

Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
“НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО”

Факультет Программной инженерии и компьютерной техники



Отчет

По лабораторной работе Windows 1

Учетные записи и авторизация в ОС MS Windows

По предмету: Информационная безопасность

Вариант 1

Студент:

Андрейченко Леонид Вадимович

Группа Р34301

Преподаватель:

Маркина Татьяна Анатольевна

Санкт-Петербург

2023

Содержание

Цель работы.....	3
Программные и аппаратные средства используемые при выполнении работы.....	3
Основная часть.....	4
1 Определения.....	4
2 Создание пользователя.....	4
Вариант 2.1.....	4
Вариант 2.2.....	7
Вариант 2.3.....	9
Вариант 2.4.....	10
Возможности.....	11
3 Создание администратора.....	17
Вариант 3.1.....	17
Вариант 3.2.....	19
Вариант 3.3.....	20
Ограничения.....	22
4 Политики UAC (User Account Control).....	24
5 Задание по варианту.....	26
Анализ реализации механизма защиты в ОС Windows 10.....	29
Дополнительная часть.....	31
1 Опишите создание профиля пользователя и его копирование (на основе Windows Server).....	31
2. Опишите настройку и работу со смарт-картами.....	38
3. Опишите отличия компонентов биометрической службы Windows 10 от предыдущих версий ОС.....	40
Выводы.....	43

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 Windows 10:

Характеристики устройства

Имя устройства	Win10Pro
Процессор	Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz
Оперативная память	4.00 ГБ
Код устройства	5EA3BFC0-5C78-4B1A-BD50- F74F6675028D
Код продукта	00328-10000-00001-AA567
Тип системы	64-разрядная операционная система, процессор x64
Перо и сенсорный ввод	Для этого монитора недоступен ввод с помощью пера и сенсорный ввод

Характеристики созданной виртуальной машины Windows Server 2019:

Характеристики устройства

Имя устройства	server
Процессор	Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz
Оперативная память	4.00 ГБ
Код устройства	8031BBF1-FE07-44A5-98DE-D2F8585A05F6
Код продукта	00429-70000-00000-AA787
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 Определения

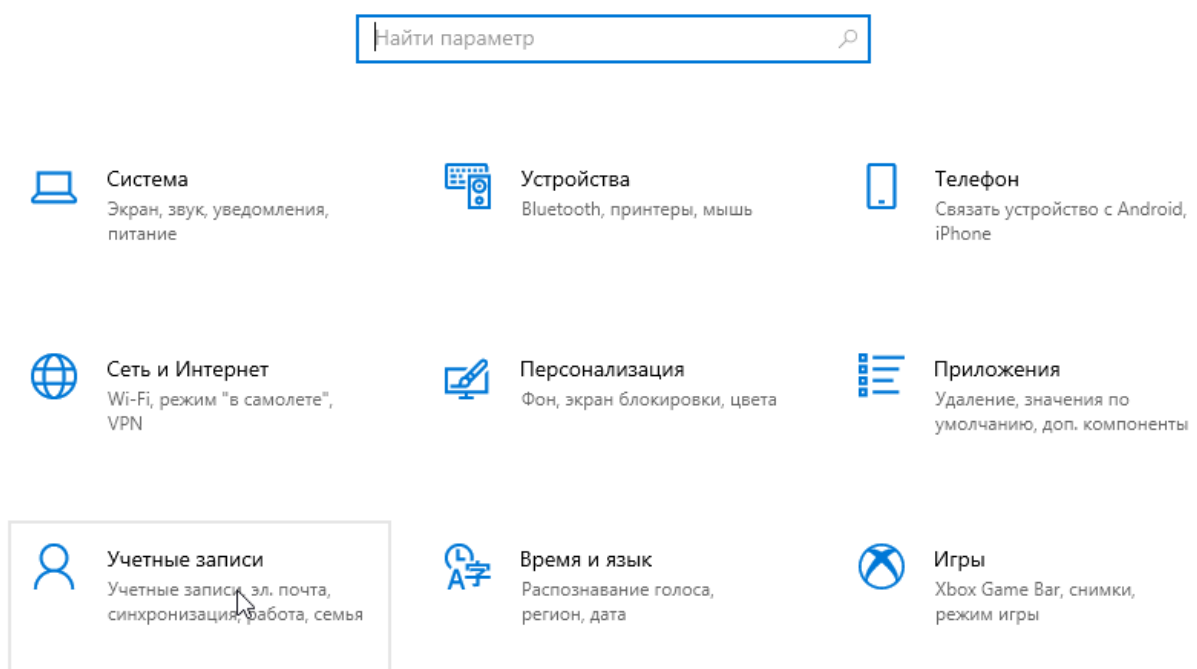
- диспетчер учетных записей (SAM - Security Account Manager)
- монитор безопасности (SRM - Security Reference Monitor)
- маркер доступа (access token)
- идентификатор безопасности (SID - Security Identifier)
- привилегии пользователя
- права пользователя (user rights)
- объект доступа
- субъект доступа
- олицетворение (impersonation)
- список контроля доступа (ACL - Access Control List)
- учетная запись
- домен

2 Создание пользователя

Вариант 2.1

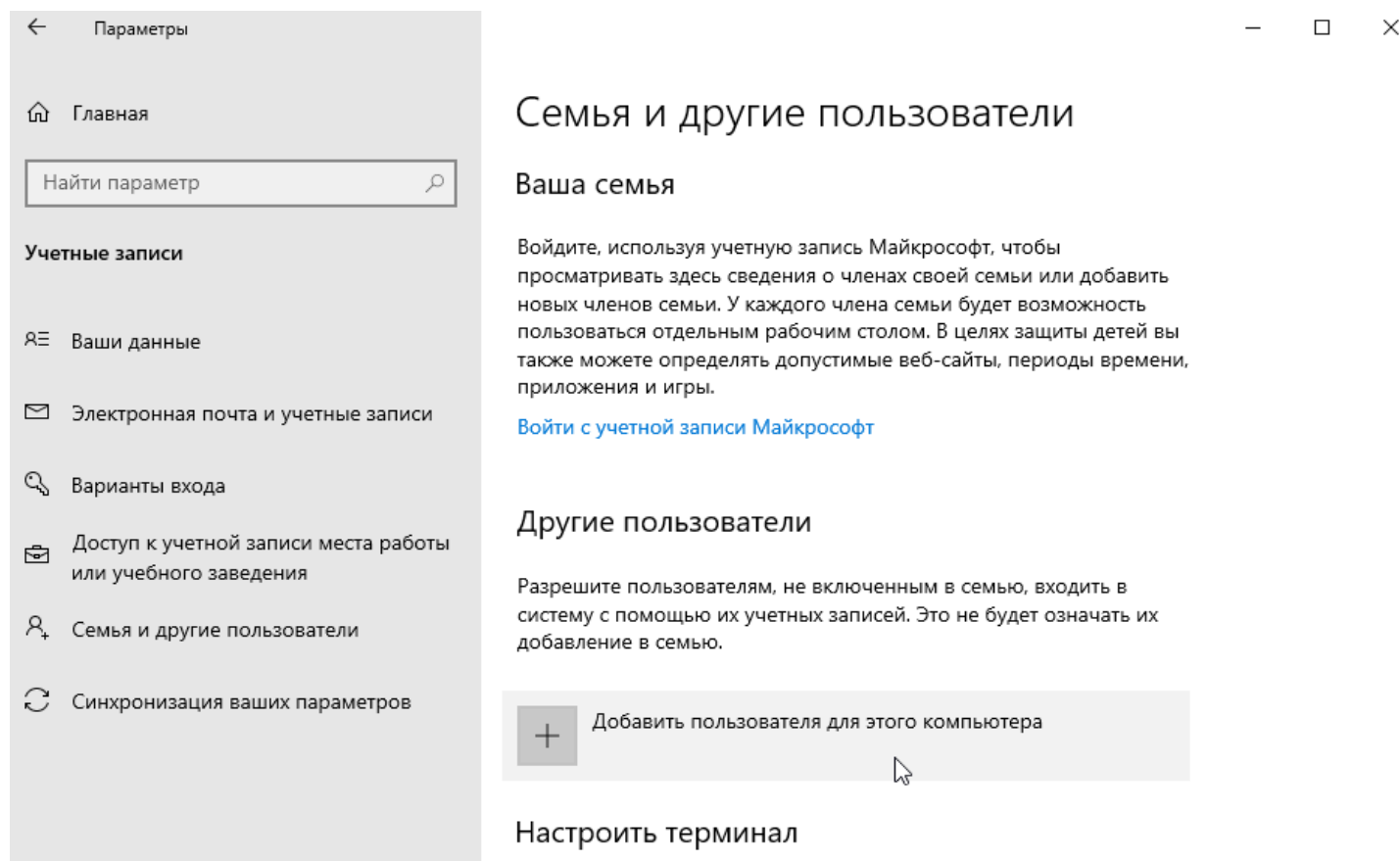
Откроем “Параметры” и выберем пункт “Учетные записи”

Параметры Windows

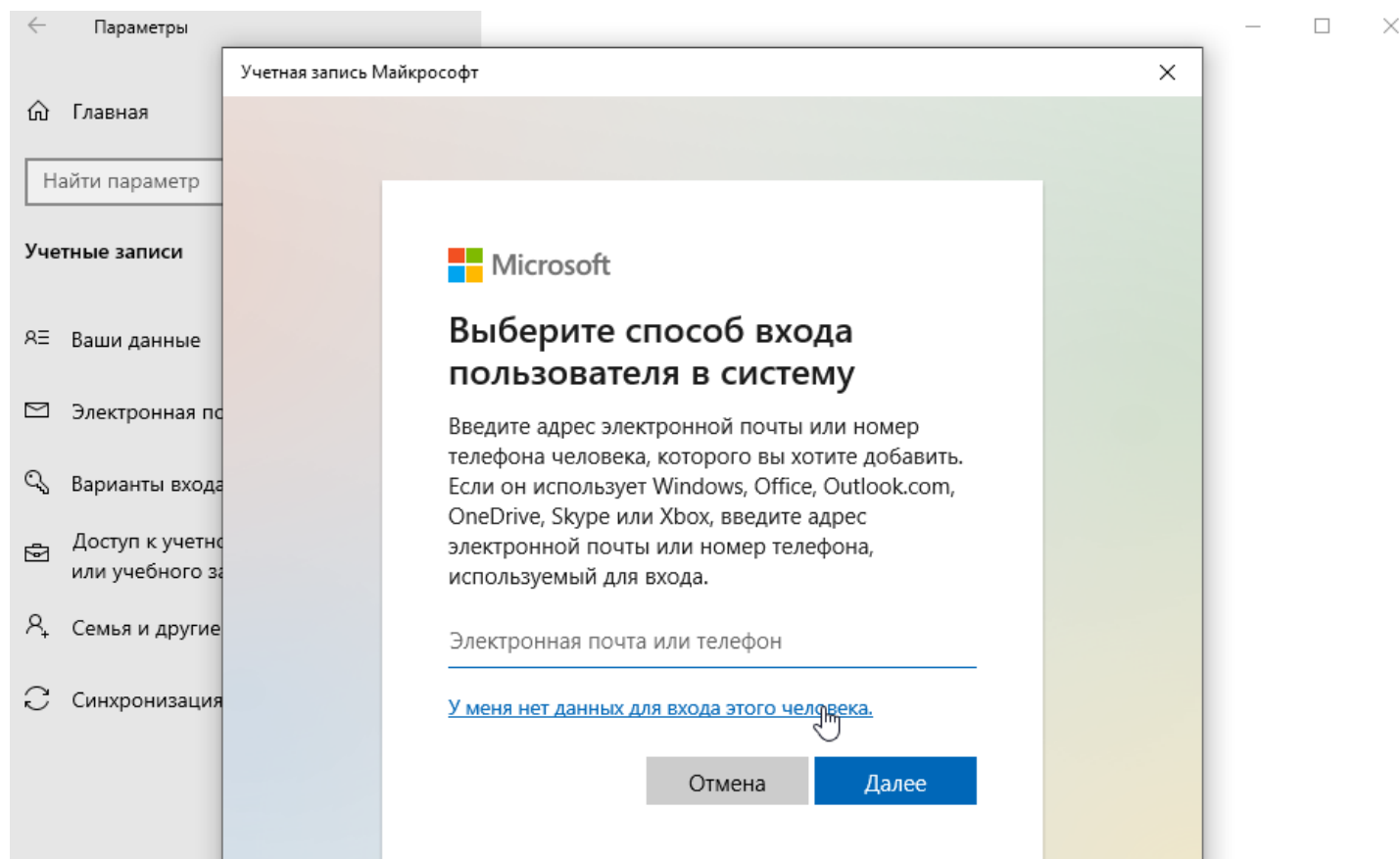


Выбрать пункт: Семья и другие пользователи

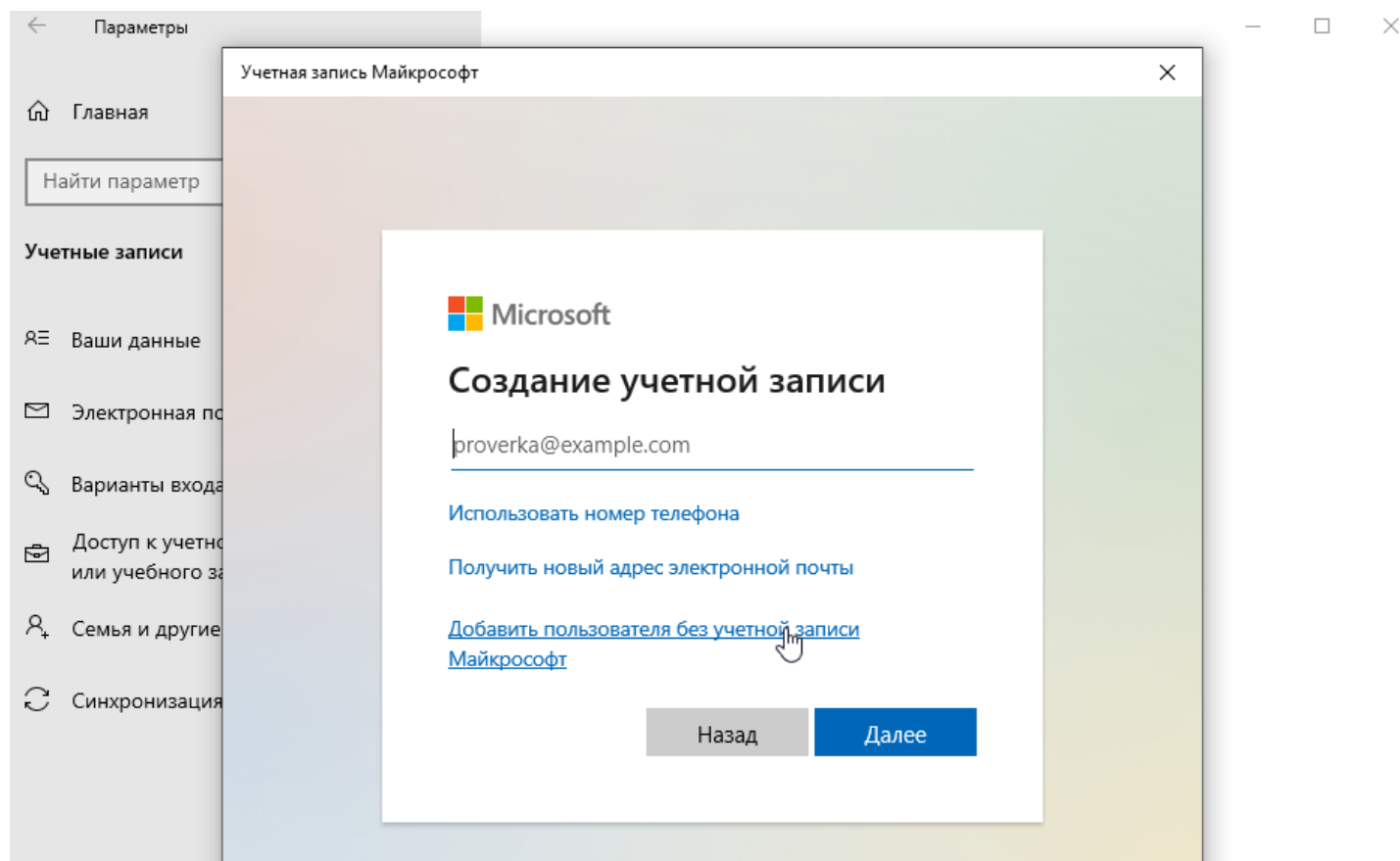
Выбрать пункт: Добавить пользователя для этого компьютера



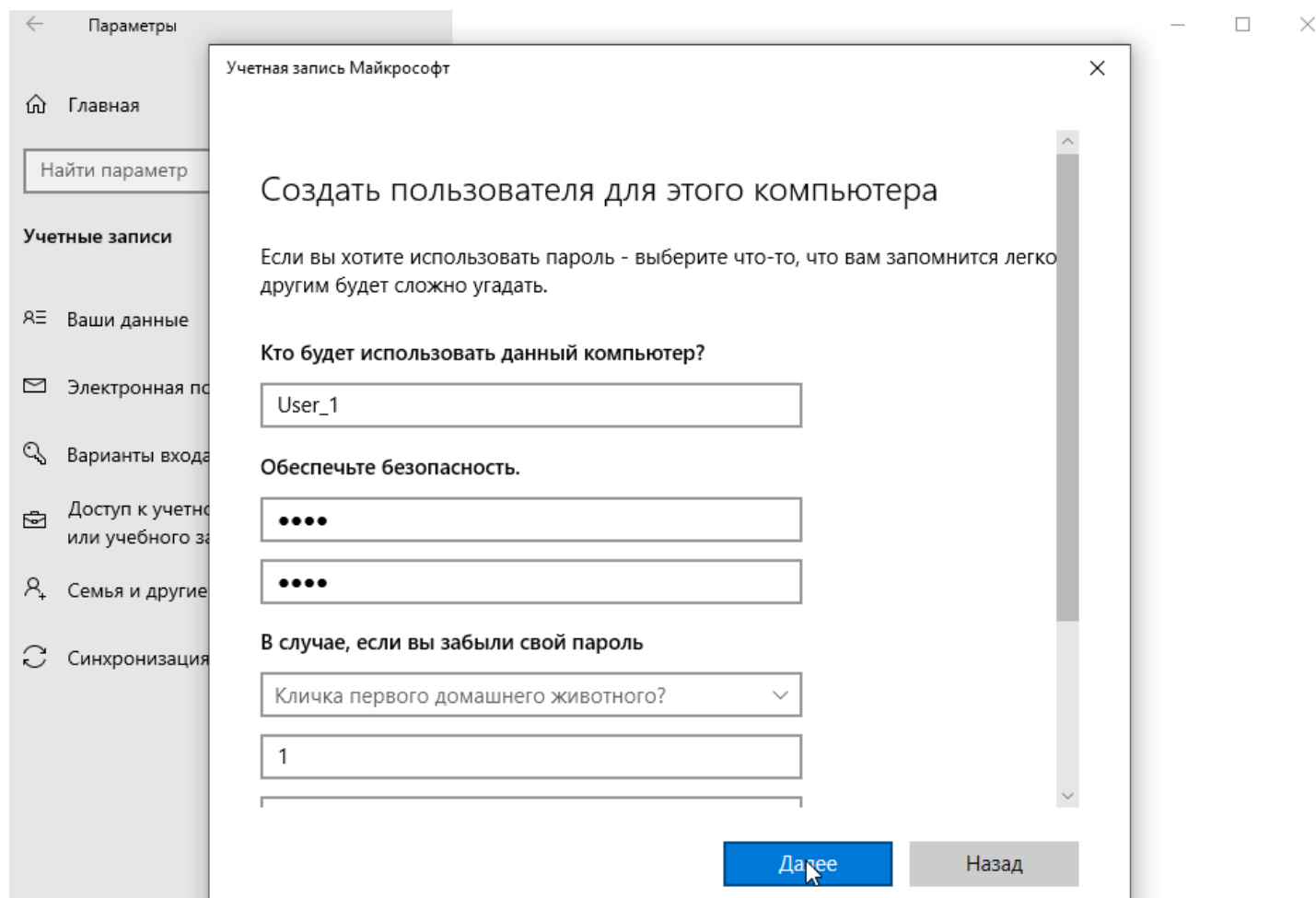
Выбрать пункт: У меня нет данных для входа этого человека



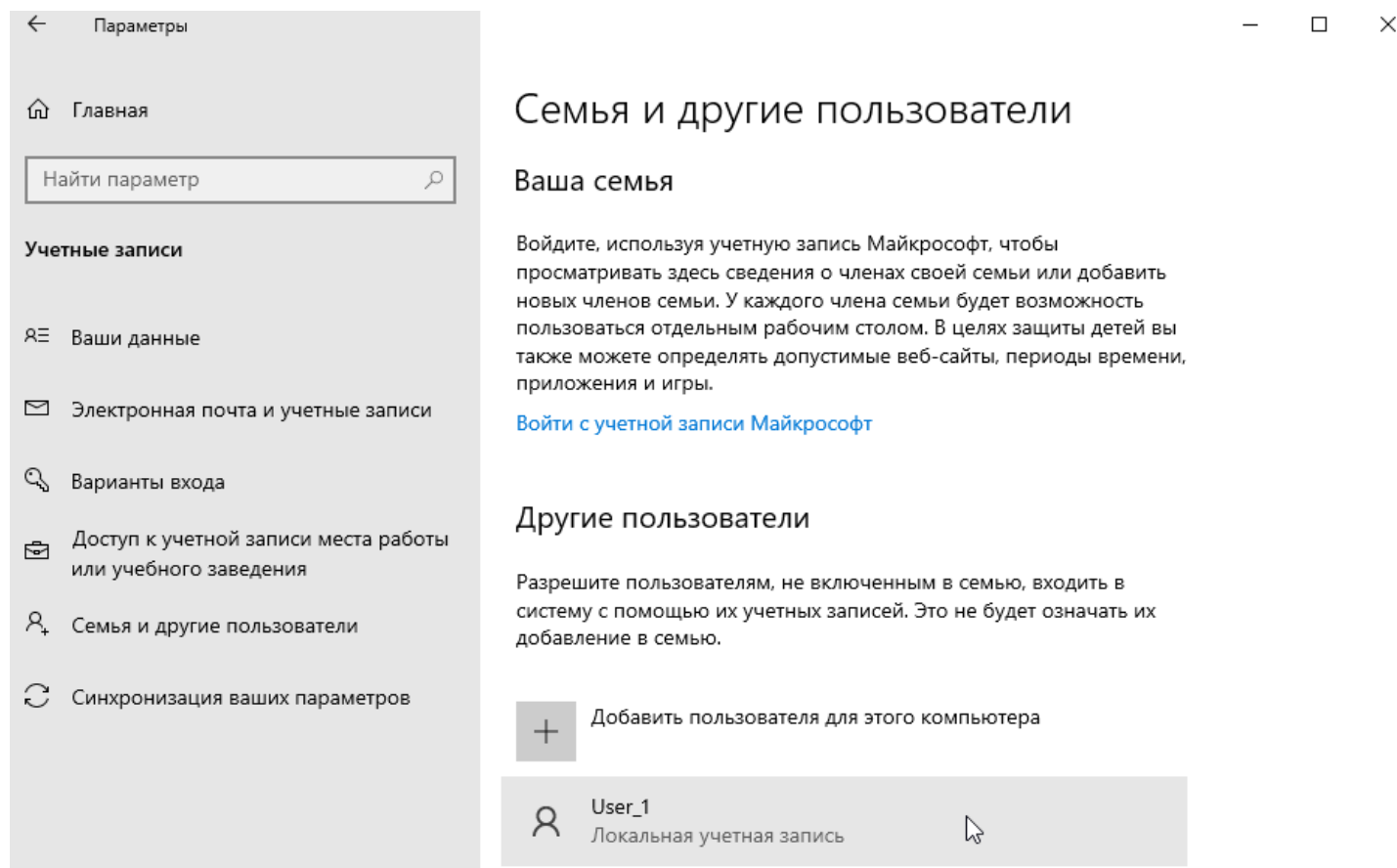
Выбрать пункт: Добавить пользователя без учетной записи Майкрософт



