

Федеральное государственное автономное образовательное учреждение высшего  
образования  
«Национальный исследовательский университет ИТМО»

Факультет программной инженерии и компьютерной техники

**Лабораторная работа 1**

**«Учетные записи и авторизация в ОС MS Windows»**

по дисциплине

**«Информационная безопасность»**

Вариант № 1

Группа: Р34102

Выполнил: Лапин А.А.

Проверил:  
Рыбаков С.Д.

Санкт-Петербург  
2024г.

# Оглавление

<b>Оглавление</b>	<b>2</b>
<b>Цель работы</b>	<b>4</b>
<b>Программно-аппаратные средства, используемые при выполнении работы</b>	<b>5</b>
<b>Основная часть</b>	<b>6</b>
1    Определения . . . . .	6
2    Создание пользователя . . . . .	6
Вариант 1. Создание нового пользователя в Параметрах Windows 11 . . . . .	6
Вариант 2. Создание нового пользователя в Панели управления . . . . .	10
Вариант 3. Создание пользователя в окне управления учетными записями пользователей . . . . .	11
Вариант 4. Создание пользователя с помощью командной строки . . . . .	15
Вариант 5. Создание пользователя с помощью PowerShell . . . . .	16
Возможности пользователя по изменению конфигурации системы . . . . .	17
3    Создание администратора . . . . .	20
Вариант 1. Создание администратора в Параметрах Windows 11 . . . . .	20
Вариант 2. Создание администратора в Управлении учетными записями пользователей . . . . .	20
Вариант 3. Создание администратора с помощью командной строки . . . . .	21
Ограничения администратора по конфигурации системы . . . . .	22
4    Параметры контроля учетных записей пользователей (UAC) . . . . .	24
Ползунок User Account Control . . . . .	24
5    Выполнить настройки механизмов защиты ОС Windows в соответствии с вариантом . . . . .	25
Меры по усилению парольной защиты. . . . .	26
Меры по усилению парольной защиты с помощью политик блокировки учетной записи в Windows 11 . . . . .	27
Меры по усилению парольной защиты с помощью команды Net Accounts . . . . .	28
6    Анализ реализации механизма защиты в ОС Windows . . . . .	29
6.1    Анализ соответствия механизма защиты ОС Windows 11 классу защищенности 1Г . . . . .	30
Соответствие подсистемы управления доступом . . . . .	30
Соответствие подсистемы регистрации и учета . . . . .	30
Соответствие подсистемы обеспечения целостности . . . . .	31
Вывод . . . . .	31
6.2    Анализ соответствия защиты Windows 11 классу защищенности 6 . . . . .	32
Дискреционный принцип контроля доступа (ПРД) . . . . .	32
Идентификация и аутентификация . . . . .	32
Тестирование . . . . .	33
Документация . . . . .	33
Тестовая и проектная документация . . . . .	33
6.3    Заключение . . . . .	33
6.4    Ключевые выводы . . . . .	34
7    Анализ результатов выполнения лабораторной работы . . . . .	34
7.1    Создание пользователей и администраторов . . . . .	34
7.2    Усиление парольной защиты . . . . .	34

7.3	Настройка контроля учетных записей пользователей (UAC) . . . . .	34
7.4	Анализ соответствия механизма защиты ОС Windows . . . . .	34
7.5	Заключение . . . . .	34

## **Цель работы**

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

# Программно-аппаратные средства, используемые при выполнении работы

Для выполнения работы было использовано ПО Parallels Desktop.

Характеристики созданной виртуальной машины:

The screenshot displays the system specifications for a Parallels ARM Virtual Machine named "8BC1". The interface includes sections for device characteristics and Windows system details, along with activation and licensing information.

**8BC1**  
Parallels ARM Virtual Machine

Переименовать этот ПК

① Характеристики устройства

Имя устройства: 8BC1  
Процессор: Apple Silicon 3.20 GHz (процессоров: 4)  
Оперативная память: 8,00 ГБ  
Код устройства: D84657A9-ED68-402B-84FF-C851A69D5C7F  
Код продукта: 00331-20250-14906-AA610  
Тип системы: 64-разрядная операционная система, процессор ARM  
Перо и сенсорный ввод: Поддержка ввода с помощью пера

Копировать ^

Ссылки по теме Домен или рабочая группа Защита системы Дополнительные параметры системы

Характеристики Windows

Выпуск: Windows 11 Pro  
Версия: 23H2  
Дата установки: 16.03.2024  
Сборка ОС: 22631.3374  
Взаимодействие: Windows Feature Experience Pack 1000.22688.1000.0

Активация Windows  
Чтобы активировать Windows, перейдите в раздел "Параметры".

[Соглашение об использовании служб Майкрософт](#)  
[Условия лицензионного соглашения на использование программного обеспечения корпорации Майкрософт](#).

