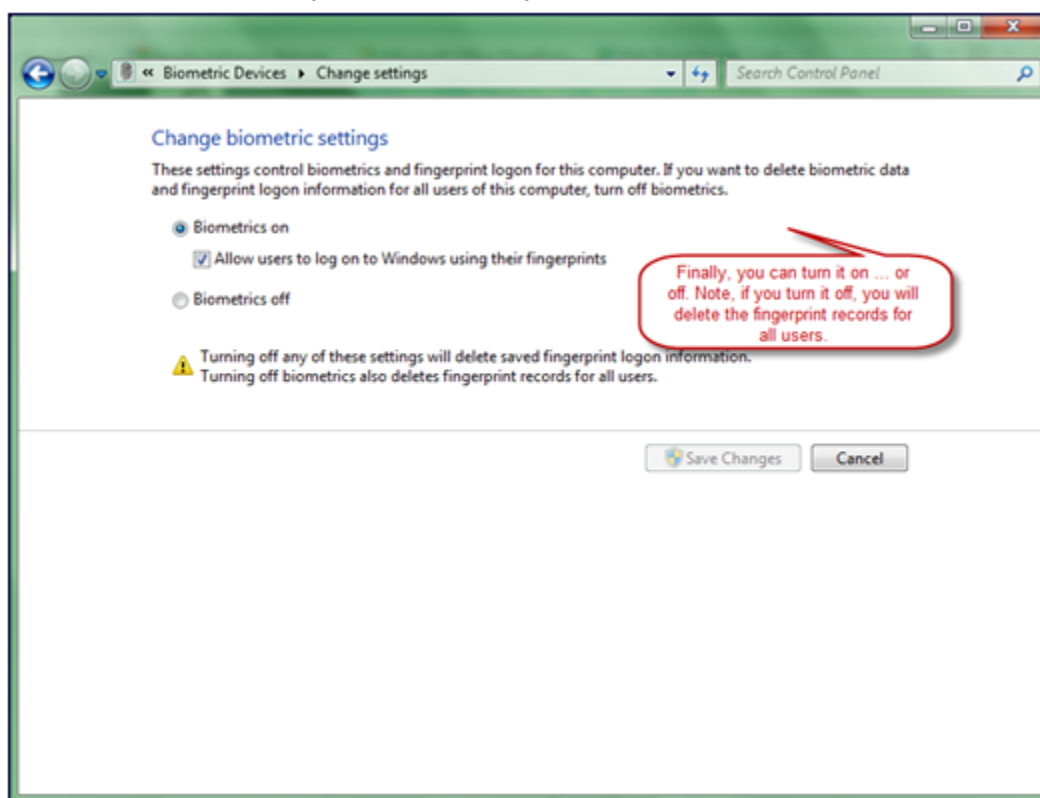
В первоначальной версии Windows Hello данной интеграции не было, однако её переместили позже в один модуль для удобства.

- **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.



Вывод

В процессе выполнения данной лабораторной работы были изучены различные способы создания учетных записей, выполнена настройка политик безопасности и рассмотрена сертификация ФСТЭК для системы Windows 10.