Затем вводим все необходимые данные для учетной записи

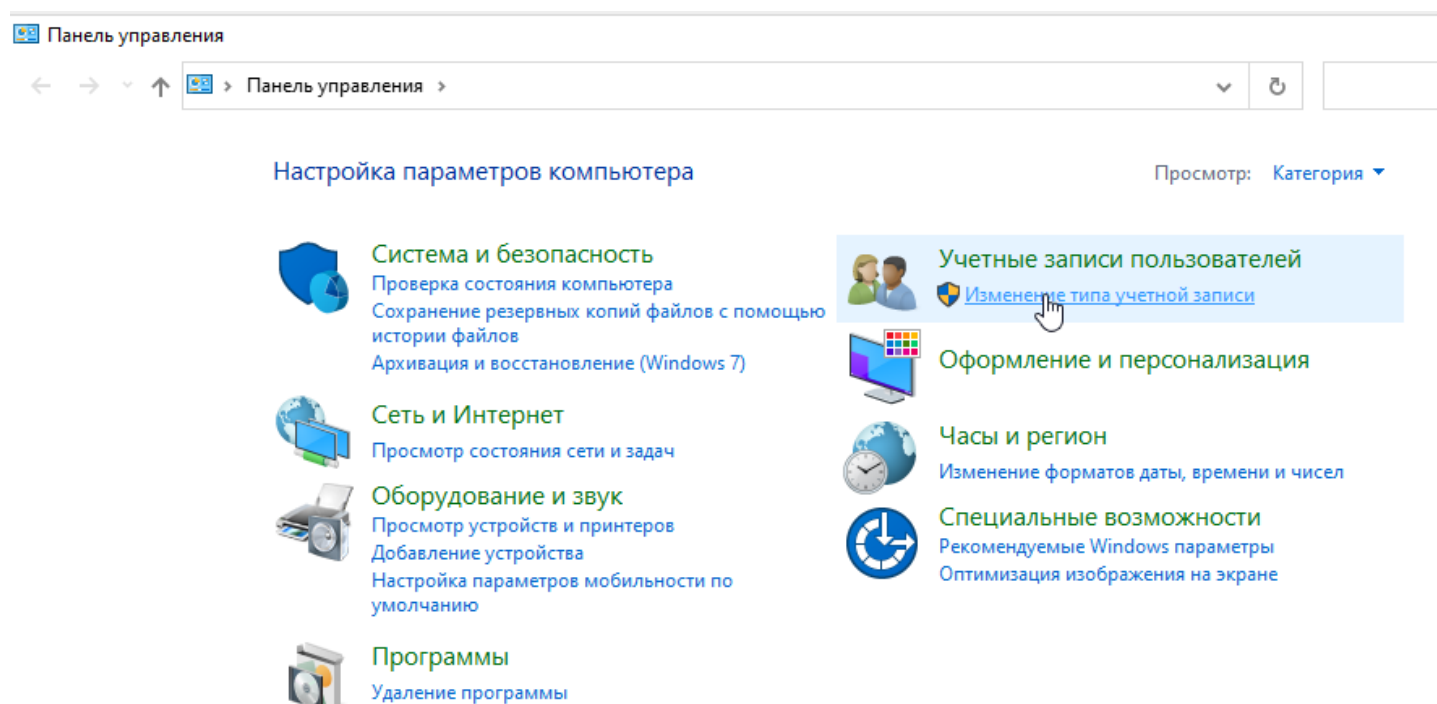


После этих действий создастся пользователь

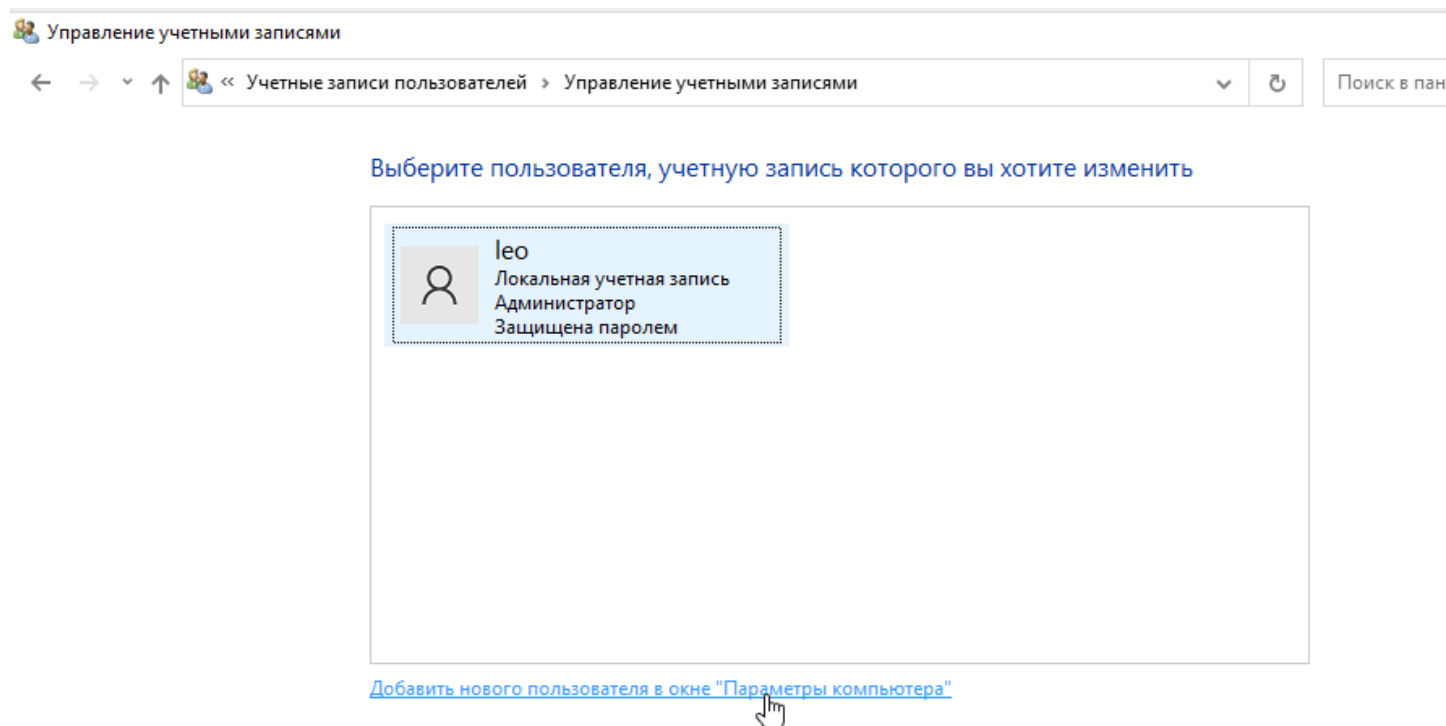


Вариант 2.2

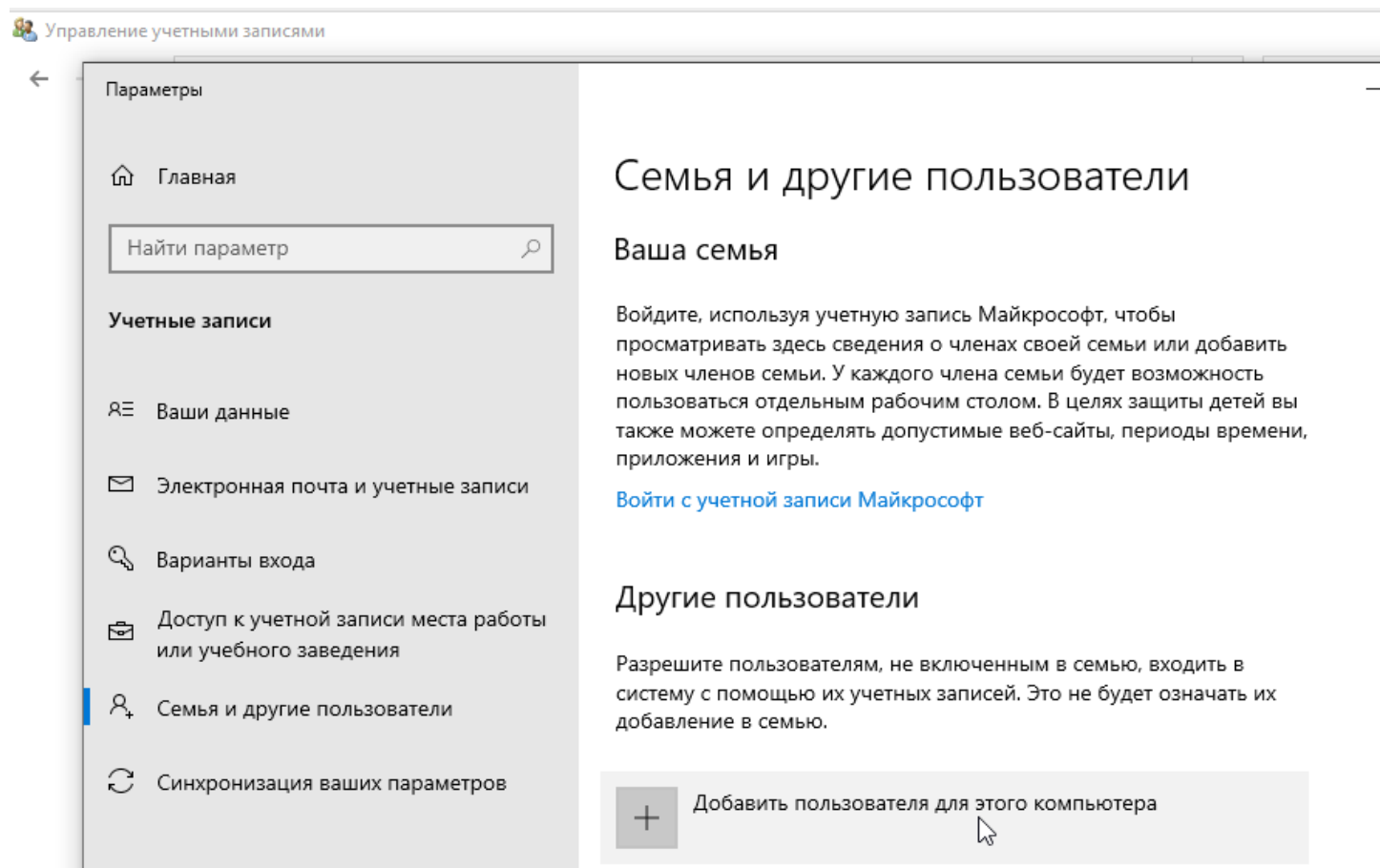
Открываем “Панель управления” и выбираем пункт “Изменение типа учетной записи”



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

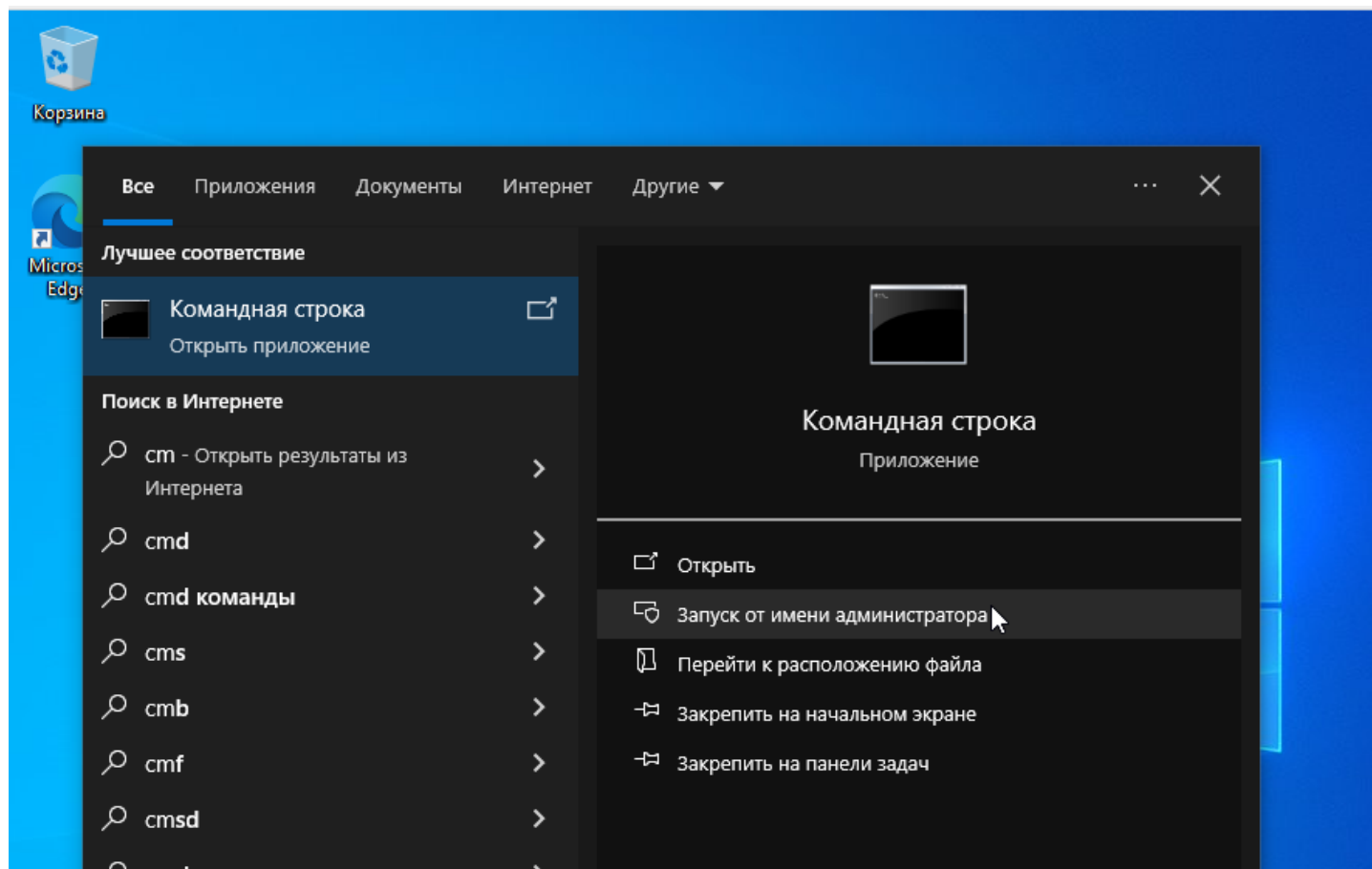


Затем повторяем те же самые действия, как и в Вариант 2.1

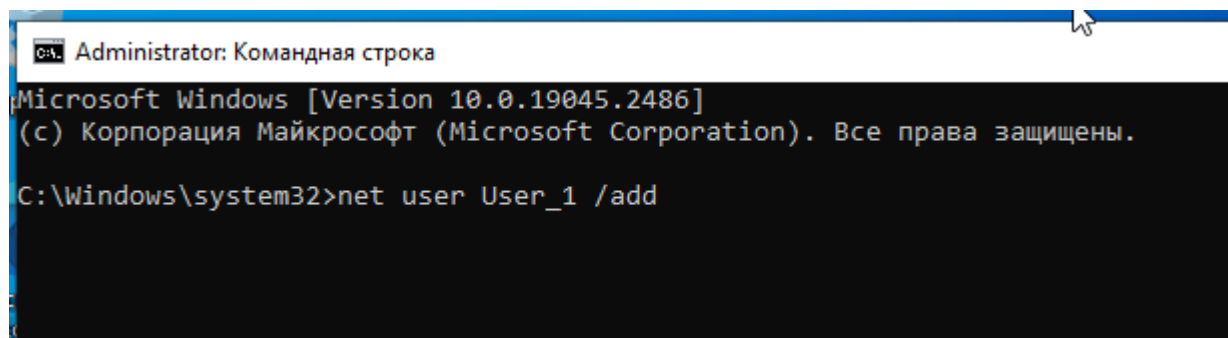


Вариант 2.3

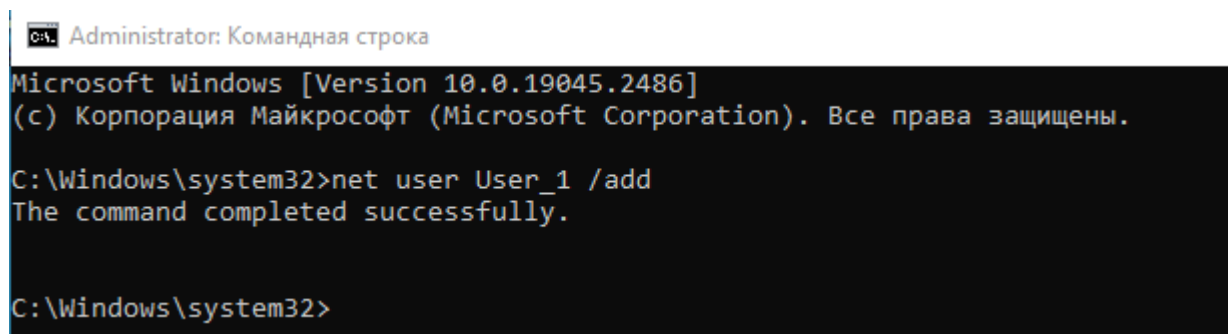
Запускаем “Командная строка” от имени администратора.



Вводим команду: `net user User_1 /add`



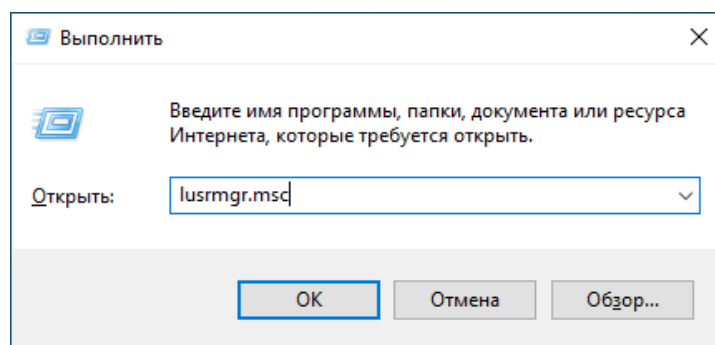
Жмем enter:



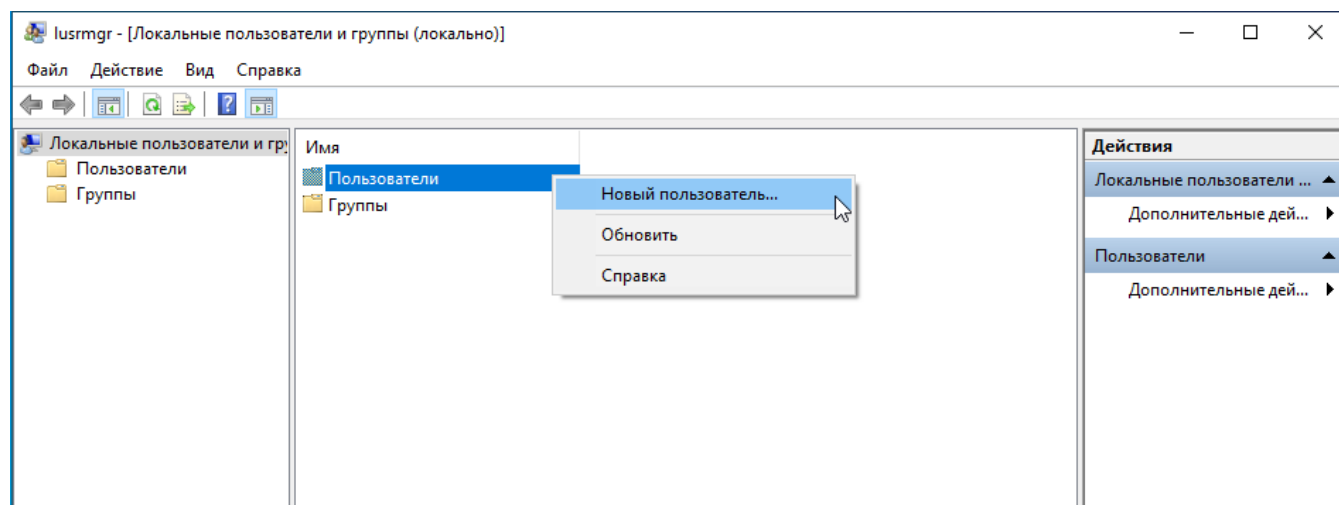
Вариант 2.4

Жмем сочетание клавиш Win + R

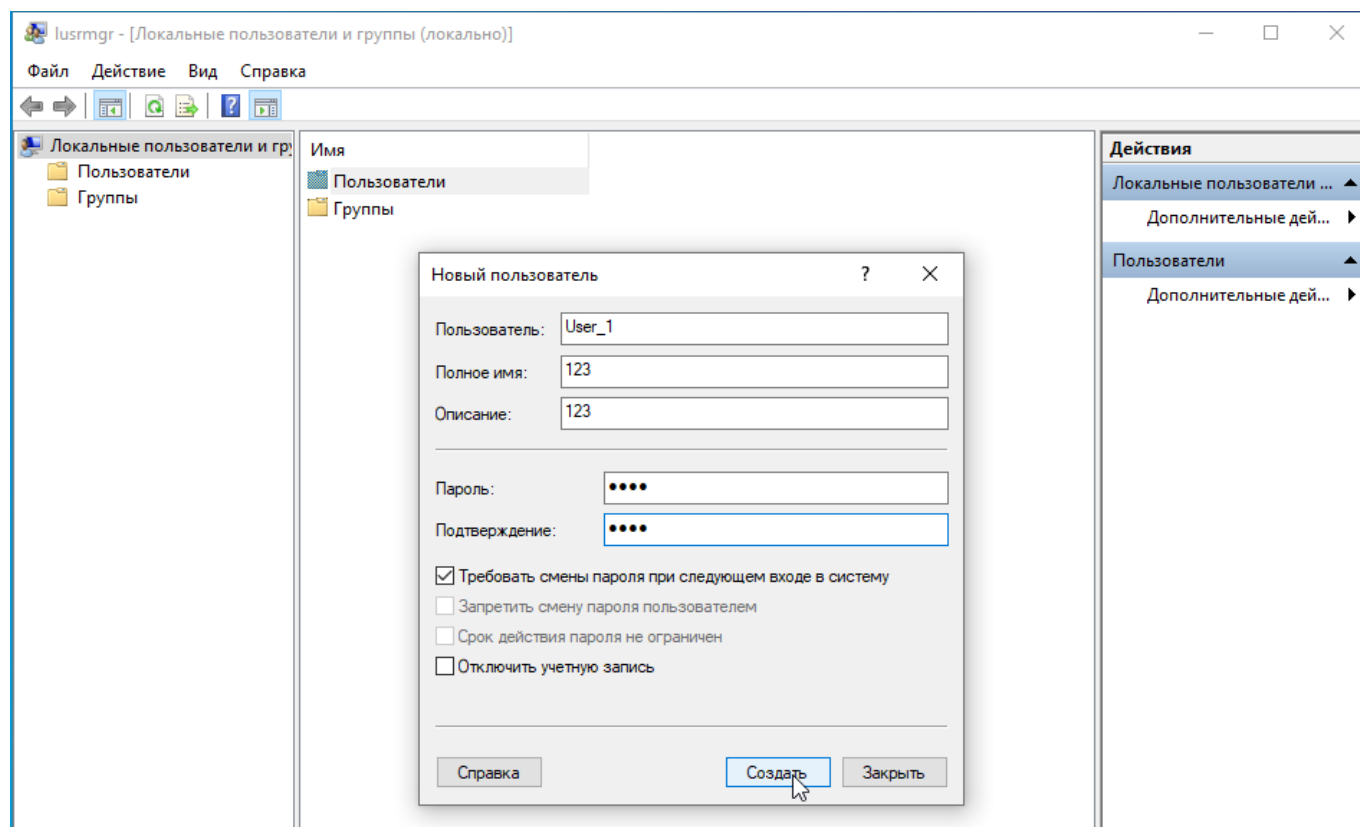
Вводим в появившейся строке: lusrmgr.msc



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



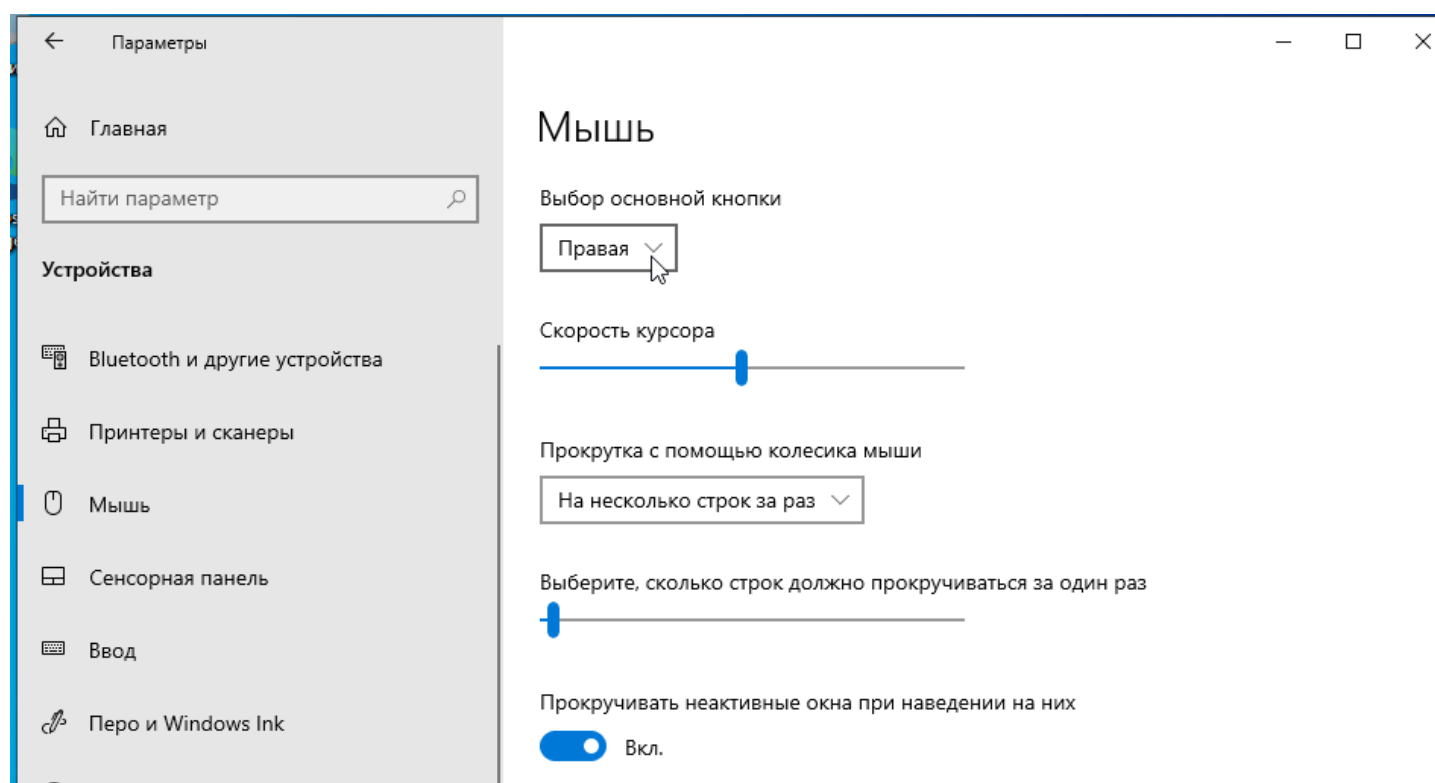
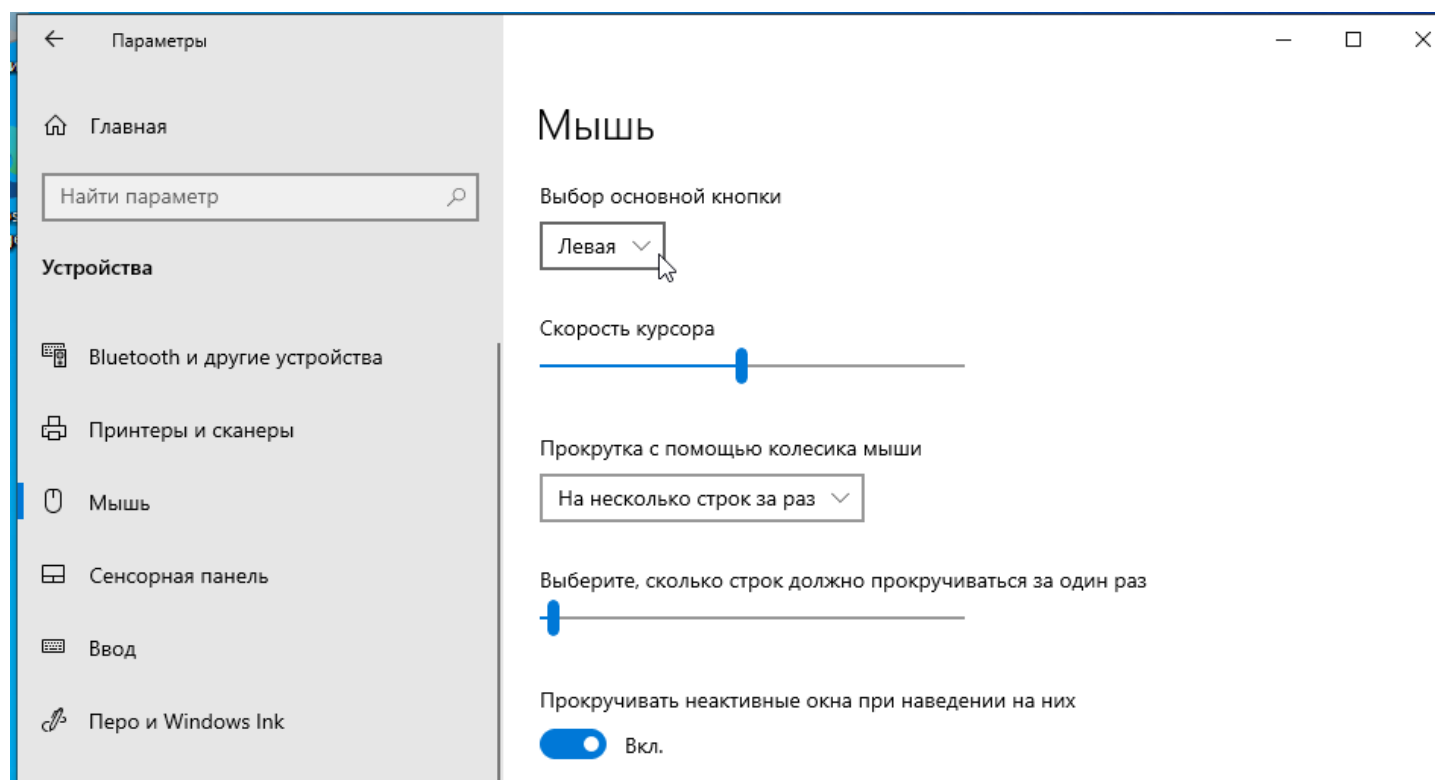
Вводим необходимые данные и нажимаем кнопку “Создать”