Рис. 1: Характеристики системы

# Основная часть

## 1 Определения

- диспетчер учетных записей (SAM);
- монитор безопасности (SRM);
- маркер доступа (access token);
- идентификатор безопасности (SID);
- привилегии пользователя;
- права пользователя (user rights);
- объект доступа;
- субъект доступа;
- олицетворение (impersonation);
- список контроля доступа (ACE);
- учетная запись;
- домен.

## 2 Создание пользователя

### Вариант 1. Создание нового пользователя в Параметрах Windows 11

1. Откроем Параметры > Учетные записи.

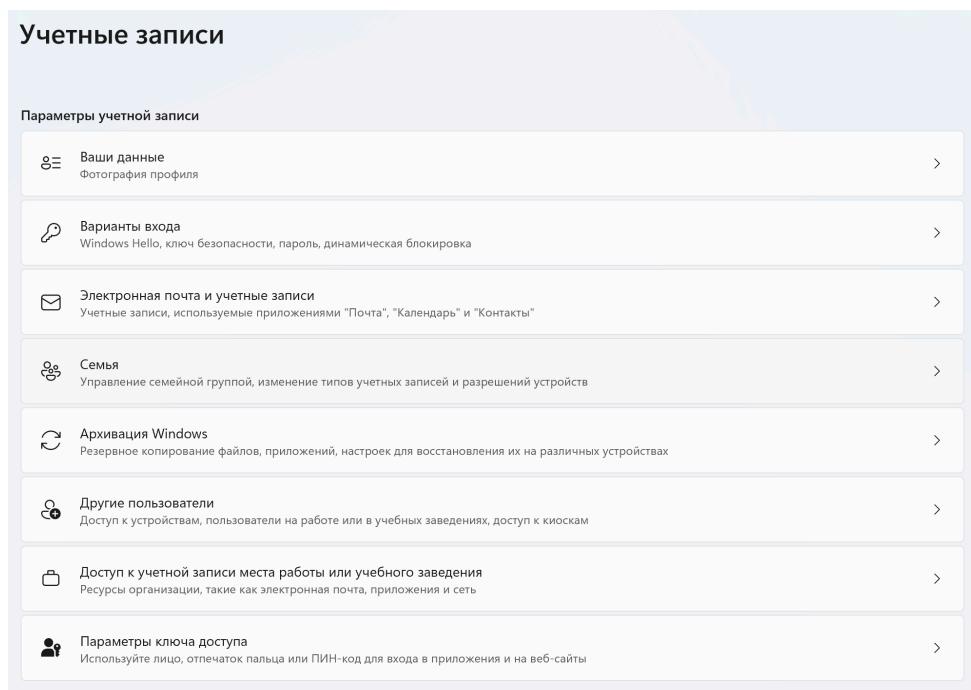


Рис. 2: Параметры учетных записей

2. Откроем Учетные записи > Другие пользователи > Добавить другого пользователя.

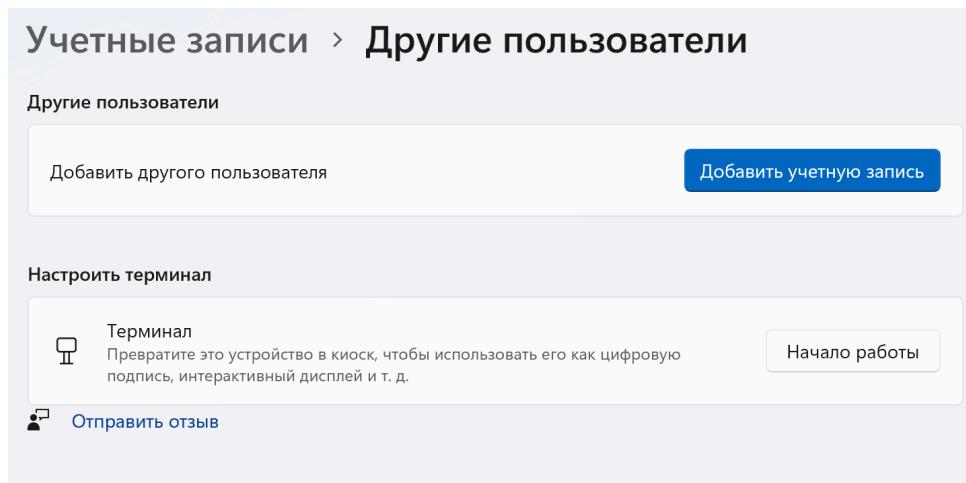


Рис. 3: Другие пользователи

3. Выберем: «У меня нет данных для входа этого человека.»