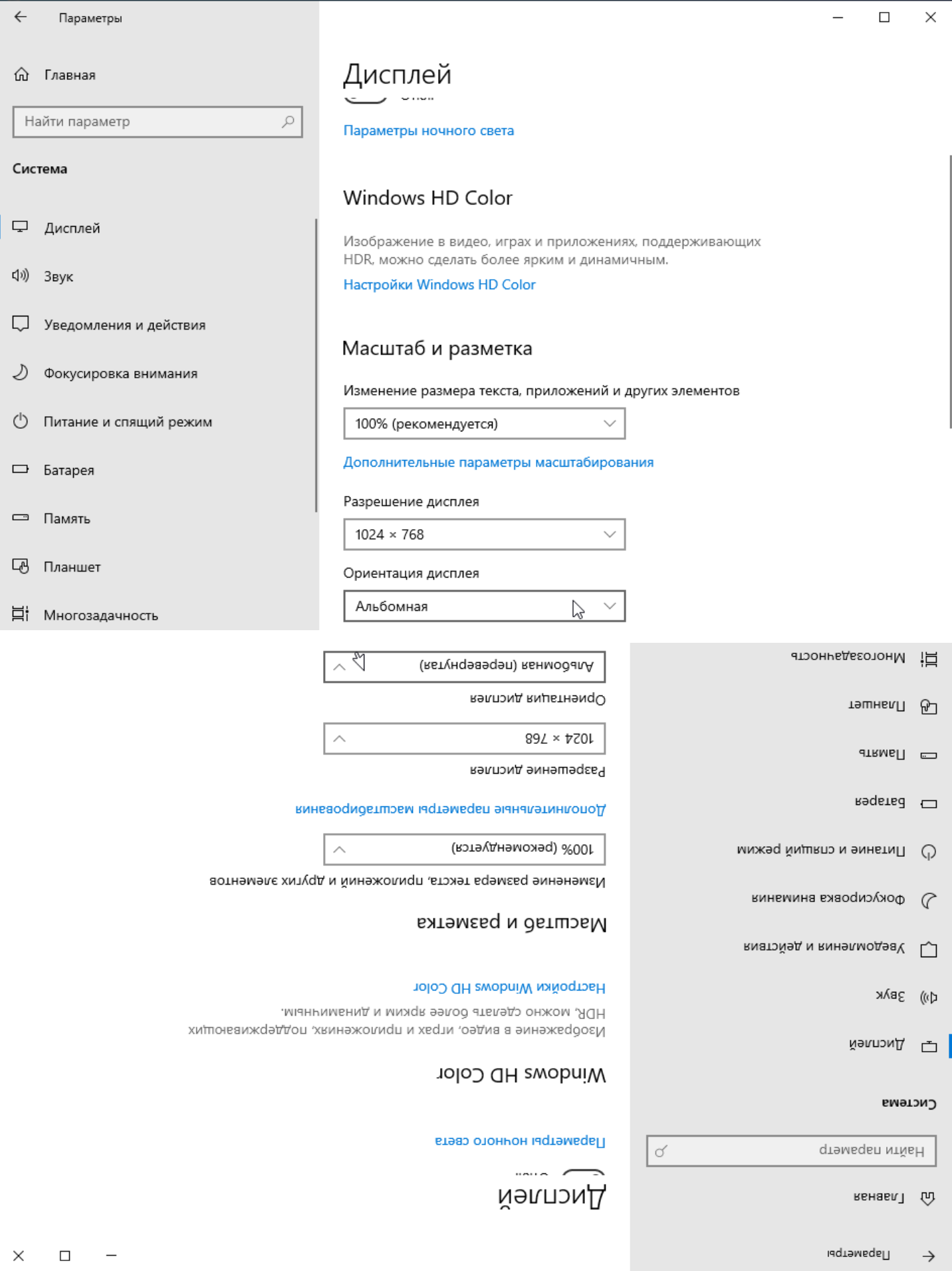
Возможности

Пользователь в Параметрах может изменить конфигурацию мыши в системе.

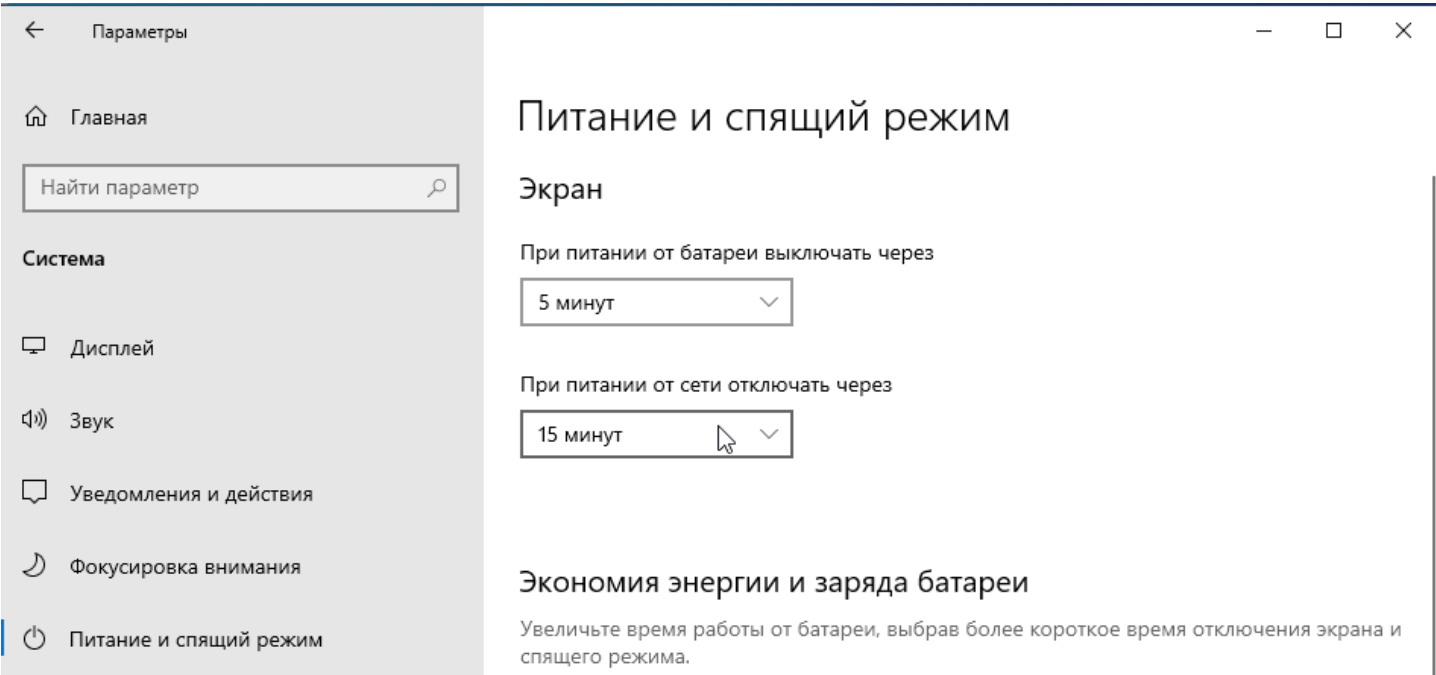
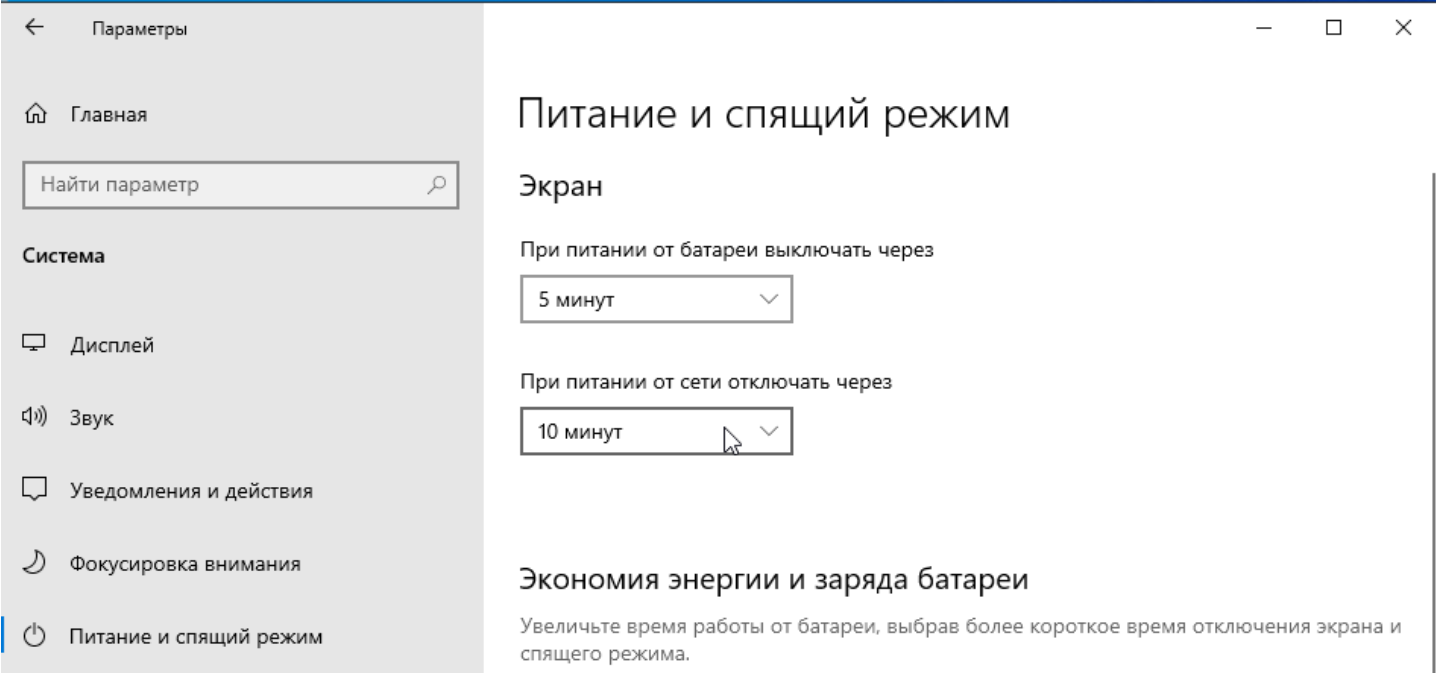
Например, изменить основную кнопку:



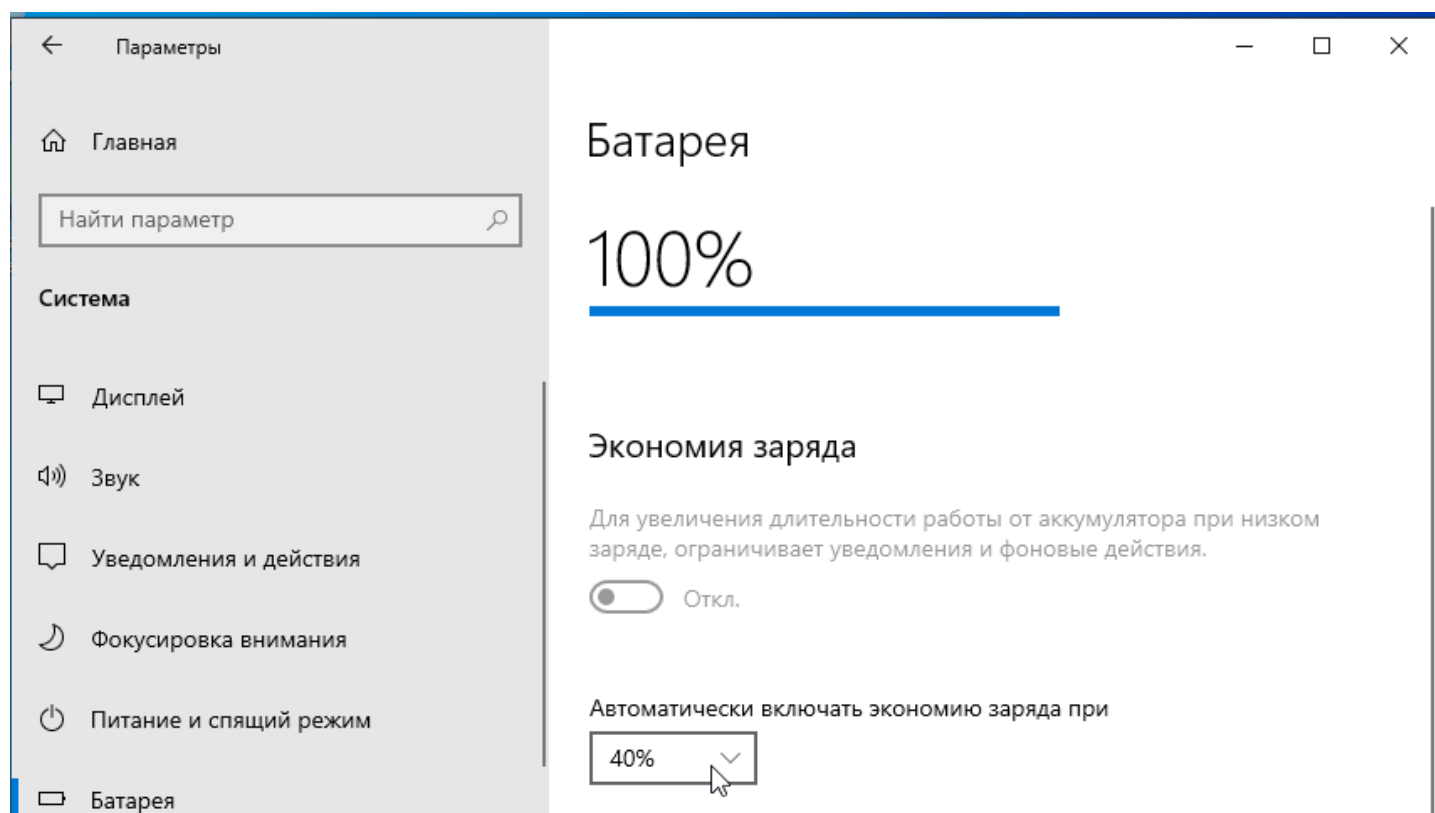
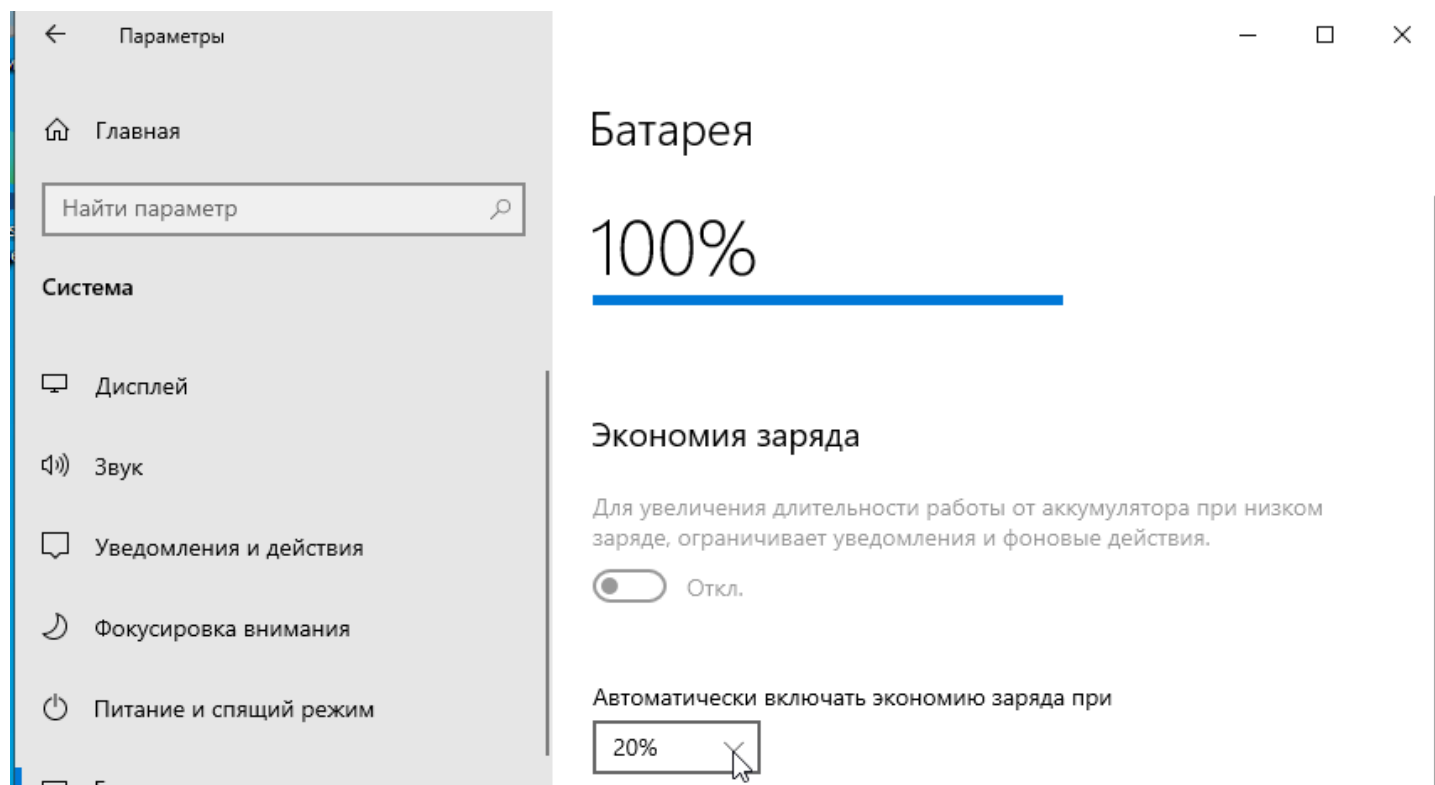
Также пользователь может изменить параметры дисплея.
Например, ориентация дисплея(перевернутая):



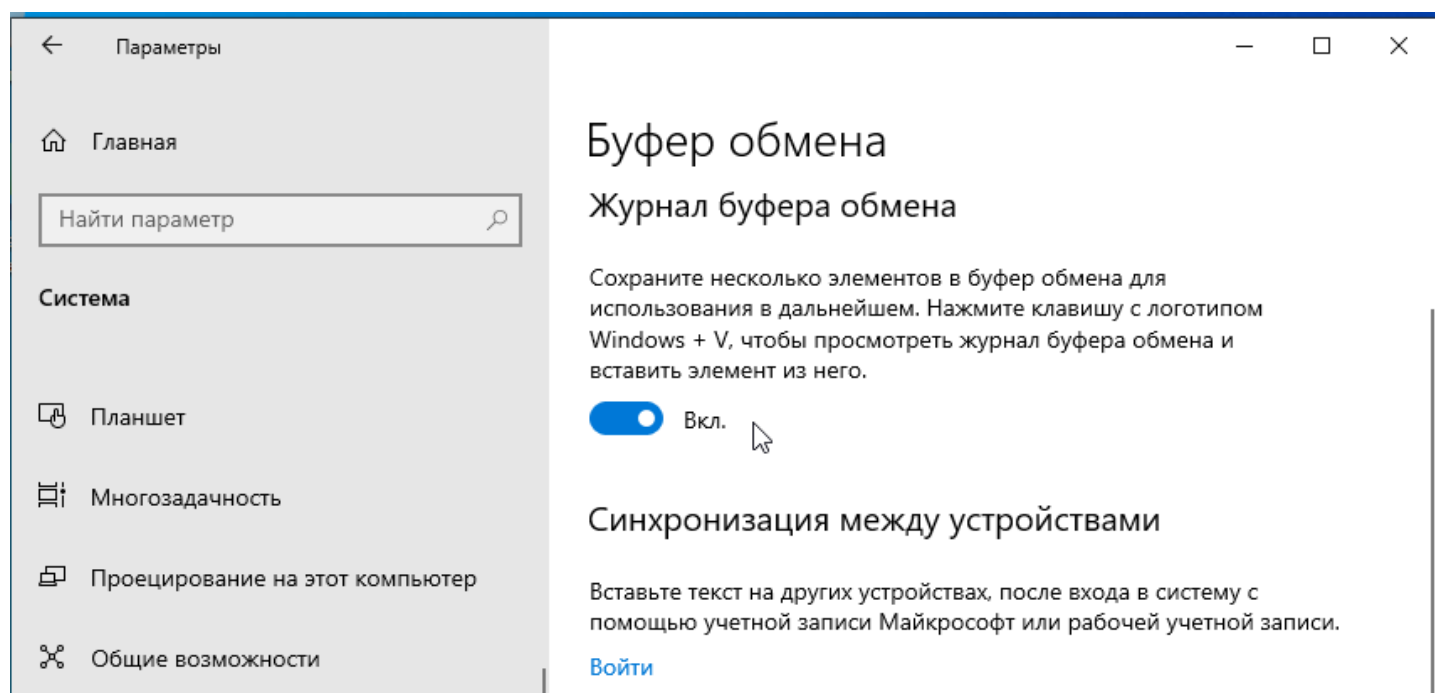
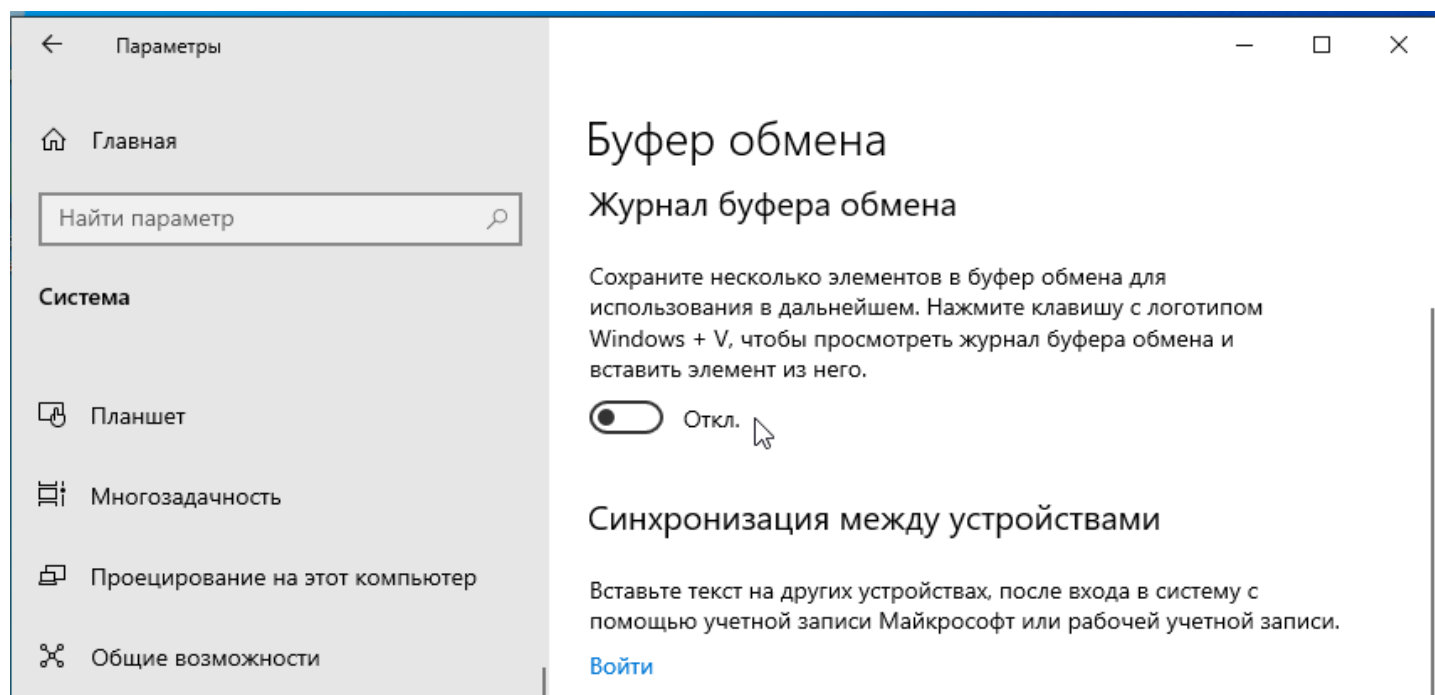
Пользователь может задать время отключения экрана



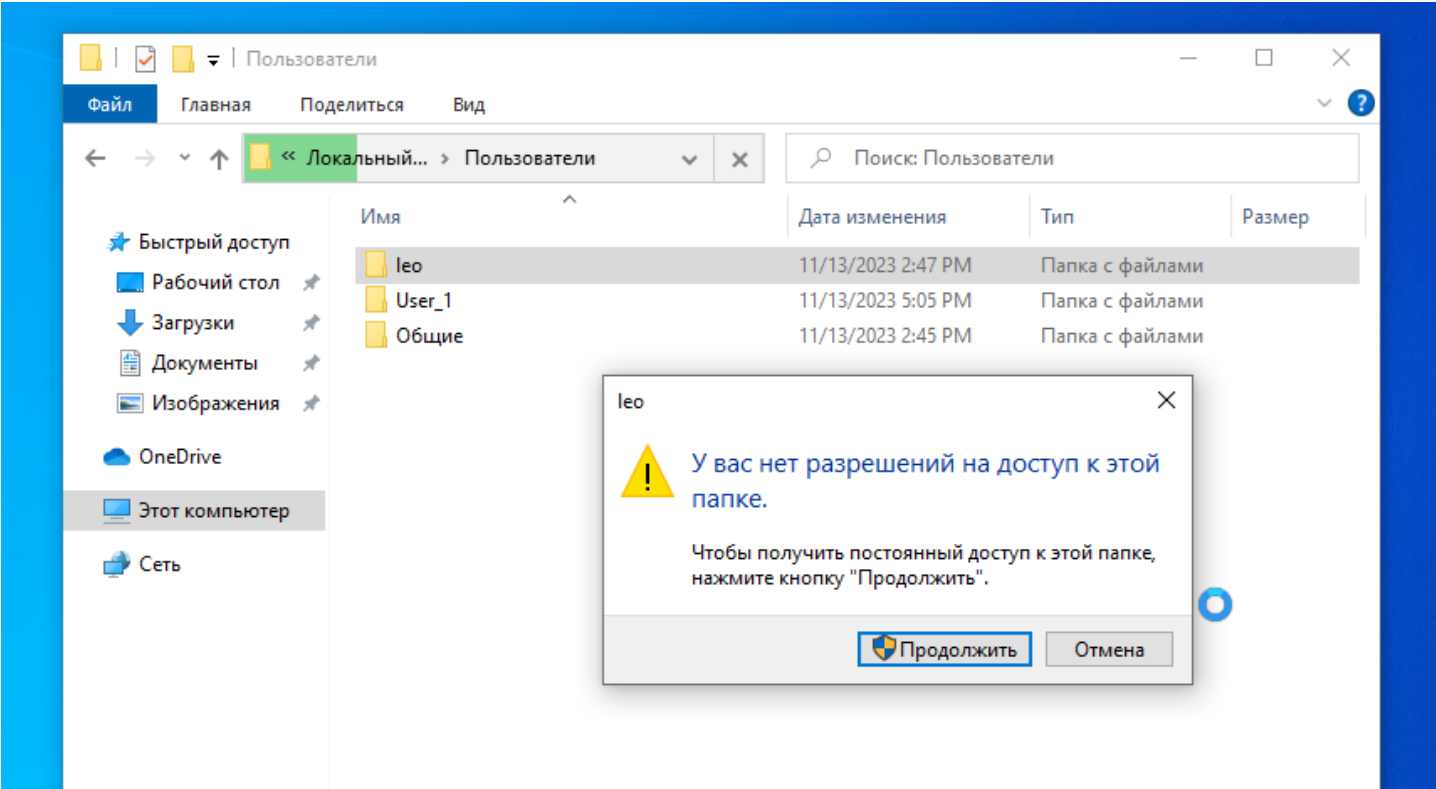
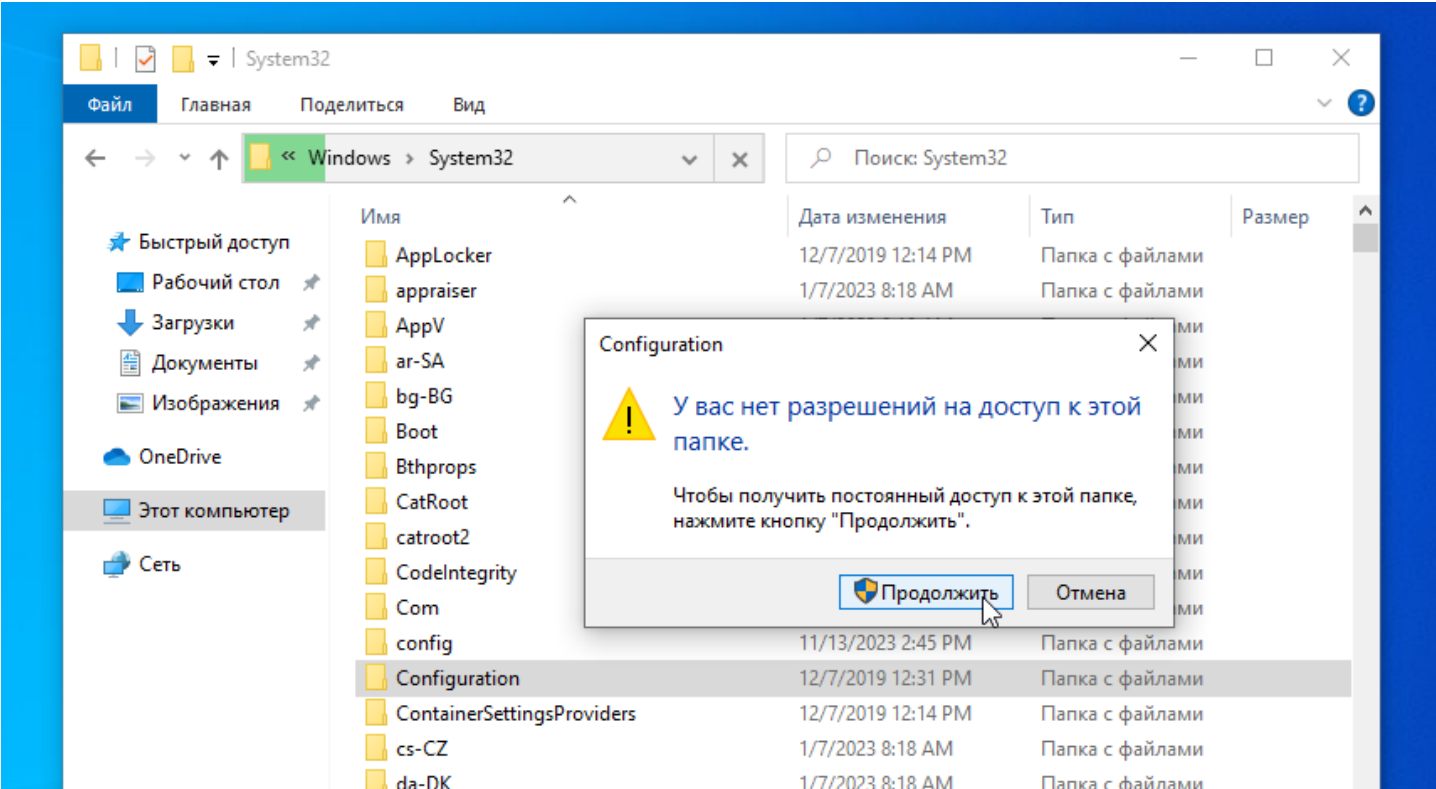
Пользователь может выбрать момент начала экономии заряда



Пользователь может включать / выключать буфер обмена



Однако обычный пользователь не может получить доступ к системной папке и папкам других пользователей

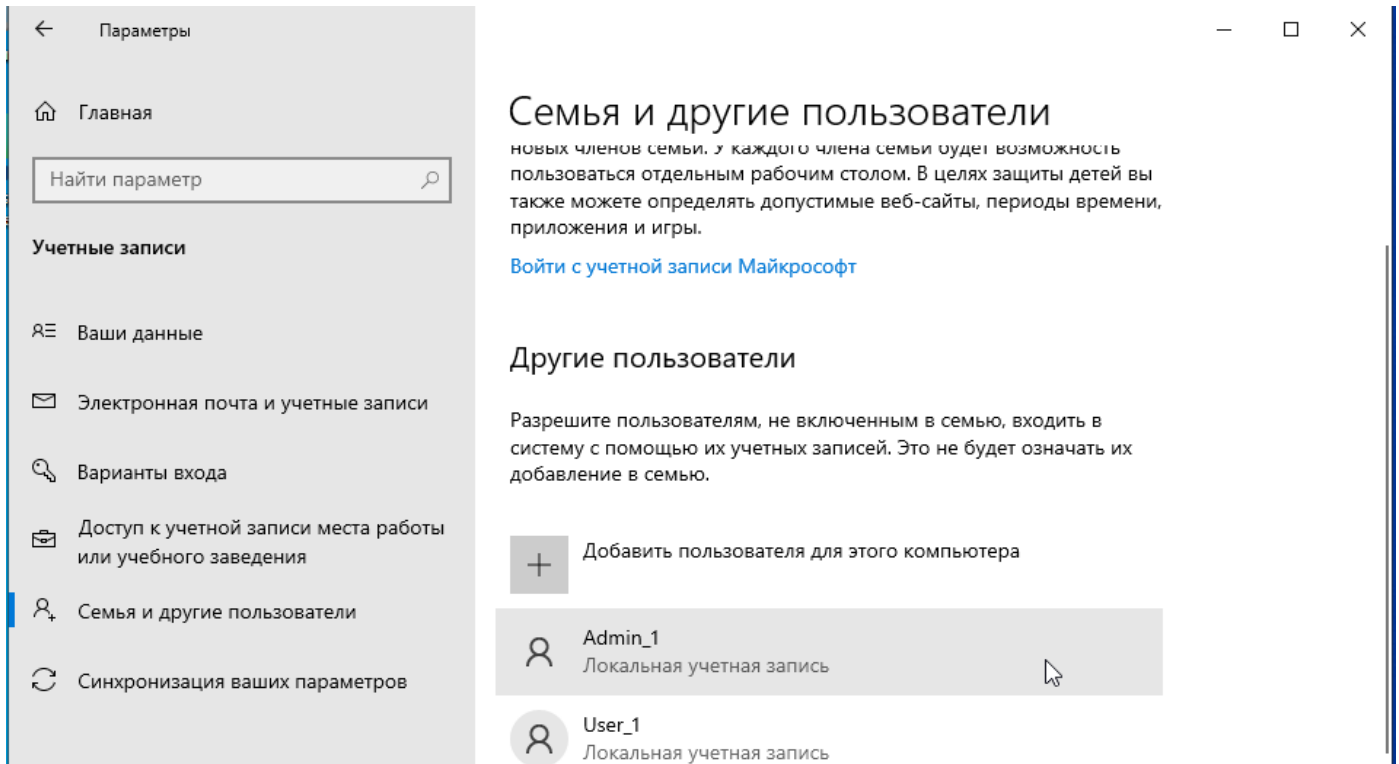


3 Создание администратора

В Windows 10 нельзя сразу создать администратора, для этого необходимо сначала создать обычного пользователя, и потом добавить его в группу администраторов.

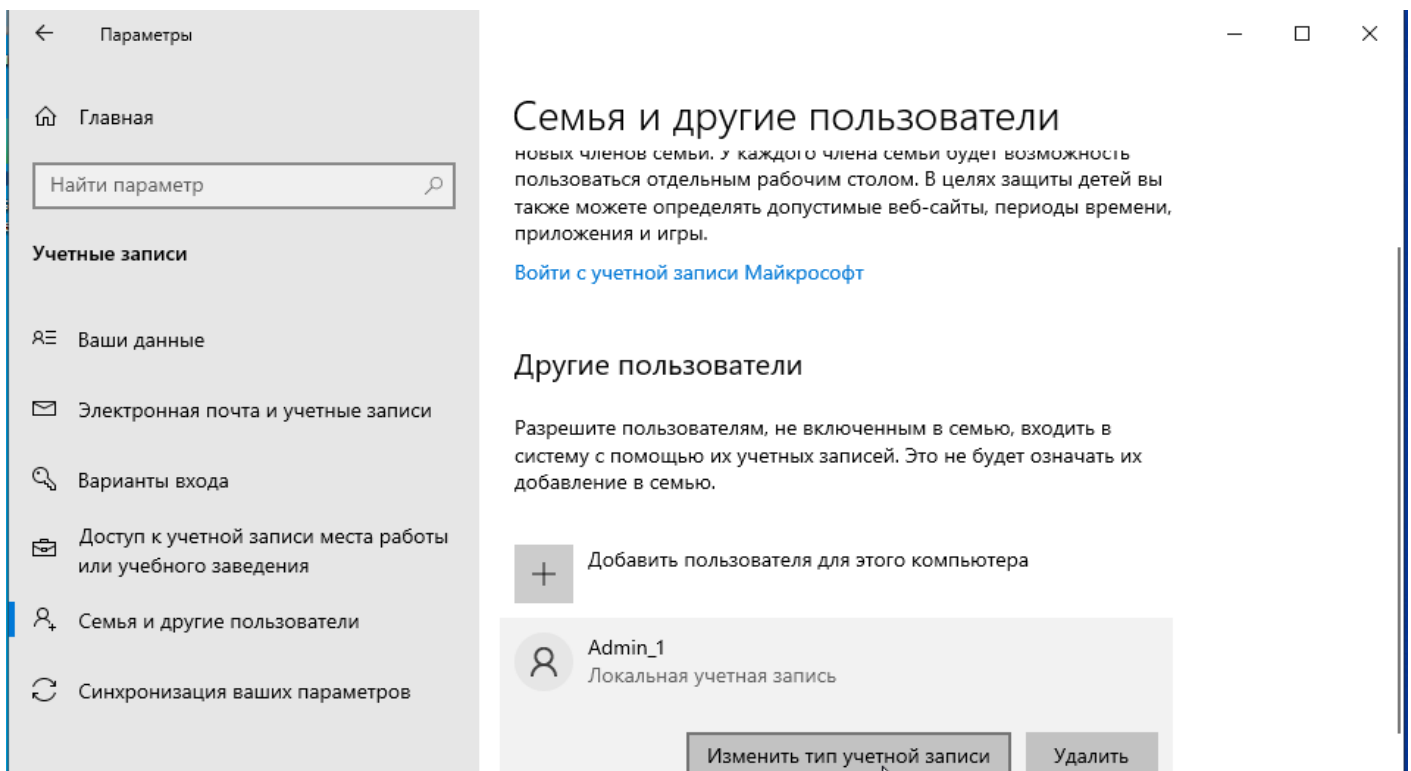
Вариант 3.1

Повторим действия из пункта Вариант 2.1 и создадим пользователя Admin_1

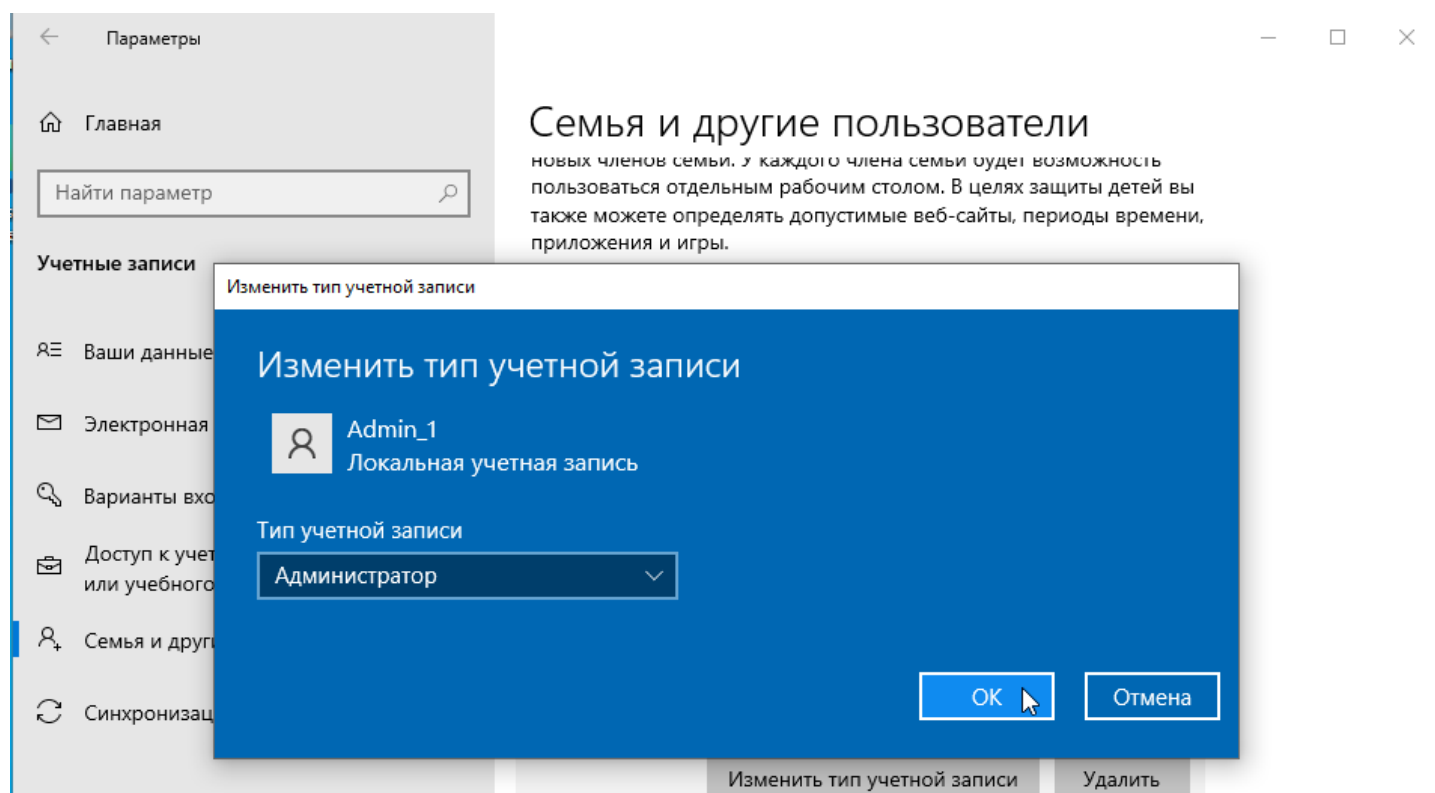


Затем нажмем на нашего пользователя Admin_2 и нажмем на появившуюся кнопку:

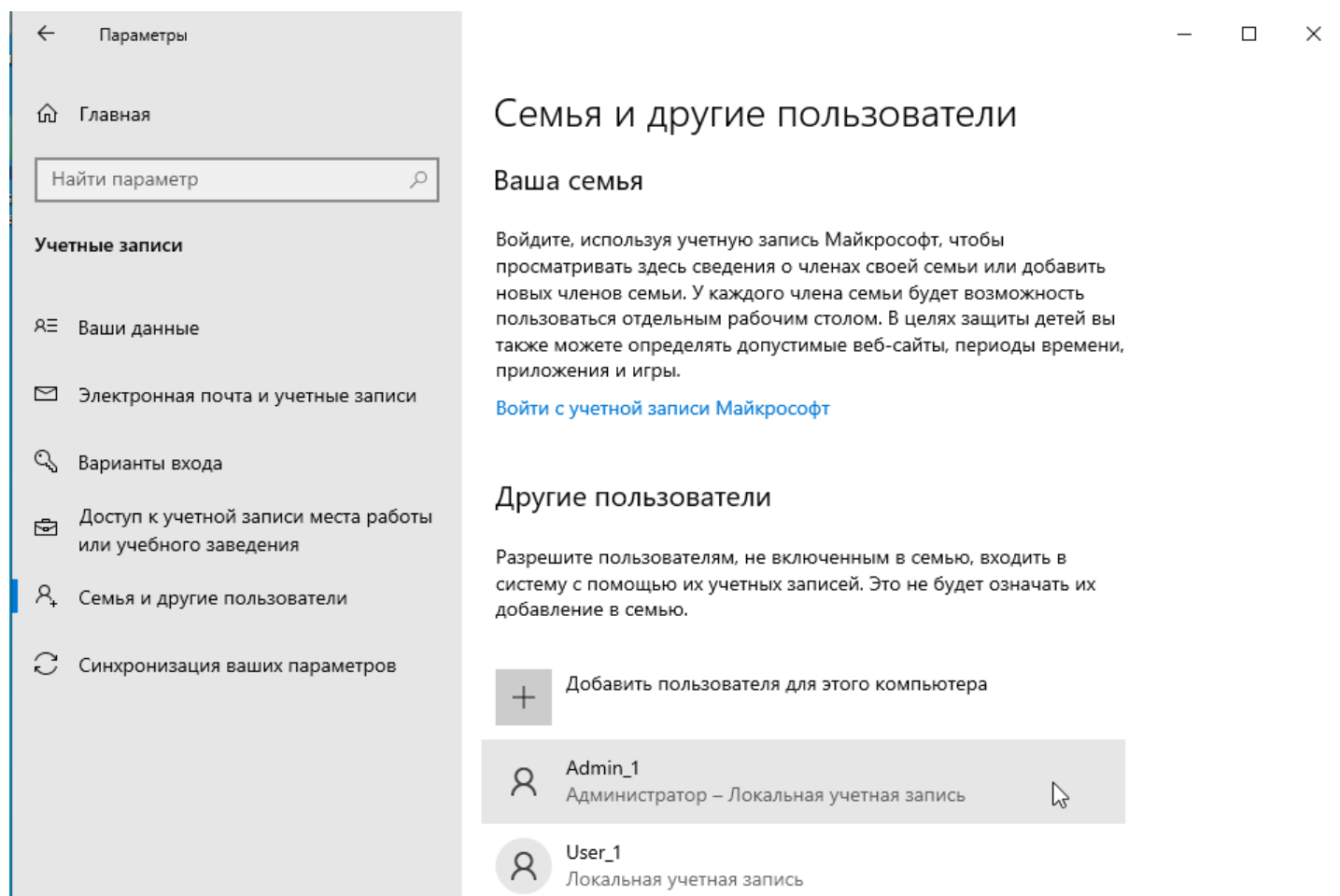
Изменить тип учетной записи



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_1

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

```
Administrator: Командная строка
Microsoft Windows [Version 10.0.19045.2486]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Windows\system32>net user Admin_1 /add
The command completed successfully.

C:\Windows\system32>net localgroup "Администраторы" Admin_1 /add
The command completed successfully.

C:\Windows\system32>_
```

```
Administrator: Командная строка
C:\Windows\system32>net localgroup

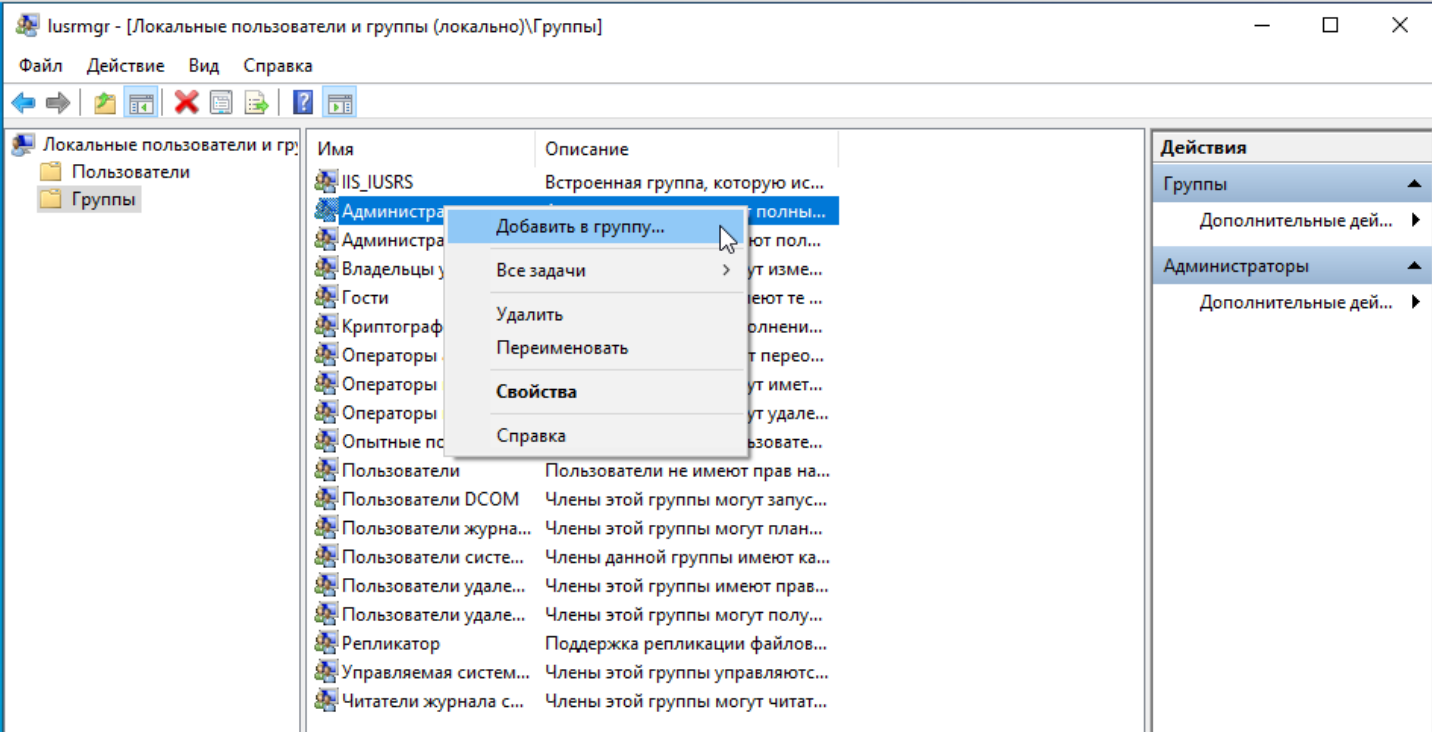
Aliases for \\WIN10PRO
-----
*IIS_IUSRS
*Администраторы
*Администраторы Нурег-V
*Владельцы устройства
*Гости
*Криптографические операторы
*Операторы архива
*Операторы настройки сети
*Операторы помощи по контролю учетных записей
*Опытные пользователи
*Пользователи
*Пользователи DCOM
*Пользователи журналов производительности
*Пользователи системного монитора
*Пользователи удаленного рабочего стола
*Пользователи удаленного управления
*Репликатор
*Управляемая системой группа учетных записей
*Читатели журнала событий
The command completed successfully.

C:\Windows\system32>_
```

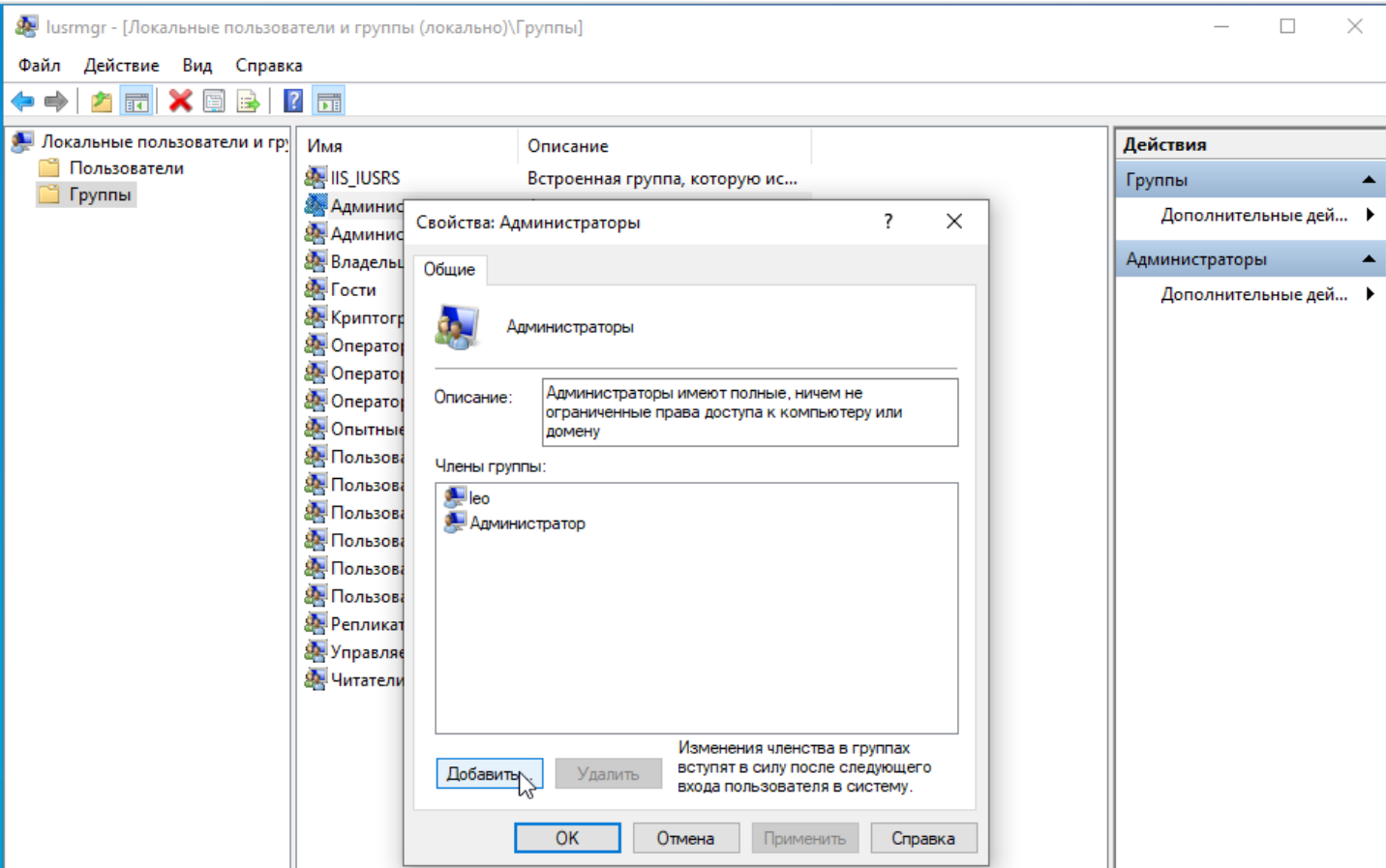
Вариант 3.3

Повторим действия из пункта Вариант 2.4: и создадим пользователя Admin_1. Затем переходим в раздел “Группы” и нажимаем правой кнопкой мыши по “Администраторы”.

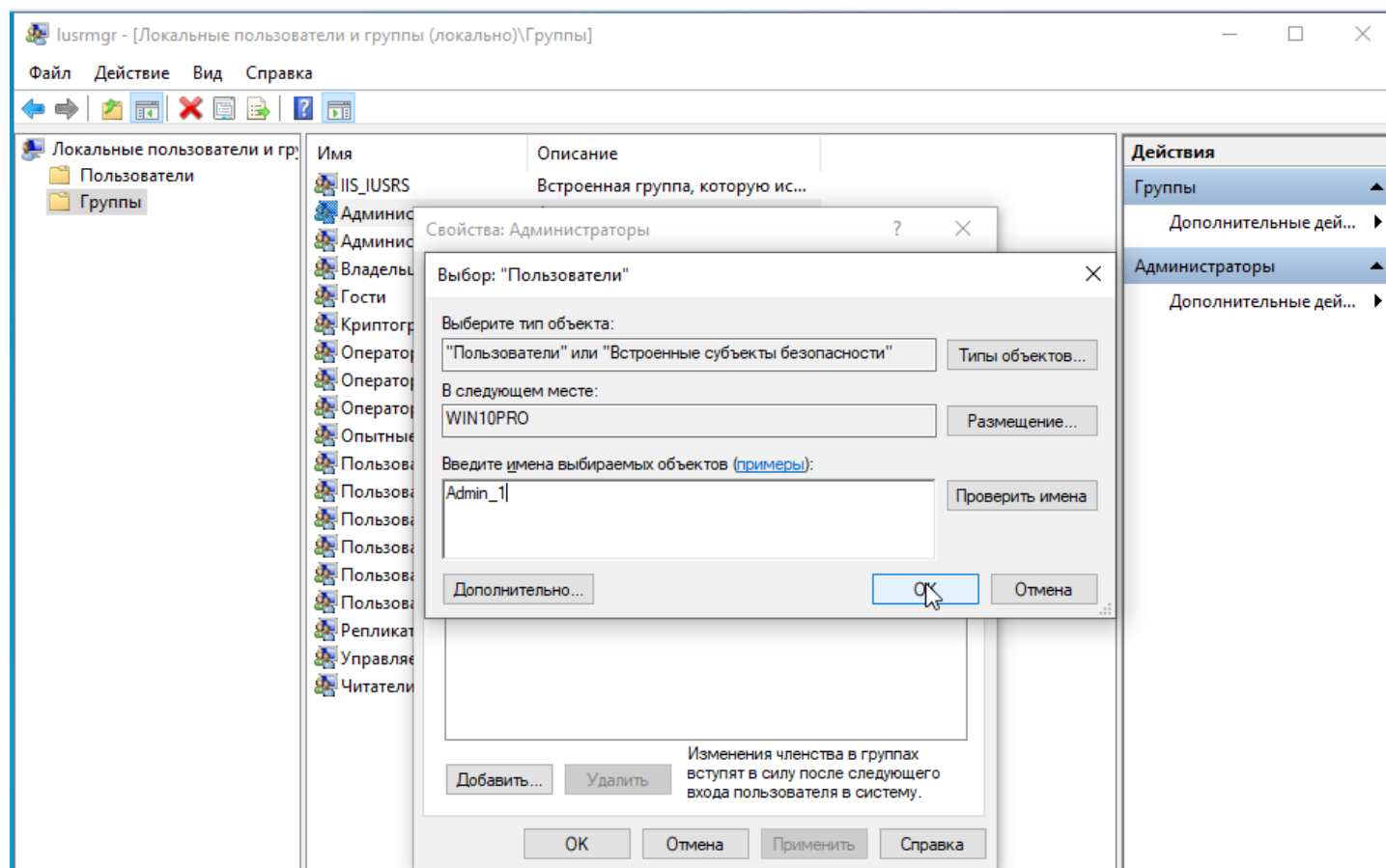
В появившемся выпадающем списке выбираем “Добавить в группу...”



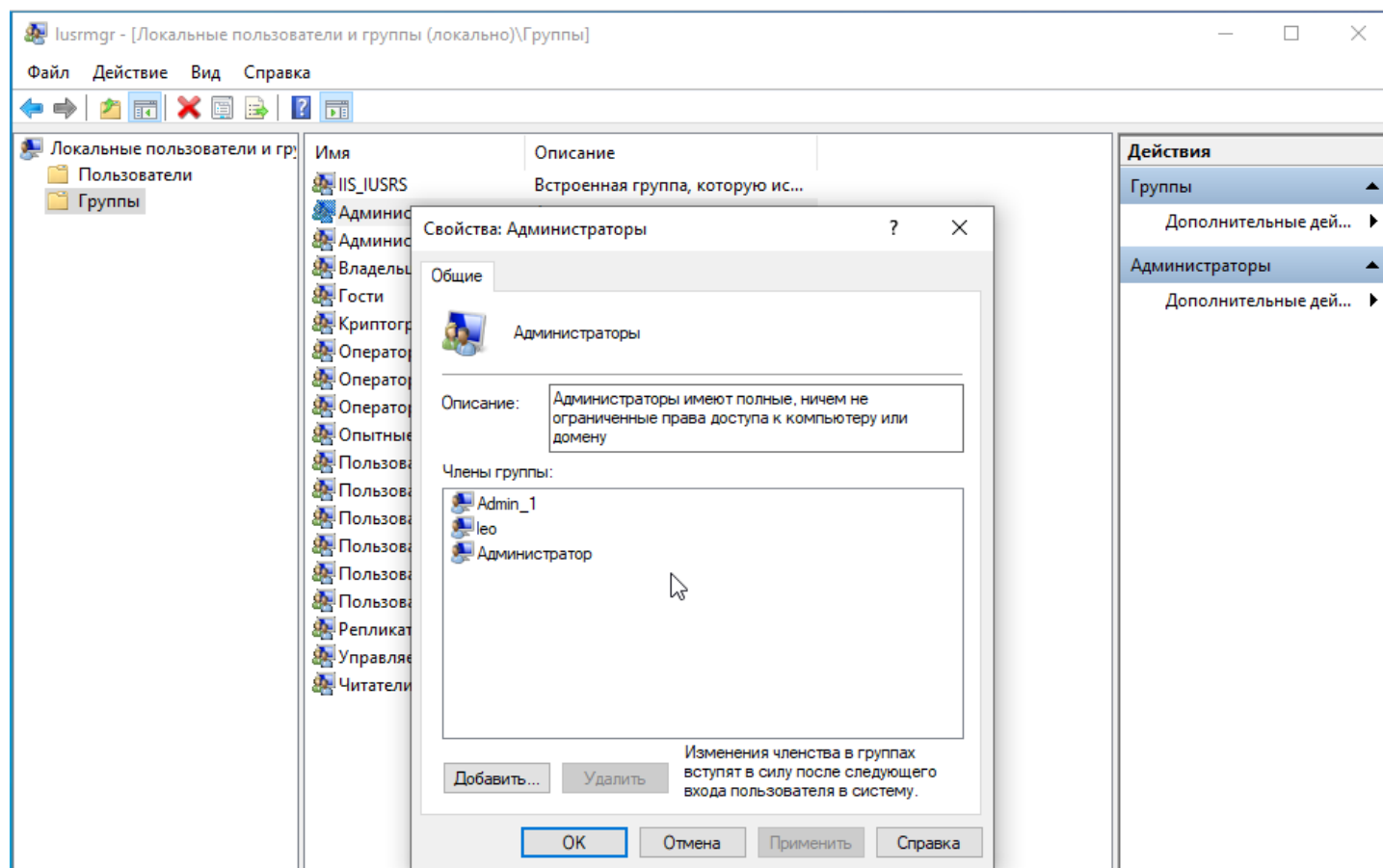
Нажимаем кнопку “Добавить...”



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

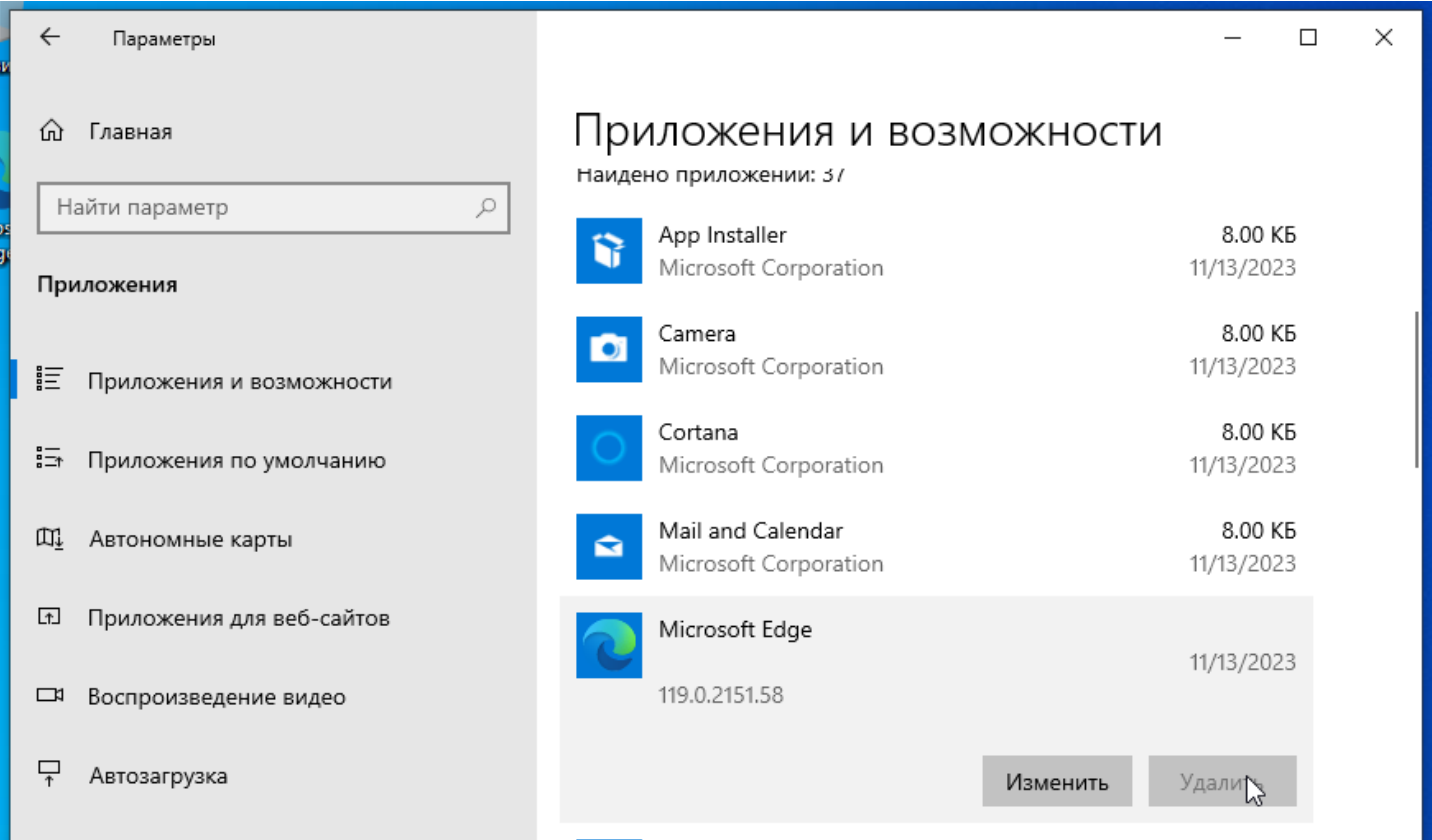


Затем нажимаем кнопки "ОК", “Применить”, “ОК”. И проверяем:

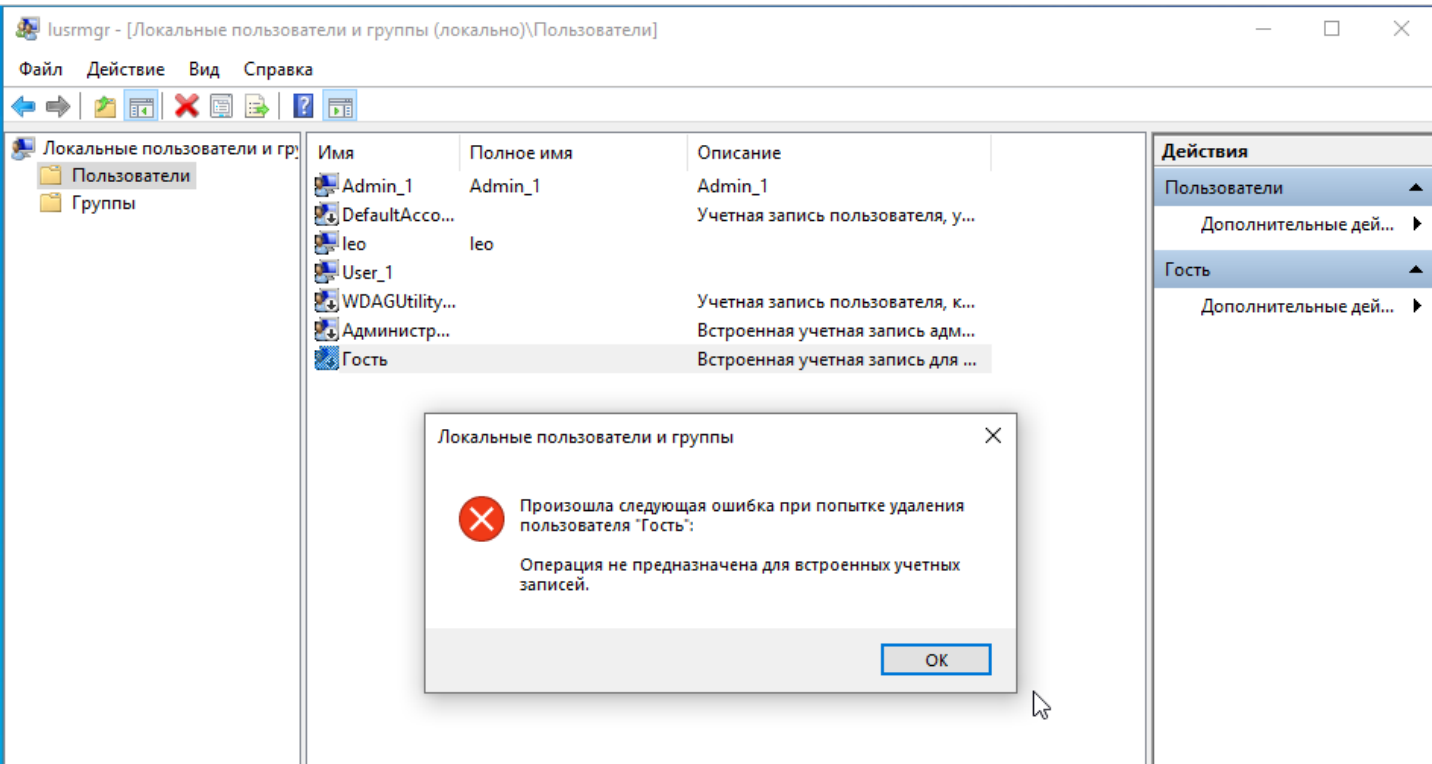


Ограничения

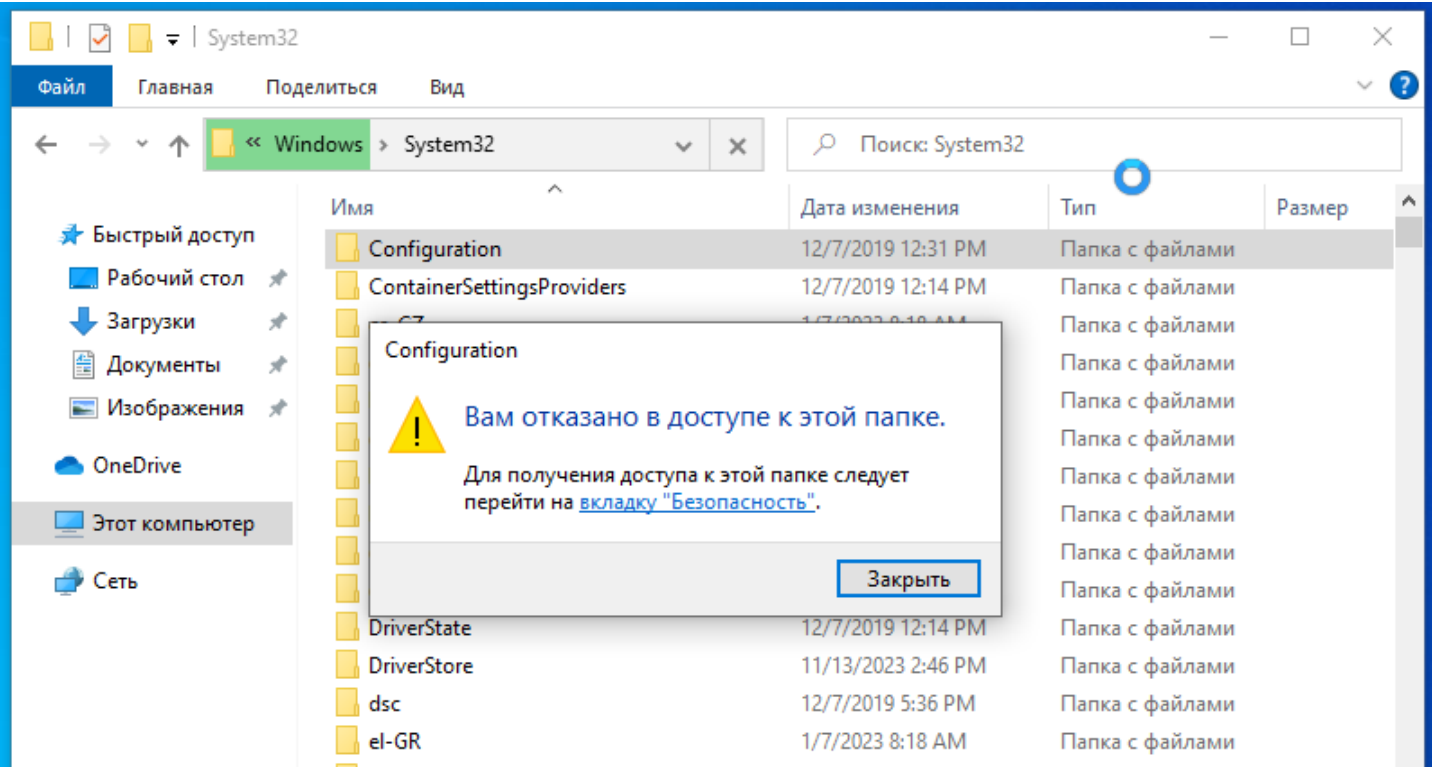
Нельзя удалить встроенные приложения (например, Microsoft Edge):



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

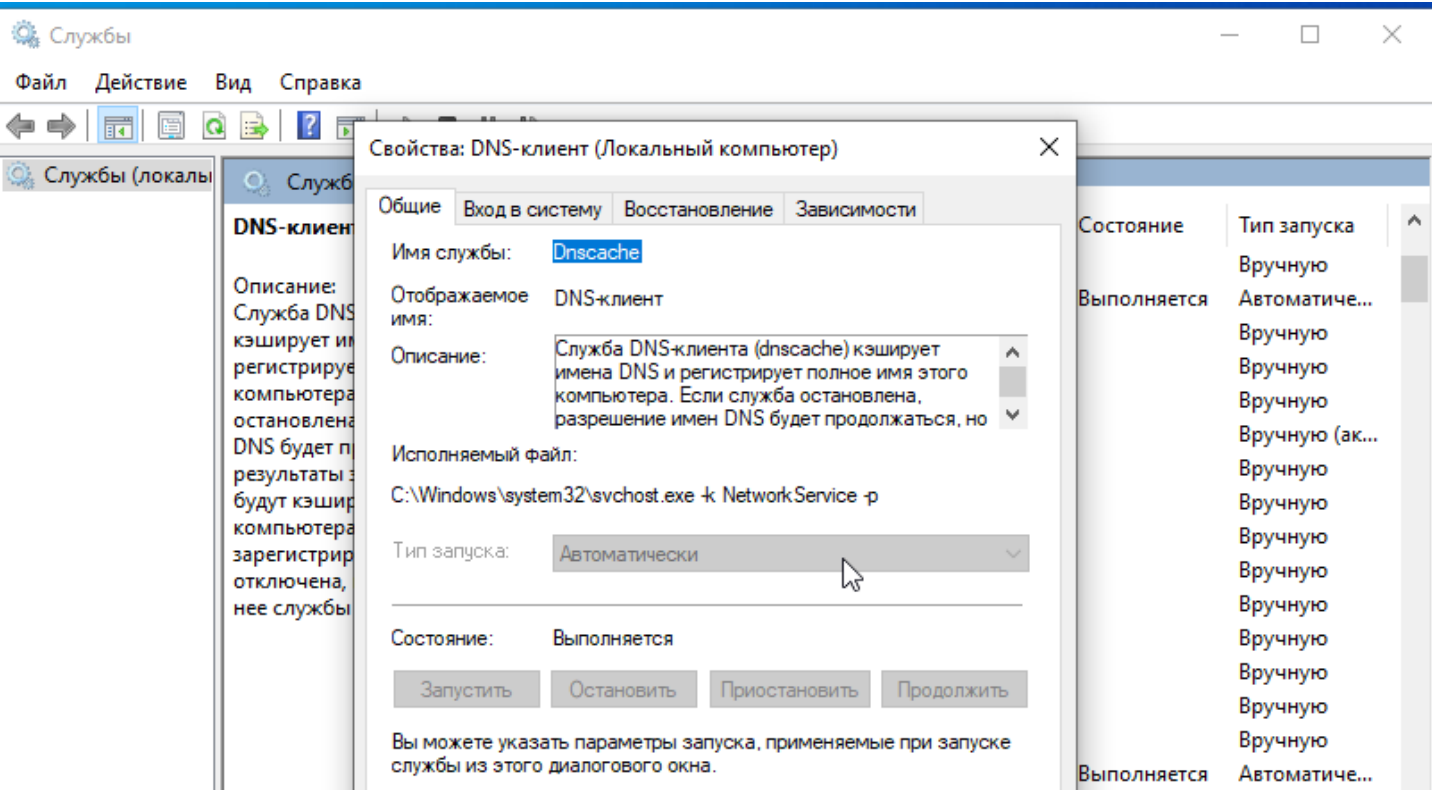


Блокировка доступа к важным системным файлам:



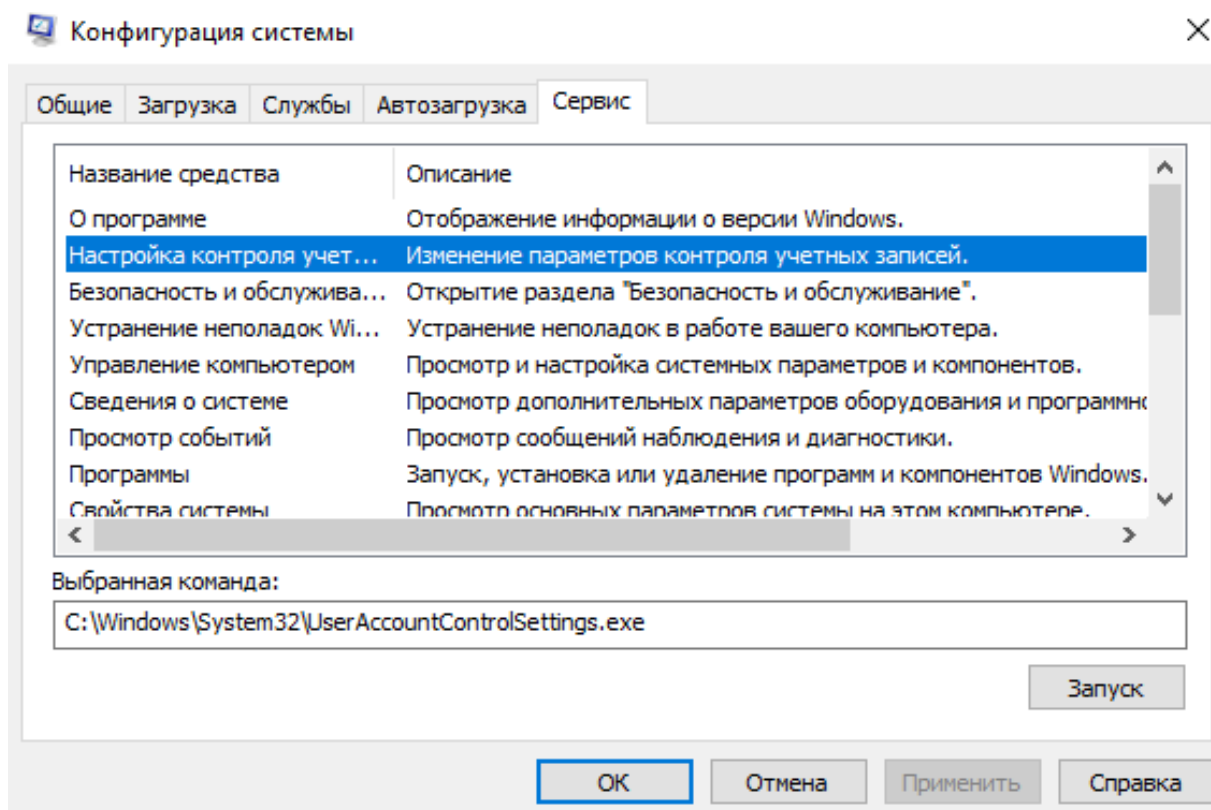
Нельзя отключить автозапуск службы например: Dnscache

Кнопку “Тип запуска” неактивна.



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.



Параметры управления учетными записями пользователей

Настройка уведомления об изменении параметров компьютера

Контроль учетных записей помогает предотвратить изменения, вносимые в компьютер потенциально опасными программами.

[Подробнее о параметрах контроля учетных записей](#)

Всегда уведомлять



Уведомлять только при попытках приложений внести изменения в компьютер (по умолчанию)

- Не уведомлять при изменении параметров Windows пользователем

i Рекомендуется при использовании знакомых приложений и посещении знакомых веб-сайтов.

Никогда не уведомлять

OK Отмена

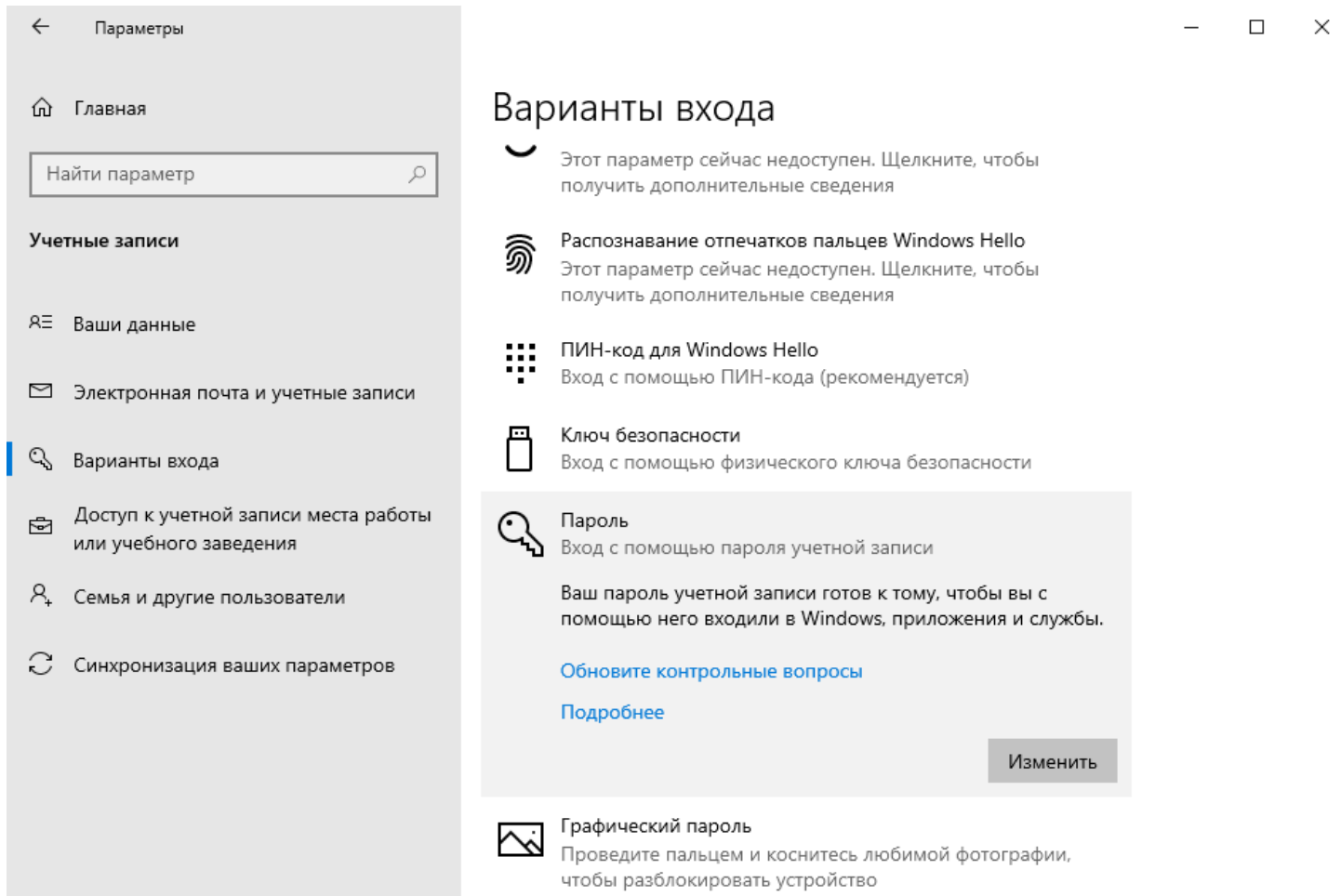
Существует 4 уровня:

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 по паролю. Рассмотреть и реализовать возможные способы усиления парольной защиты.

По умолчанию наш пароль усилен контрольными вопросами в количестве трех штук, на сам пароль нет ограничений по сложности или количеству символов.



Меры повышения надежности парольной защиты

Это можно исправить включением политики пароля, которые могут быть настроены с помощью локальной групповой политики или политикой домена.

- наложение технических ограничений (длина, увеличение алфавита (символы разных языков, спецсимволы))
- управление сроком действия паролей, их периодическая смена;
- ограничение доступа к файлу паролей
- ограничение числа неудачных попыток входа в систему
- обучение и воспитание пользователей (запрет разглашения)
- использование программных и аппаратных генераторов паролей
- ограничение повторяемости паролей (история паролей)

Часть из данных мер можно установить в политике безопасности системы

Выполнить

Введите имя программы, папки, документа или ресурса Интернета, которые требуется открыть.

Открыть:

gpedit.msc

OK

Отмена

Обзор...

Локальная политика безопасности

Файл Действие Вид Справка

Параметры безопасности

Политики учетных записей

Политика паролей

Политика блокировки учетной записи

Локальные политики

Монитор брандмауэра Защитника

Политики диспетчера списка сетей

Политики открытого ключа

Политики ограниченного использования

Политики управления приложениями

Политики IP-безопасности на "Локальной"

Конфигурация расширенной политики

Политика	Параметр безопасности
Аудит минимальной длины пароля	Не определено
Вести журнал паролей	0 сохраненных паролей
Максимальный срок действия пароля	42 дн.
Минимальная длина пароля	0 зн.
Минимальный срок действия пароля	0 дн.
Ослабить ограничение минимальной длины пароля	Не определено
Пароль должен отвечать требованиям сложности	Отключен
Хранить пароли, используя обратимое шифрование	Отключен

Локальная политика безопасности

Файл Действие Вид Справка

Параметры безопасности

Политики учетных записей

Политика паролей

Политика блокировки учетной записи

Локальные политики

Монитор брандмауэра Защитника

Политики диспетчера списка сетей

Политики открытого ключа

Политики ограниченного использо

Политики управления приложения

Политики IP-безопасности на "Лока

Конфигурация расширенной полит

Политика

Время до сброса счетчика блокировки

Пороговое значение блокировки

Продолжительность блокировки учетной записи

Разрешить блокировку учетной записи администратора

Параметр безопасности

10 мин.

10 ошибок входа в сис...

10 мин.

Включен

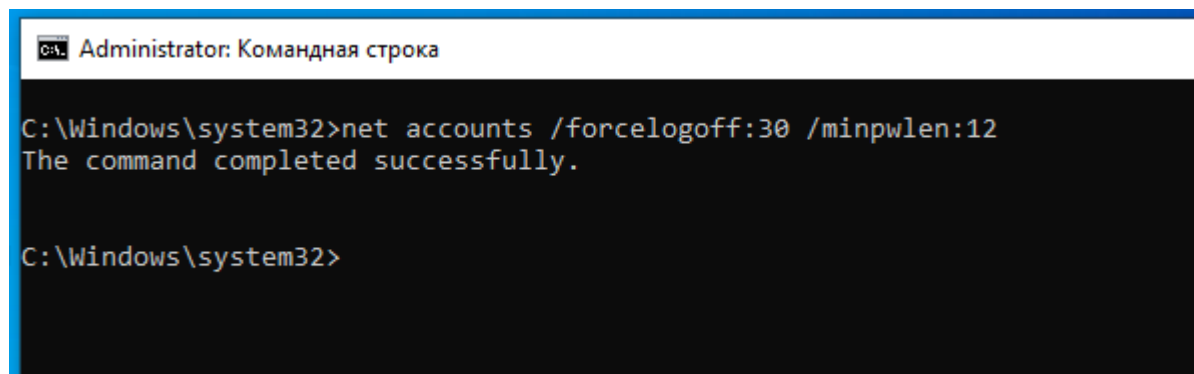
- Аудит минимальной длины пароля
 - Зачем нужно: Устанавливает минимальную длину пароля.
 - Цель: Увеличение сложности пароля и повышение уровня безопасности.
- Вести журнал паролей
 - Зачем нужно: Запоминает предыдущие пароли пользователя.
 - Цель: Предотвращение повторного использования старых паролей.
- Максимальный срок действия пароля
 - Зачем нужно: Ограничивает период действия пароля.
 - Цель: Принудительное изменение пароля через определенный период для предотвращения его долговременного использования.
- Минимальный срок действия пароля
 - Зачем нужно: Устанавливает минимальный период времени перед тем, как пользователь может изменить свой пароль.
 - Цель: Предотвращение слишком частой смены паролей и повышение безопасности.
- Пароль должен отвечать требованиям сложности
- Хранить пароли используя обратимое шифрование
 - Хранение паролей с использованием обратимого шифрования считается плохой практикой в области безопасности данных, и обычно не рекомендуется.

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

- /forceloggoff - 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:12
```



```
Administrator: Командная строка

C:\Windows\system32>net accounts /forceloff:30 /minpwlen:12
The command completed successfully.

C:\Windows\system32>
```

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 No4369, 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:

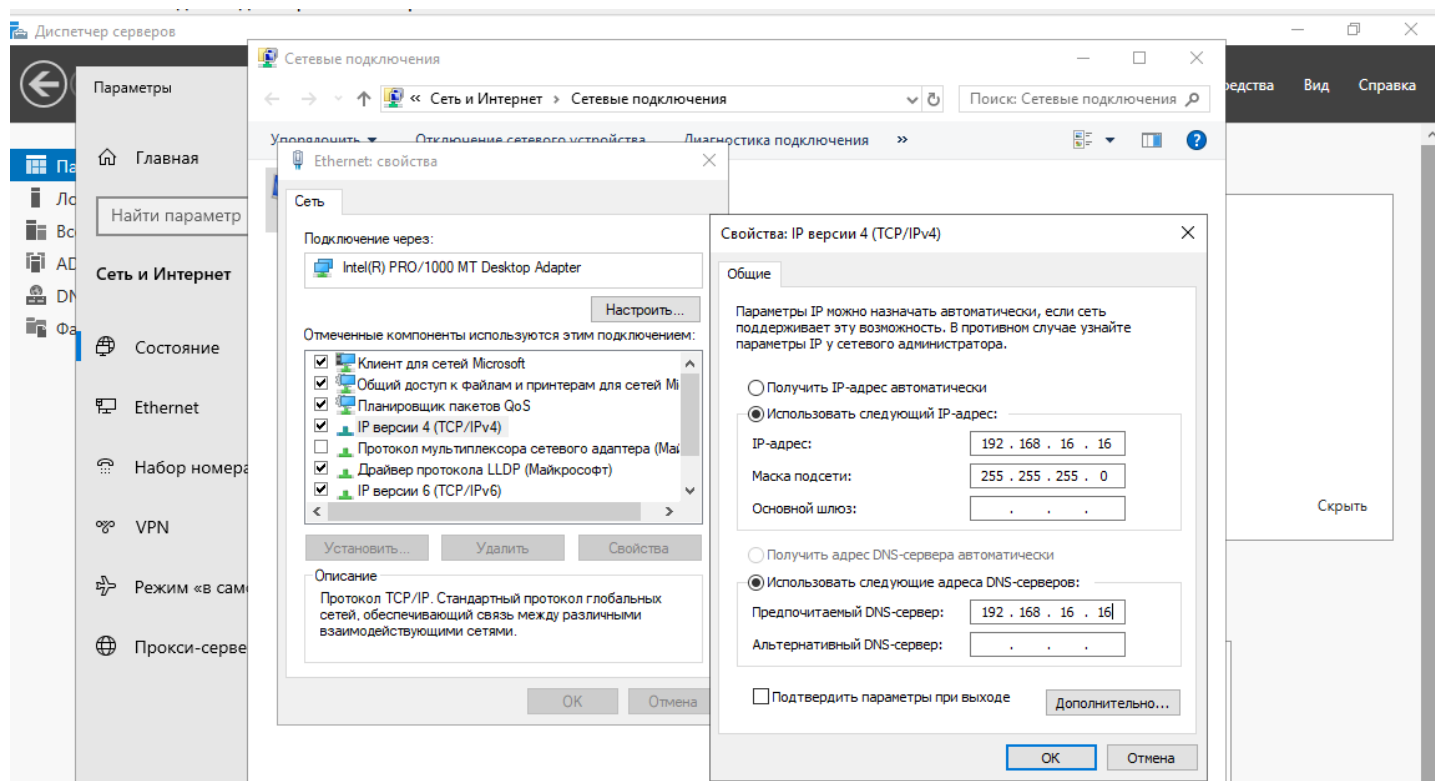
- Дискреционный принцип контроля доступ В рамках данного требования необходимо контролировать доступ наименованных субъектов (пользователей) к наименованным объектам, а это реализовано с помощью ассоциирования пользователя с группой.
- Идентификация и аутентификация В рамках данного требования пользователь 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

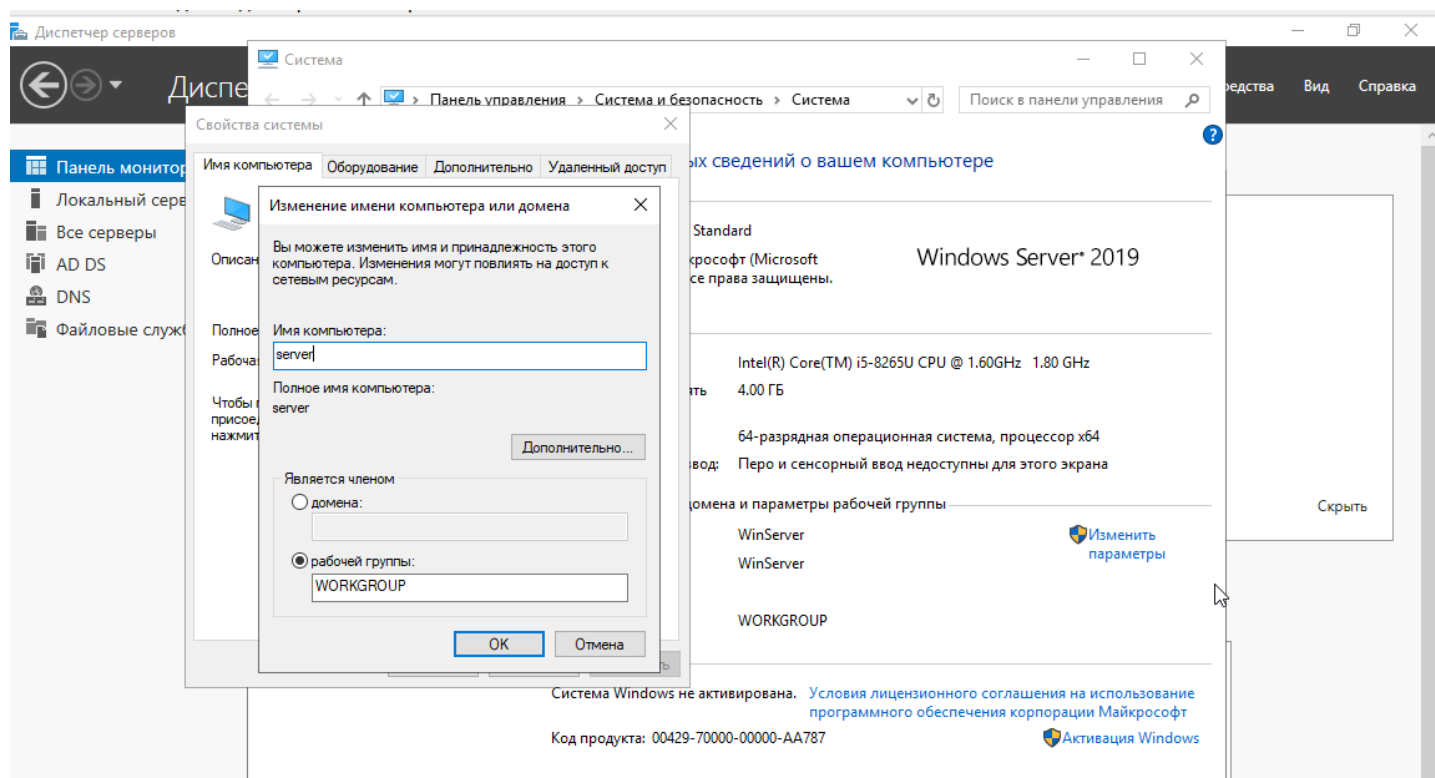
1 Опишите создание профиля пользователя и его копирование (на основе Windows Server)

Так как механизм Active Directory подразумевает не одноранговую, а централизованную систему, то для его реализации нам понадобится Windows Server, запущенный, в моем случае, на VirtualBox.

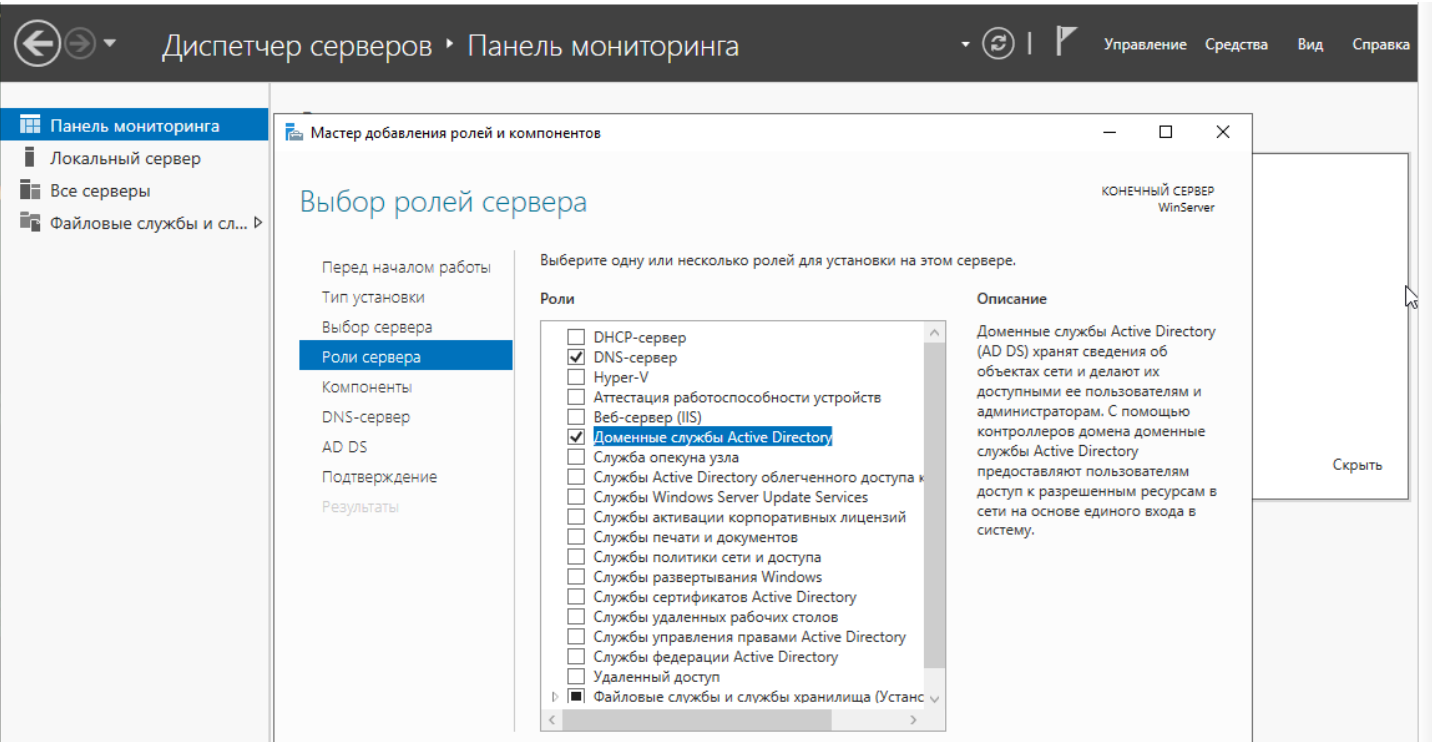
Прежде всего создадим статичный ip адрес для нашей виртуальной машины



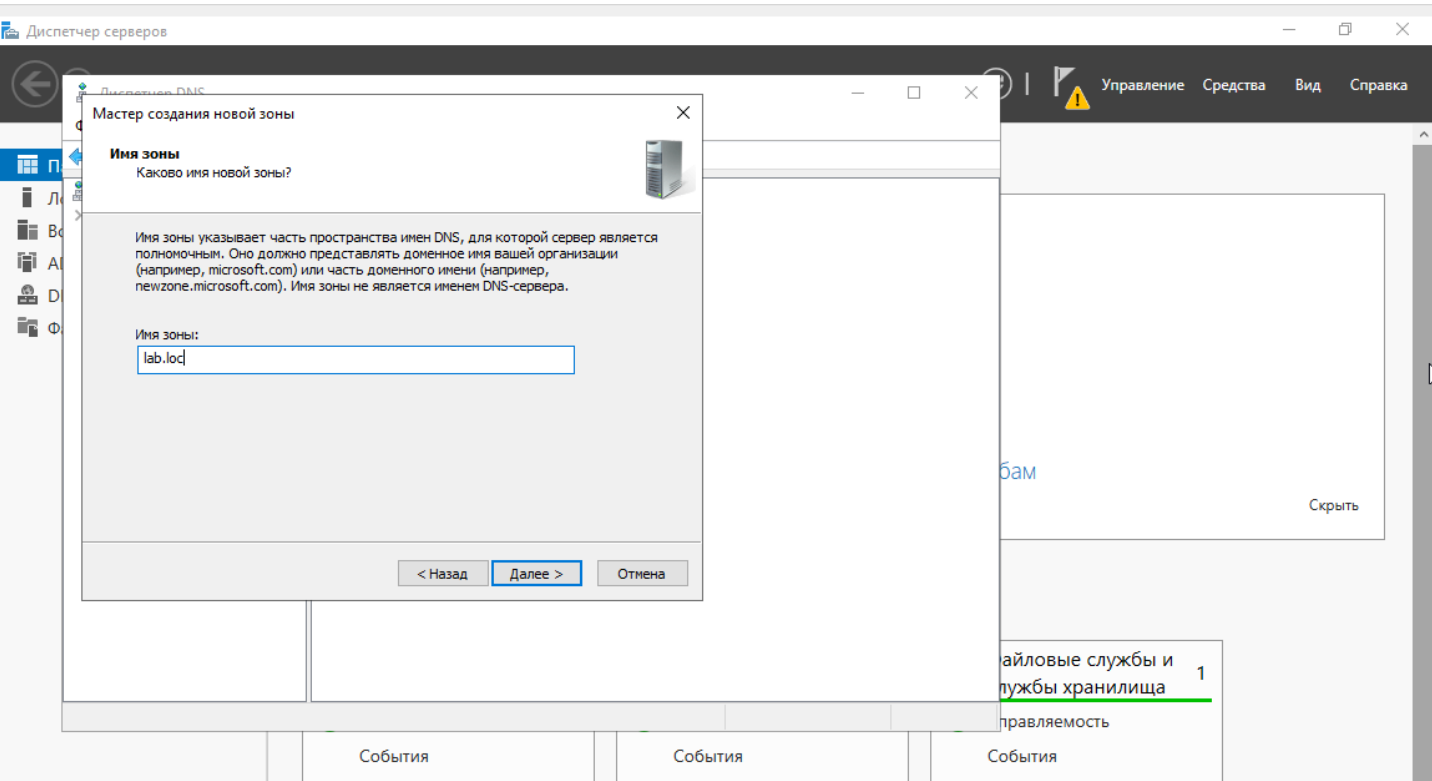
Далее изменим имя нашего сервера



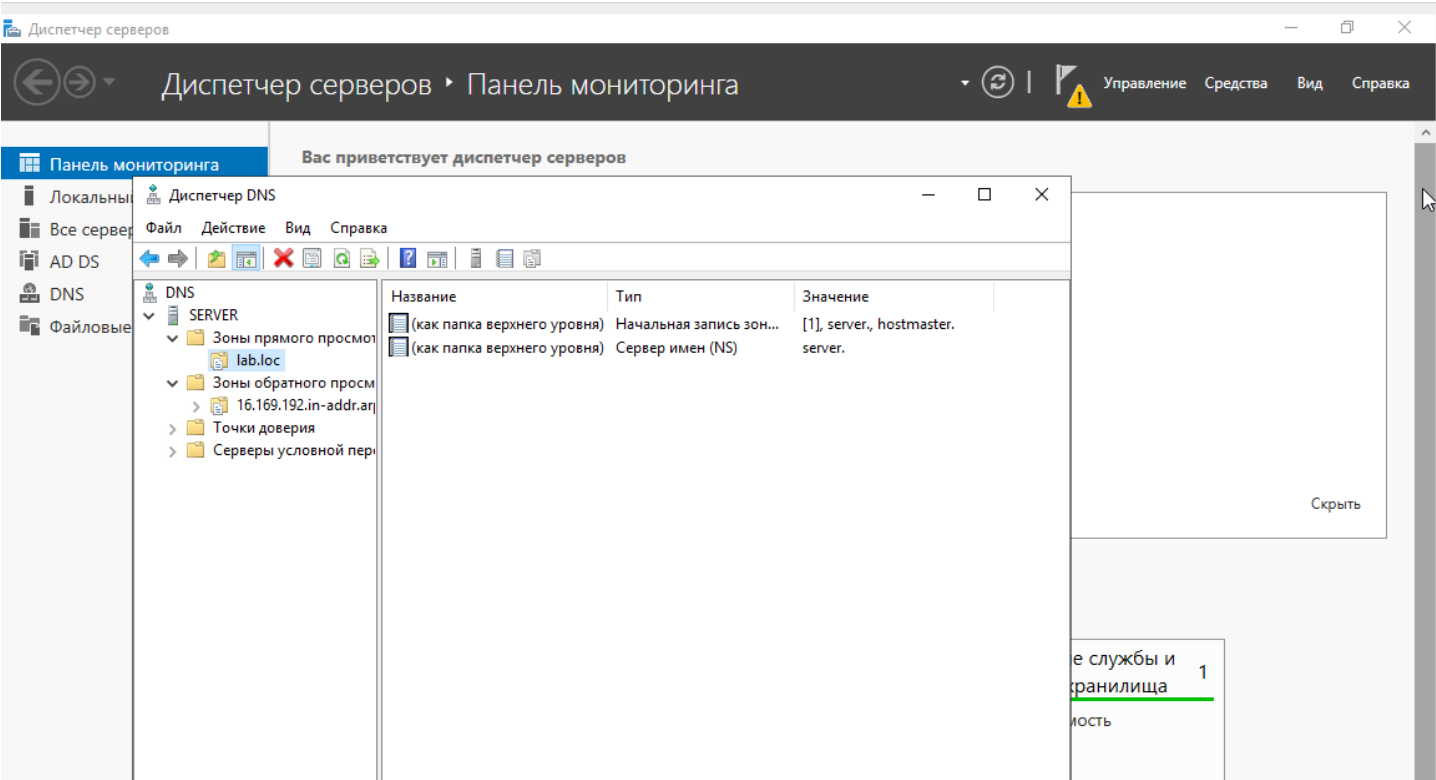
Далее поднимаем службу ДНС на сервере:



Создаем новую зону в службе ДНС

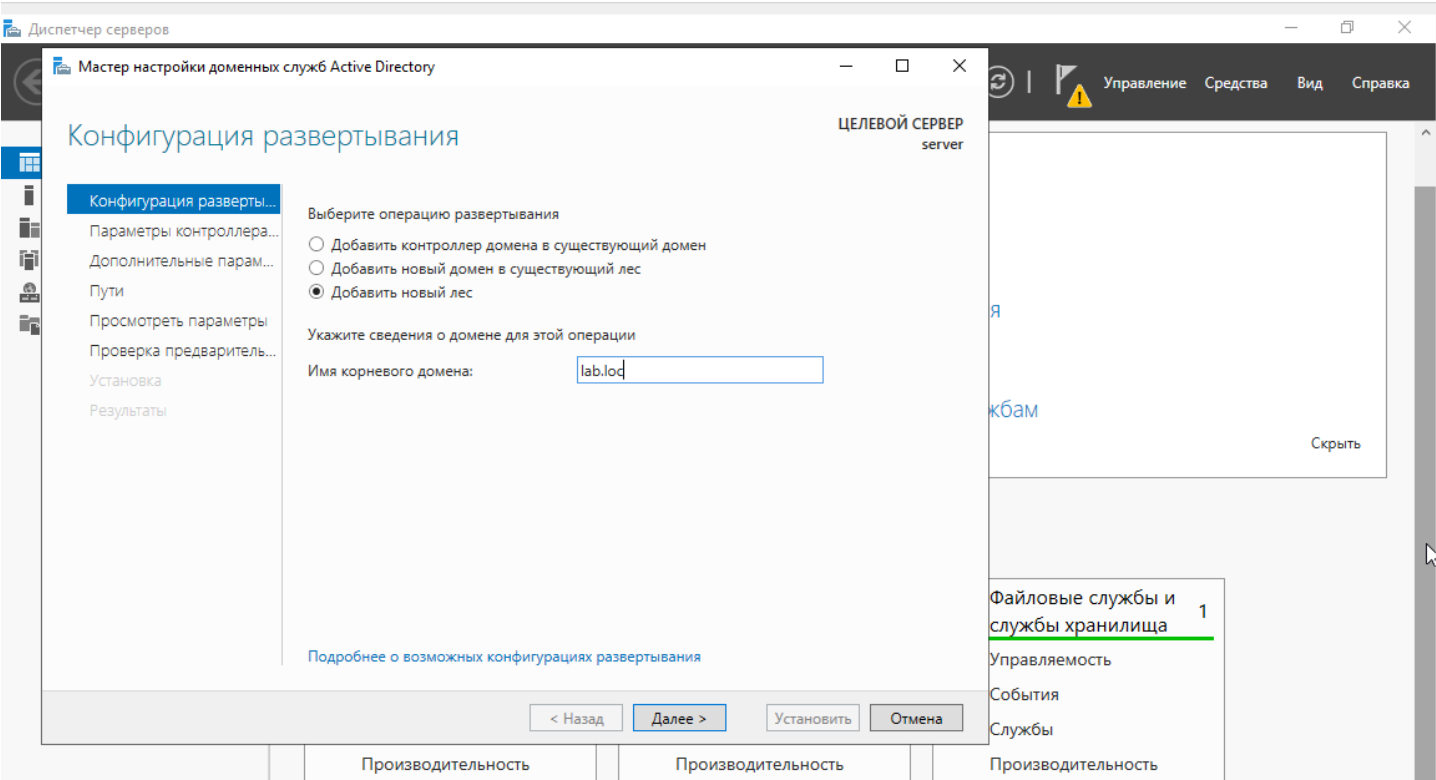


Проверяем

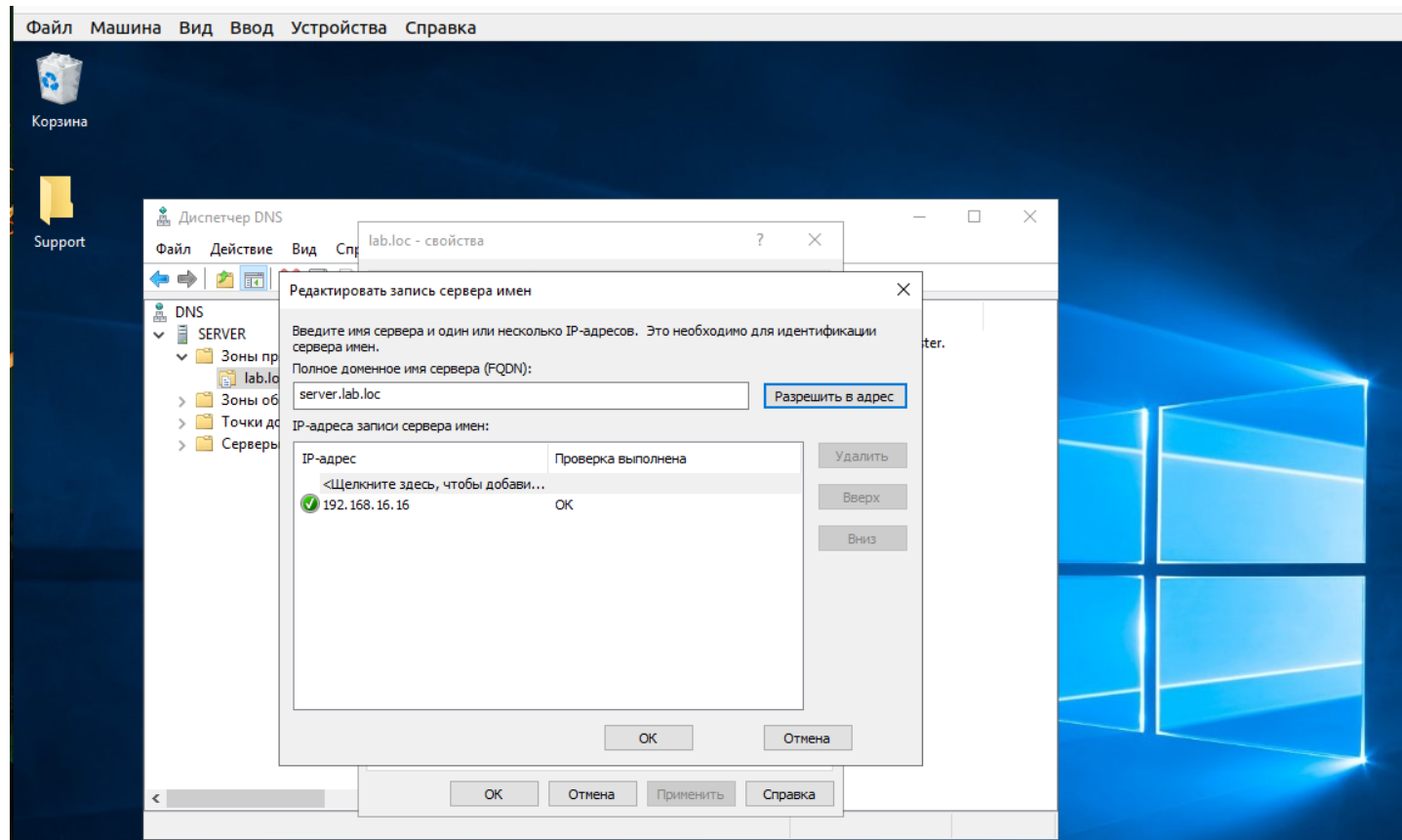


Далее произведем настройку контроллера Active Directory

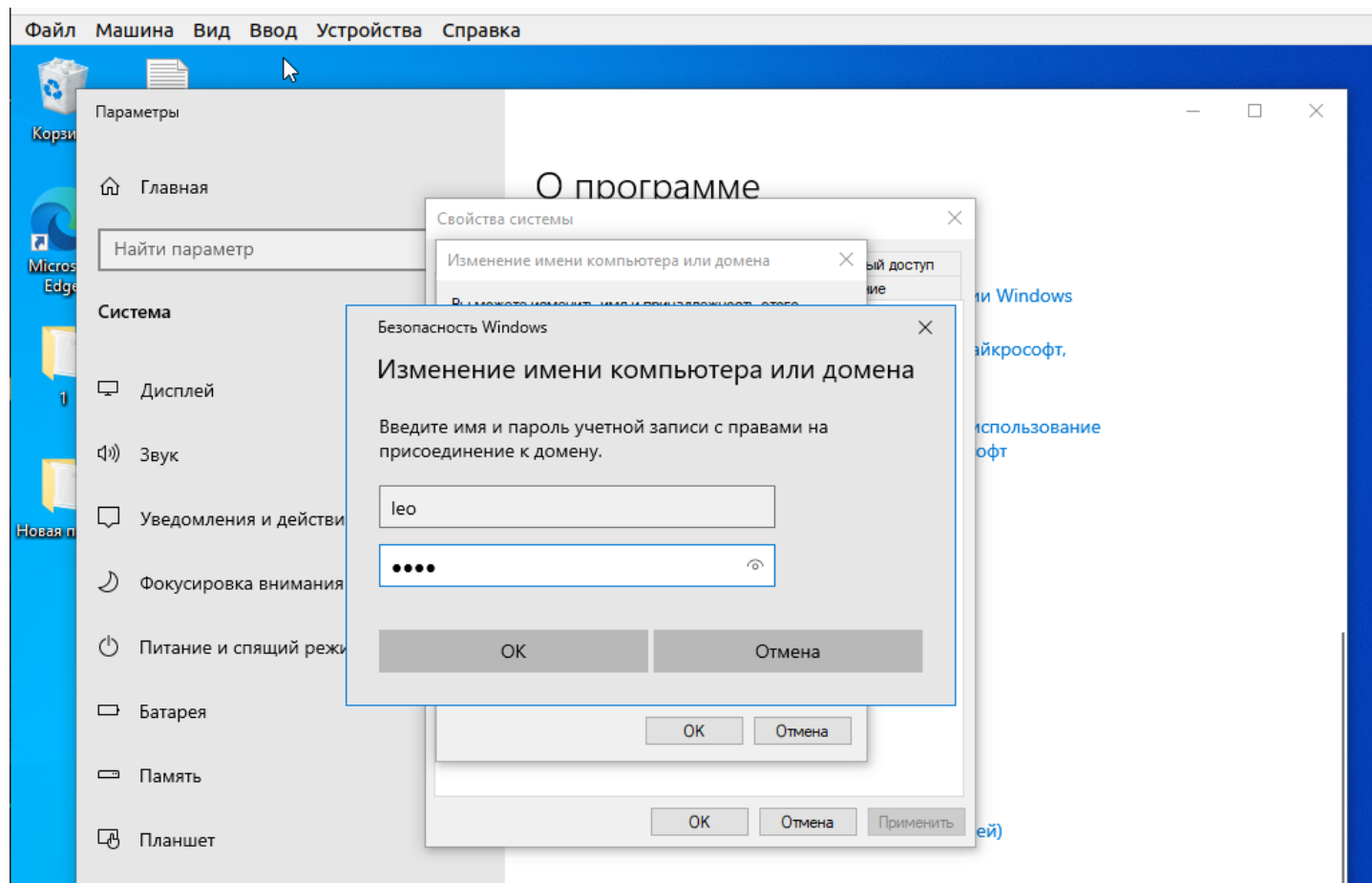
Повышаем роль данного сервера до уровня контроллера домена



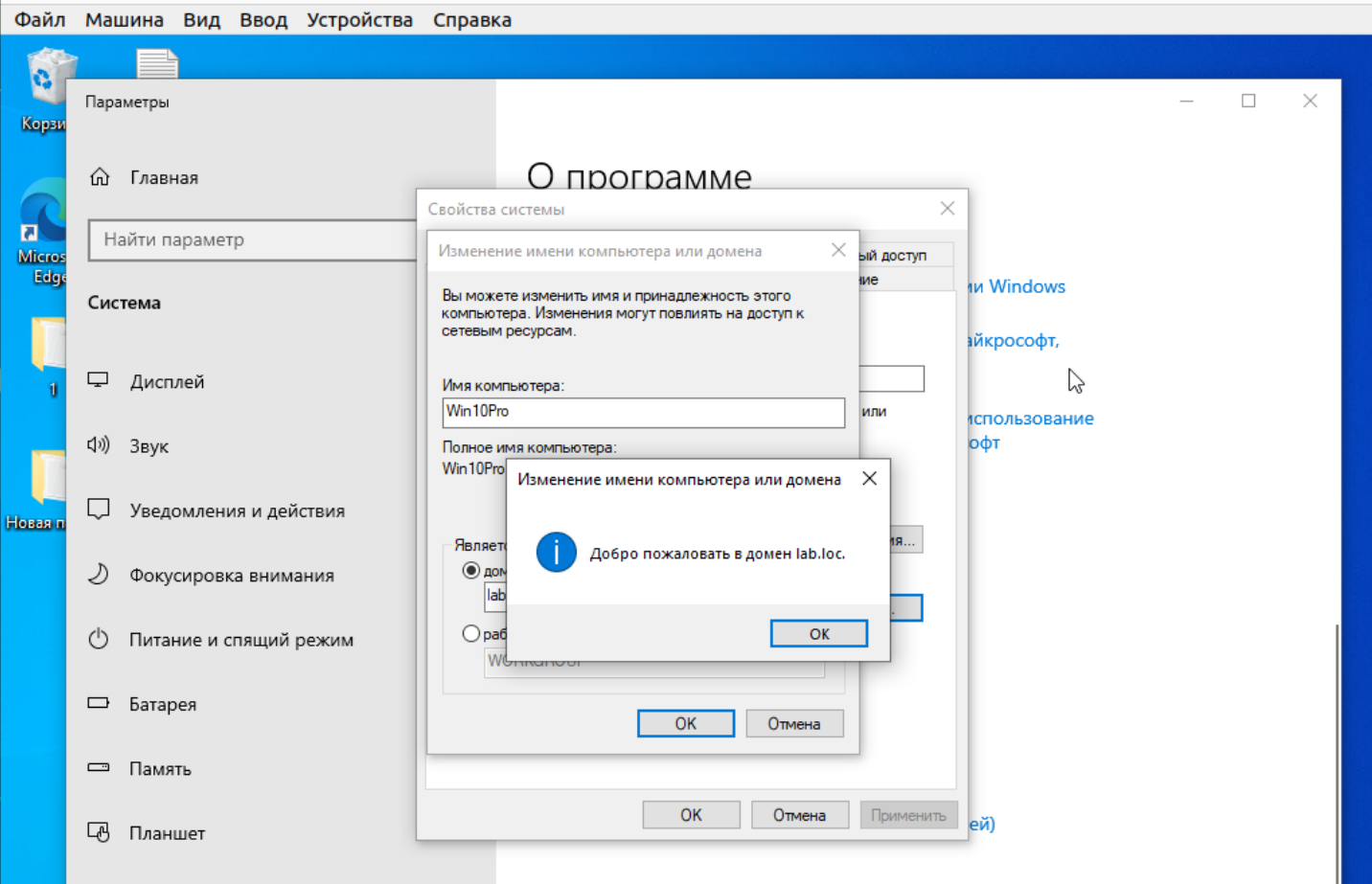
Далее сопоставляем полное доменное имя DNS сервера и ip адрес контроллера



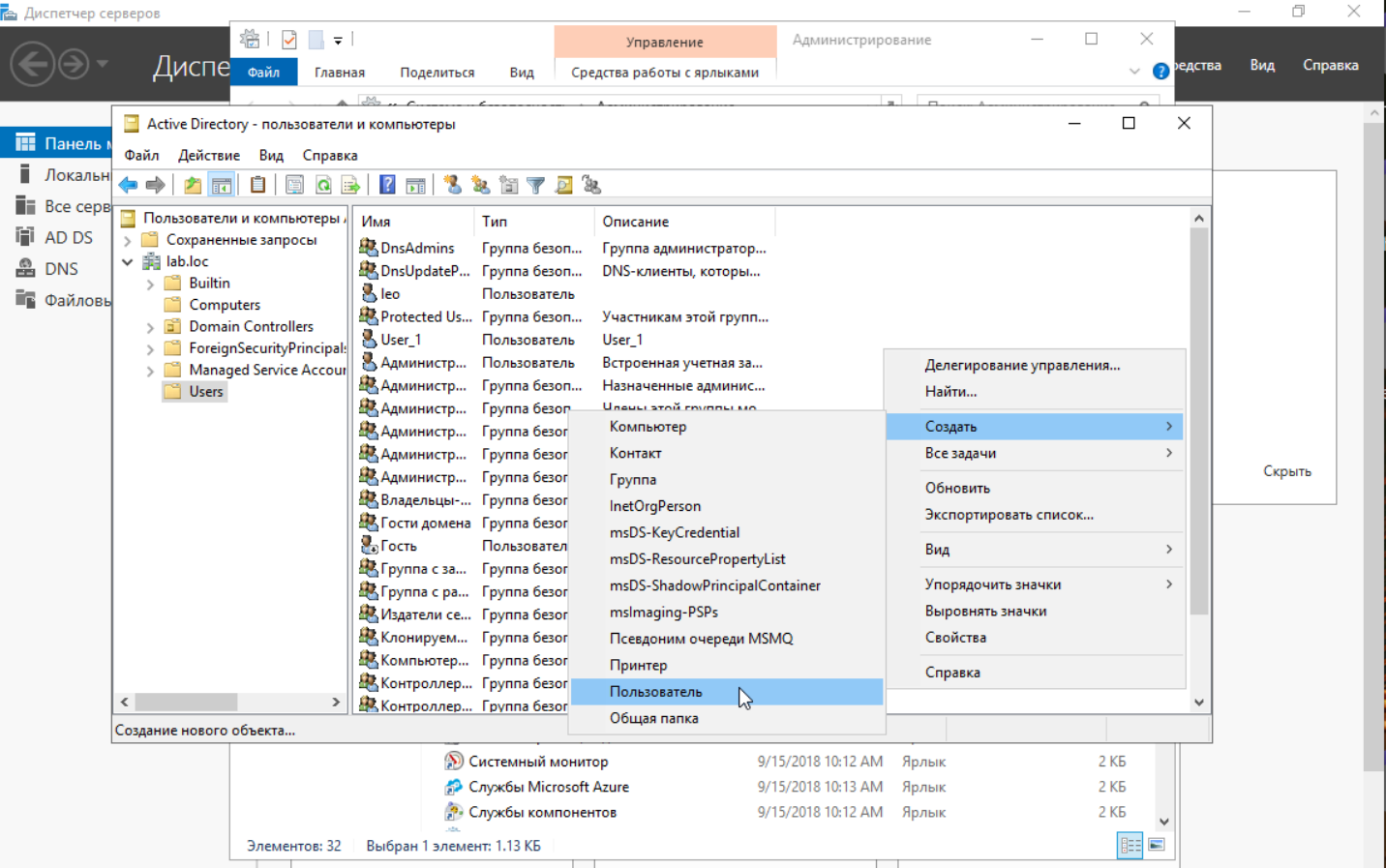
Далее с машины клиента заходим в изменение домена, вводим созданный нами и заходим как администратор.



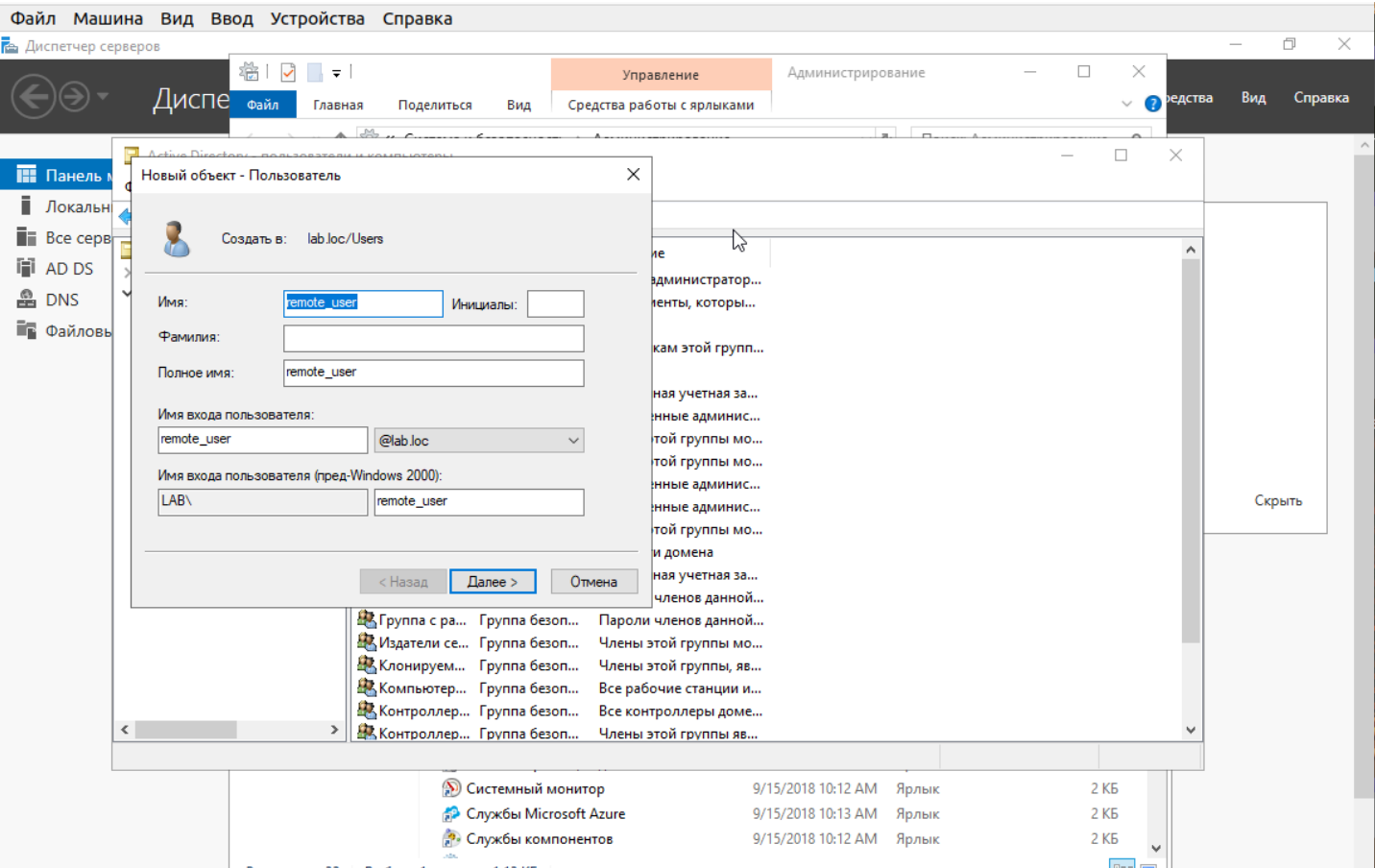
Успешно вошли



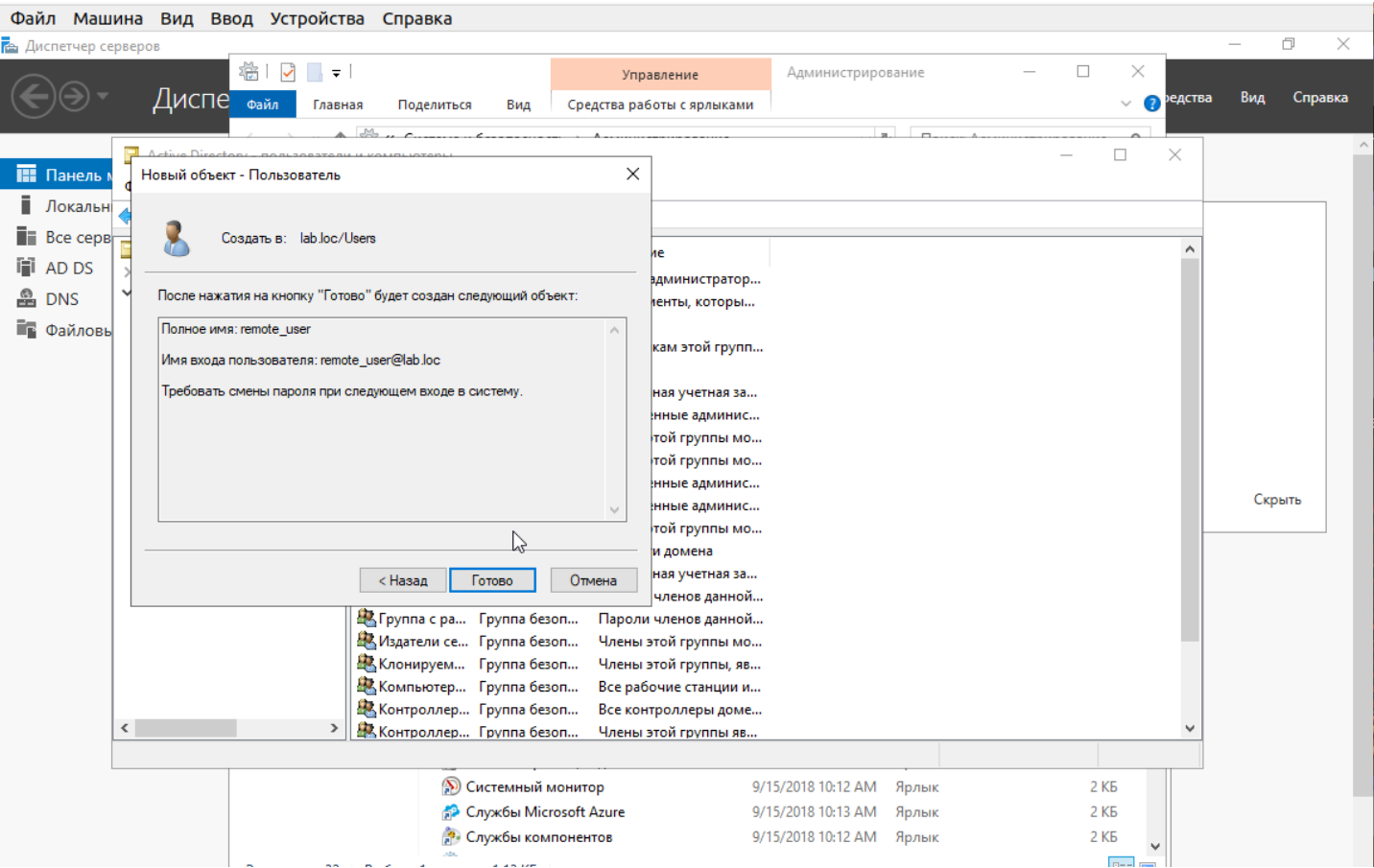
Теперь с сервера можно создать нового пользователя



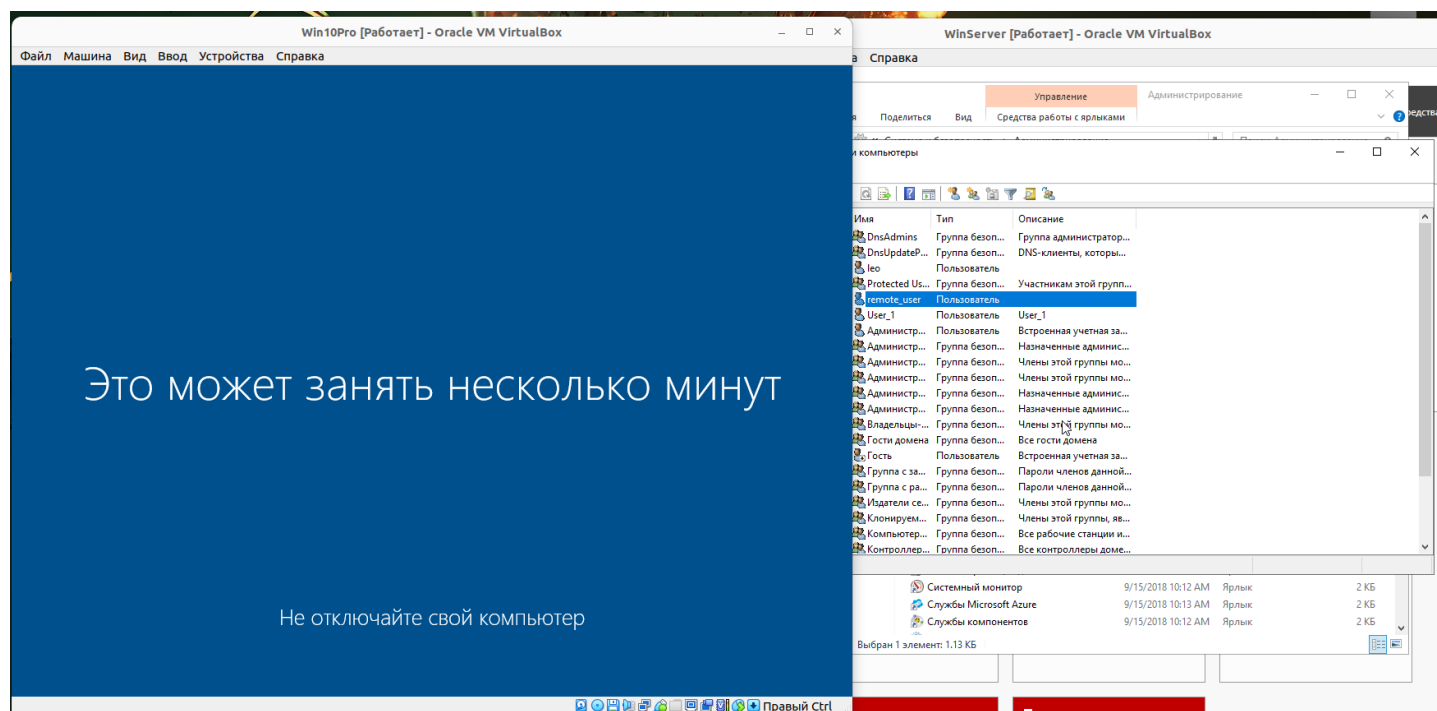
Вводим необходимые данные



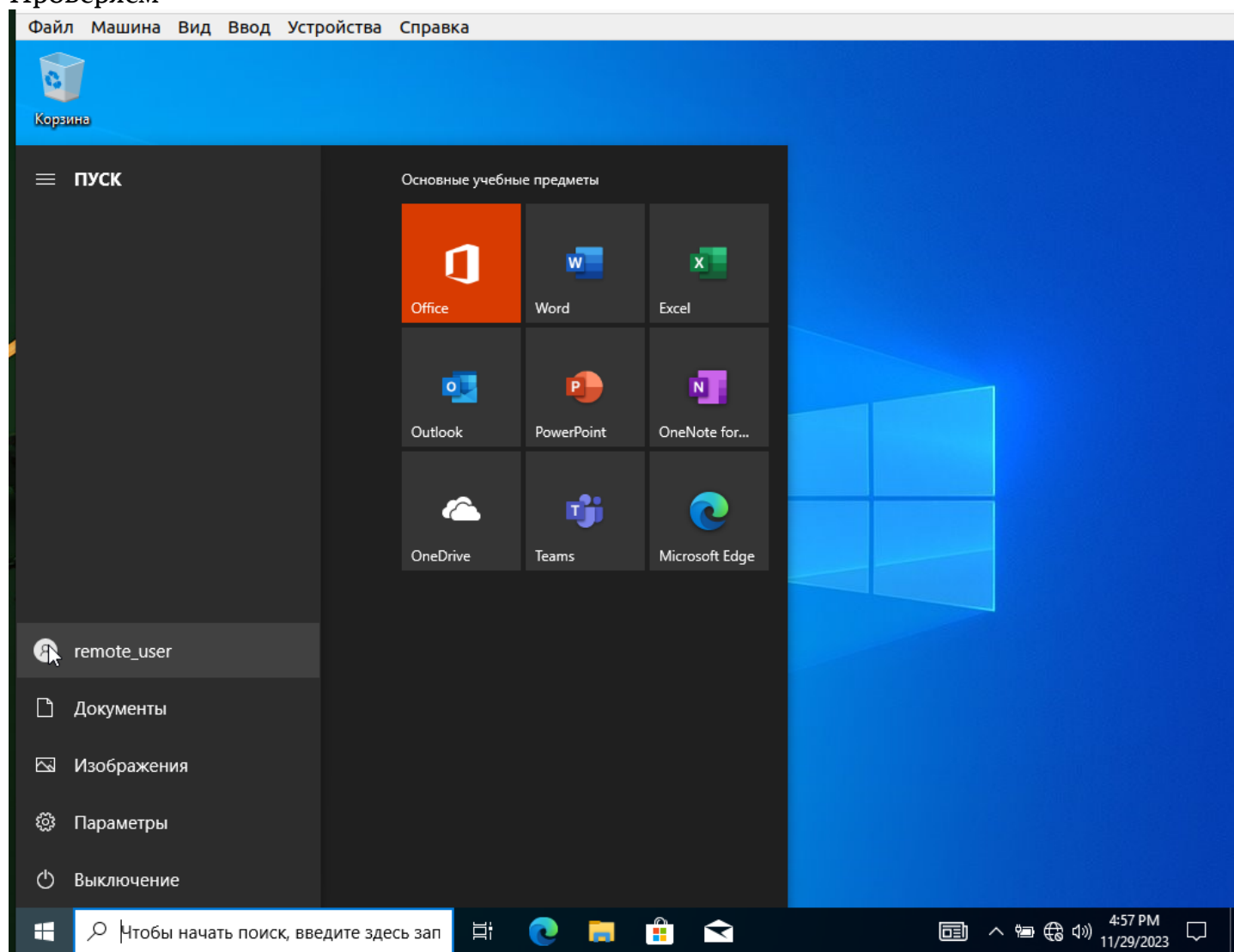
Жмем готово



Теперь можно войти с клиентской машины под новым удаленным пользователем



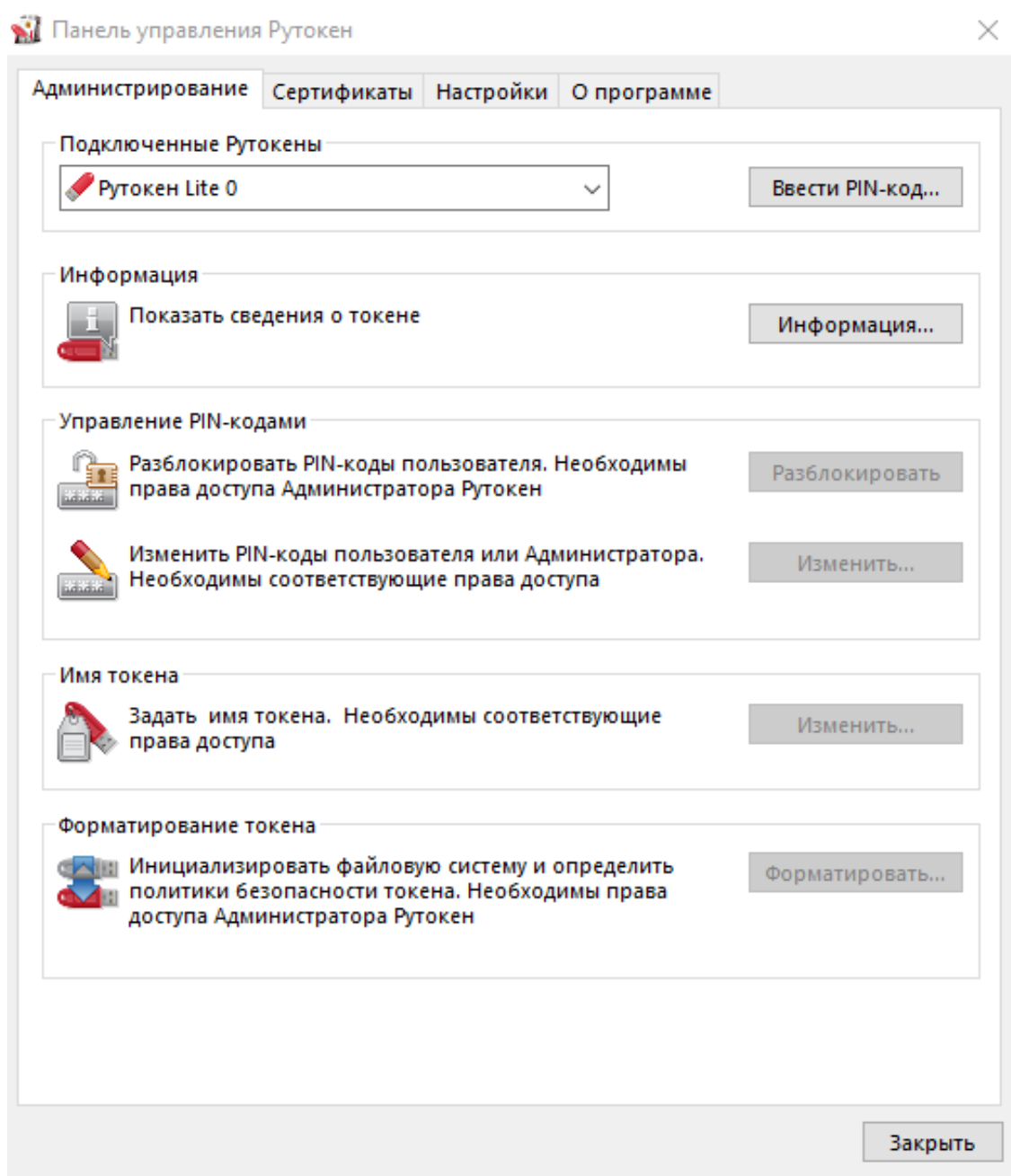
Проверяем



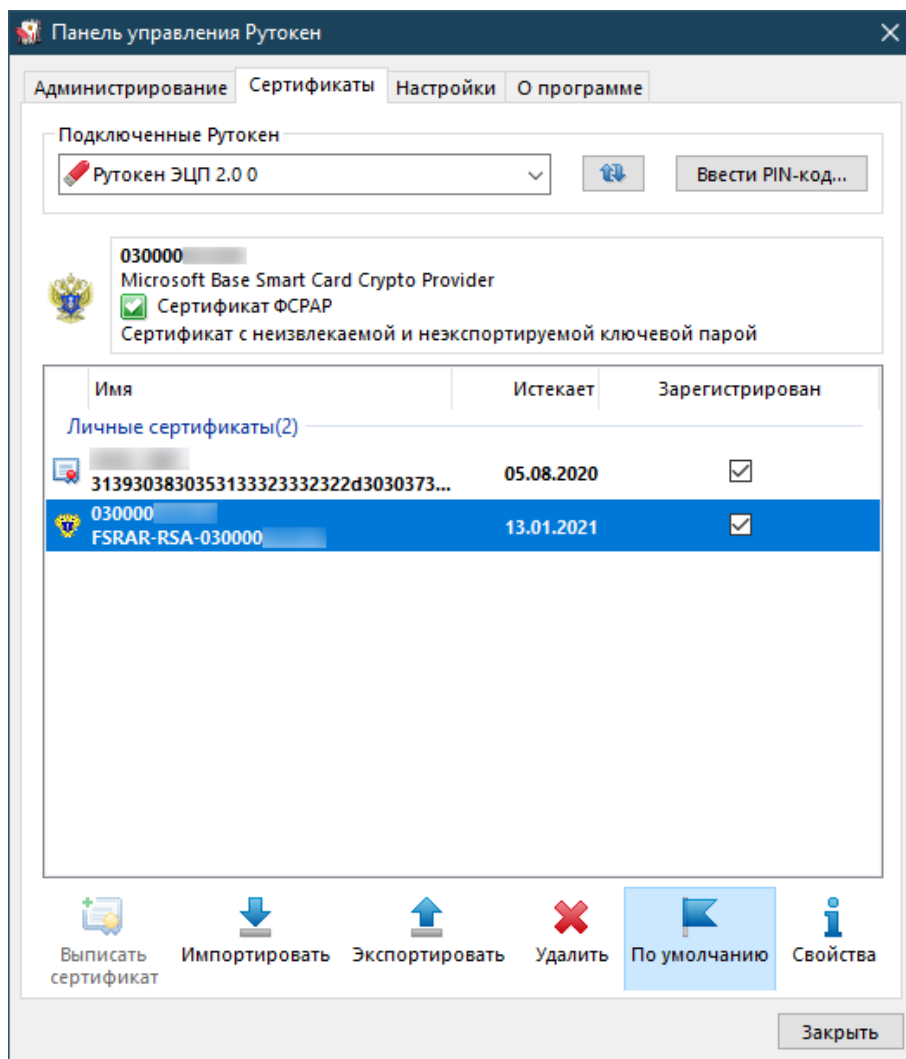
2. Опишите настройку и работу со смарт-картами

Смарт-карта в Windows - это вид физической или виртуальной карточки, содержащей микропроцессор и хранилище данных. Она используется для аутентификации пользователя, обеспечения безопасного доступа к компьютеру или защиты конфиденциальной информации.

Для работы со смарт-картами на локальных машинах необходимо подготовить окружение путем установки программного обеспечения под конкретную смарт-карту. В моем случае смарт-карта типа Рутокен, значит нужно установить соответствующий драйвер:

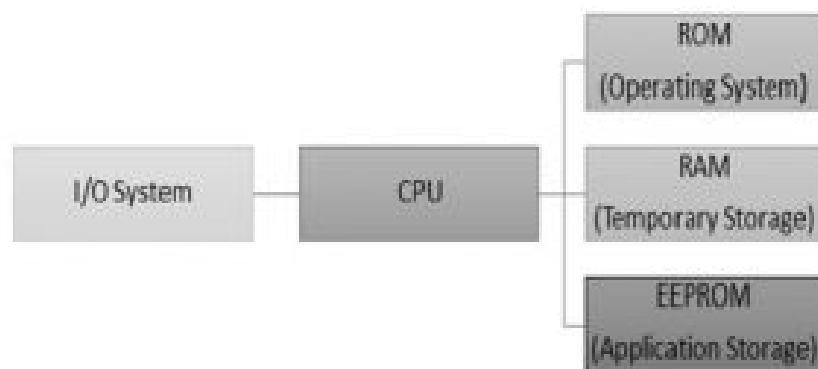
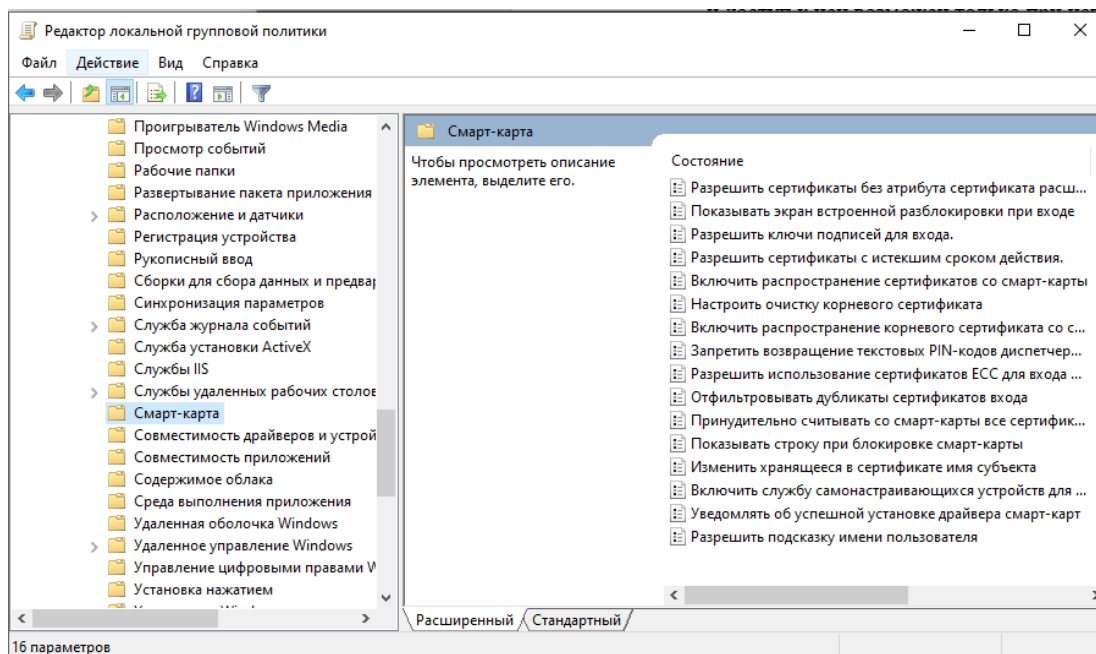


Сама смарт-карта должна быть выдана удостоверяющим центром и содержать минимальный объем информации, необходимый для аутентификации и авторизации. После установки драйверов панель управления Рутокен обнаруживает смарт-карту:



Для **локальной** работы интеграция смарт-карт проводится непосредственно самим пользователем, и составляет подготовку окружения и настройку нового способа аутентификации. Впоследствии для входа в систему нужно будет вставить физический носитель и ввести опциональные шаги для авторизации (пароль, ПИН-код и т.п.).

Для **домена** в корпоративной среде установкой способов входа занимается администратор сервера, который помимо активации входа по смарт-карте способен конфигурировать политики работы с картами:



Архитектура смарт-карт

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

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.

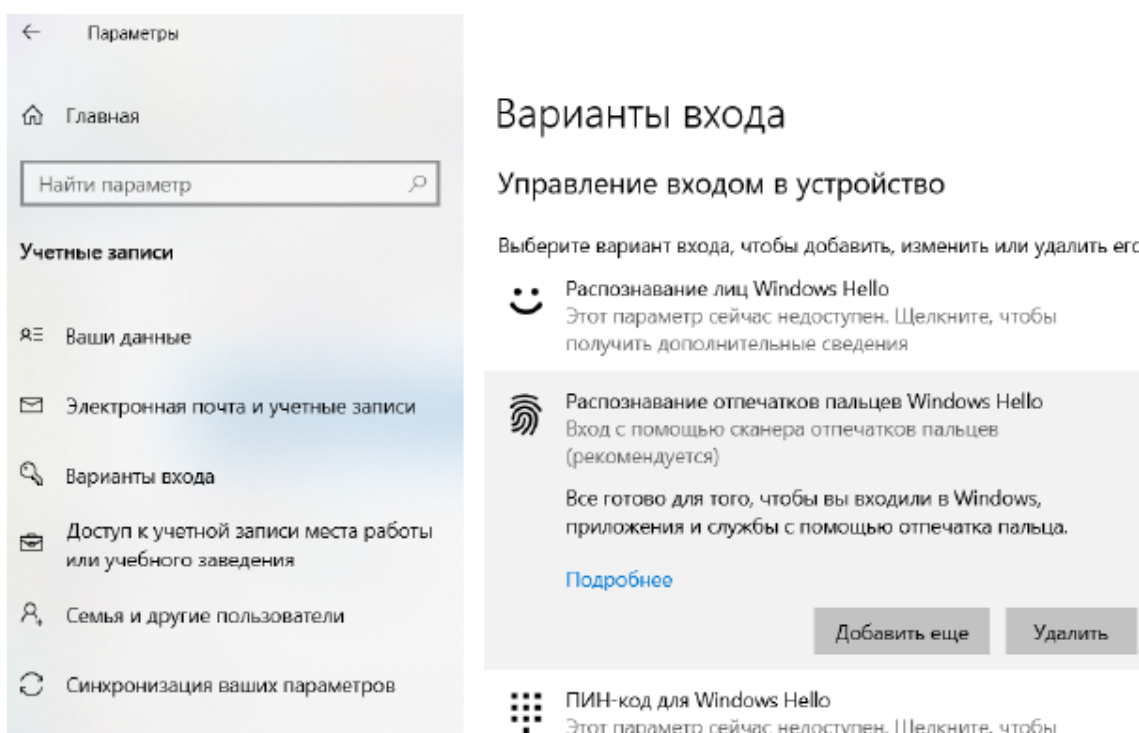


- **Объединение двухфакторной аутентификации и биометрического распознавания в одном модуле**

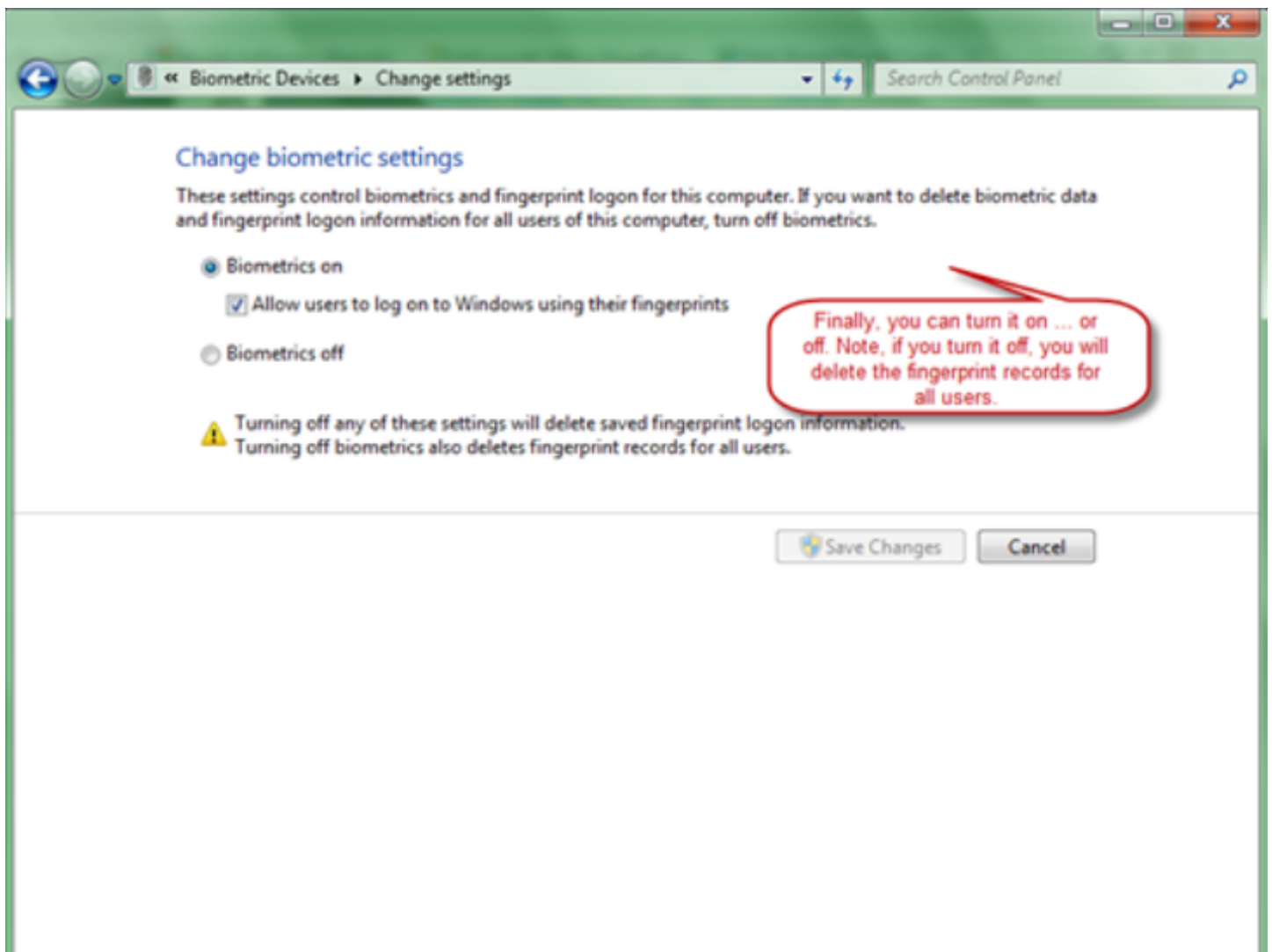
В первоначальной версии Windows Hello данной интеграции не было, однако её переместили позже в один модуль для удобства.

- **Процесс настройки и предустановленные пакеты**

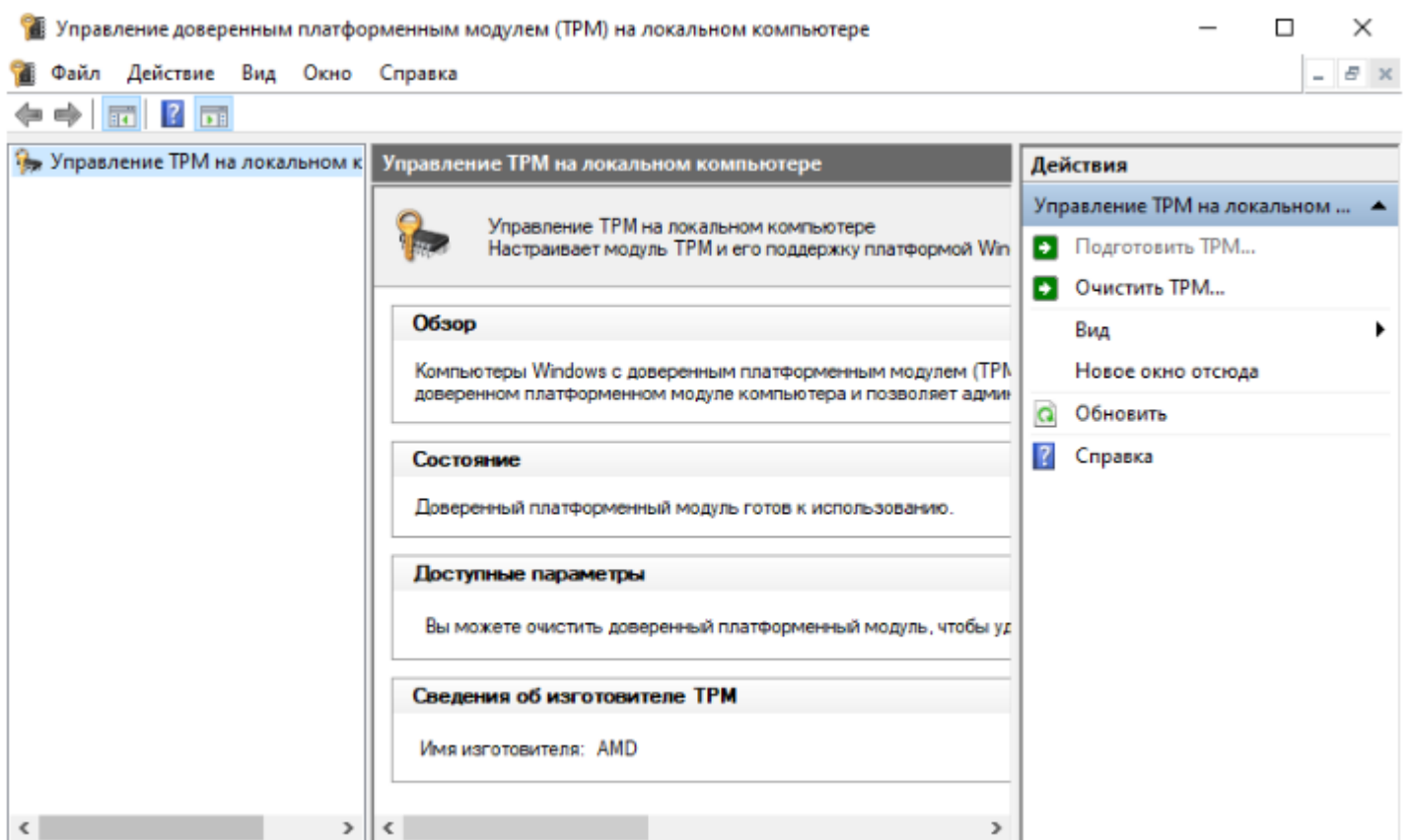
В Windows 10 биометрические функции вынесены в раздел настройки конкретных пользователей.



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



Также Windows 10 стала хранить биометрические данные на аппаратном «Доверенном платформенном модуле», не передавая их нигде по сети или в облаке:



Были регламентированы ограничения на устройства, с которыми работает Windows Hello, например, требования к датчику для сканирования отпечатков пальцев имеют вид:

Допустимый диапазон производительности для сенсорных датчиков с любым размером области сканирования

- Коэффициент ложного пропуска (FAR): $<0,001-0,002\%$
- Эффективный действующий FRR с защитой от подделывания или определением живучести: $<10\%$

Допустимый диапазон производительности для датчиков с поддержкой движения пальцем

- Коэффициент ложного пропуска (FAR): $<0,002\%$
- Эффективный действующий FRR с защитой от подделывания или определением живучести: $<10\%$

Выводы

В результате выполнения лабораторной работы я узнал основные типы учетных записей в Windows, научился делегировать им разные привилегии и создавать пользователей разными способами. В качестве задания по варианту реализовал механизм Active Directory на базе Windows Server 2019, на котором я развернул DNS-сервер и создал локальный домен. Возникли некоторые проблемы с подключением основной и виртуальной машины по сети, но я решил их корректной настройкой сетевого моста. Как результат, могу сказать, что система безопасности в Windows – вещь очень комплексная, и в зависимости от настройки она может сделать вашу систему как защищенной, так и уязвимой.