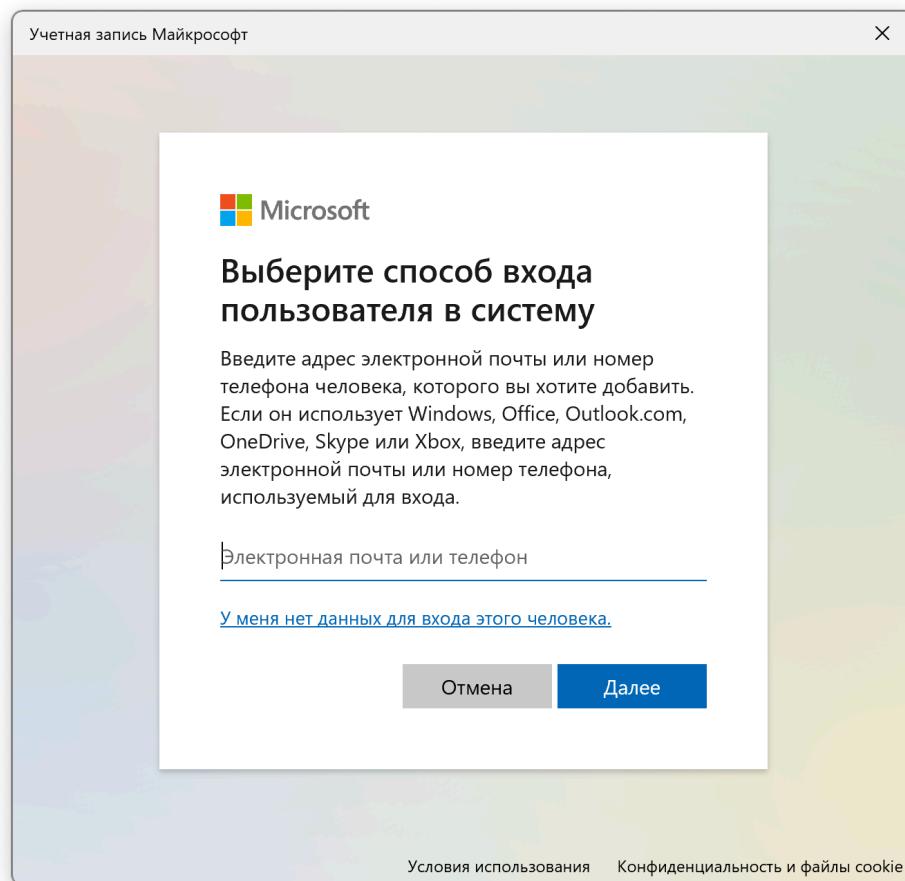


Рис. 4: Добавление пользователя

4. Выберем: «Добавить пользователя без учетной записи Майкрософта»

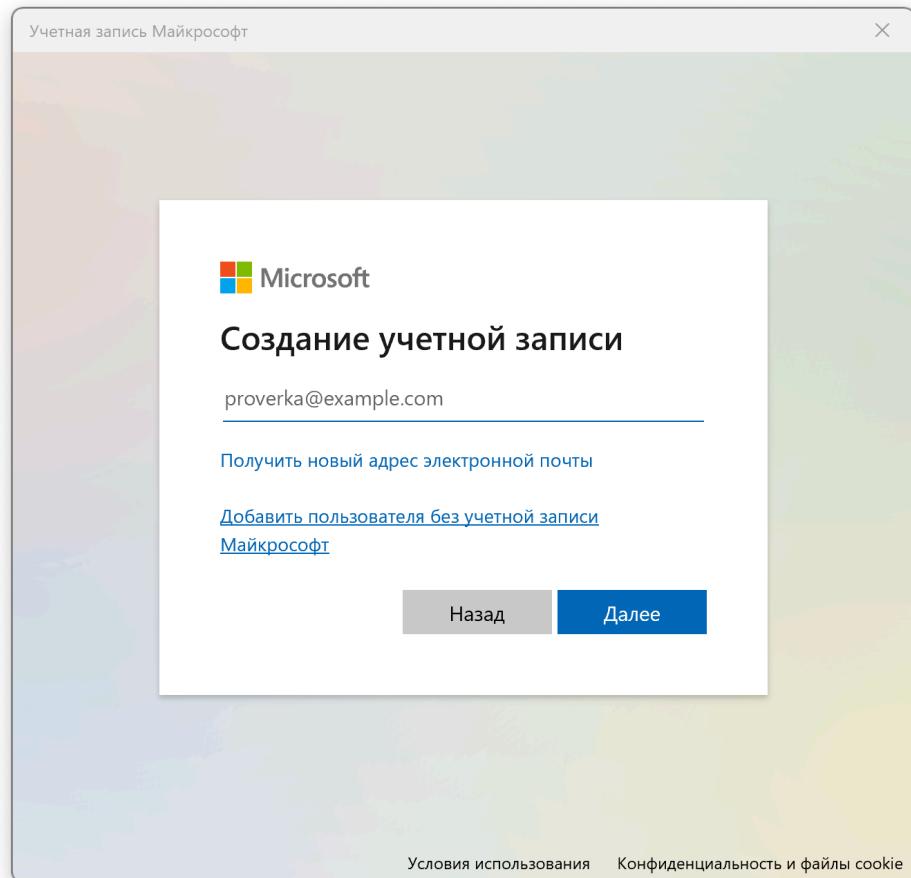


Рис. 5: Создание учетной записи

5. Вводим имя пользователя, пароль и контрольные вопросы.

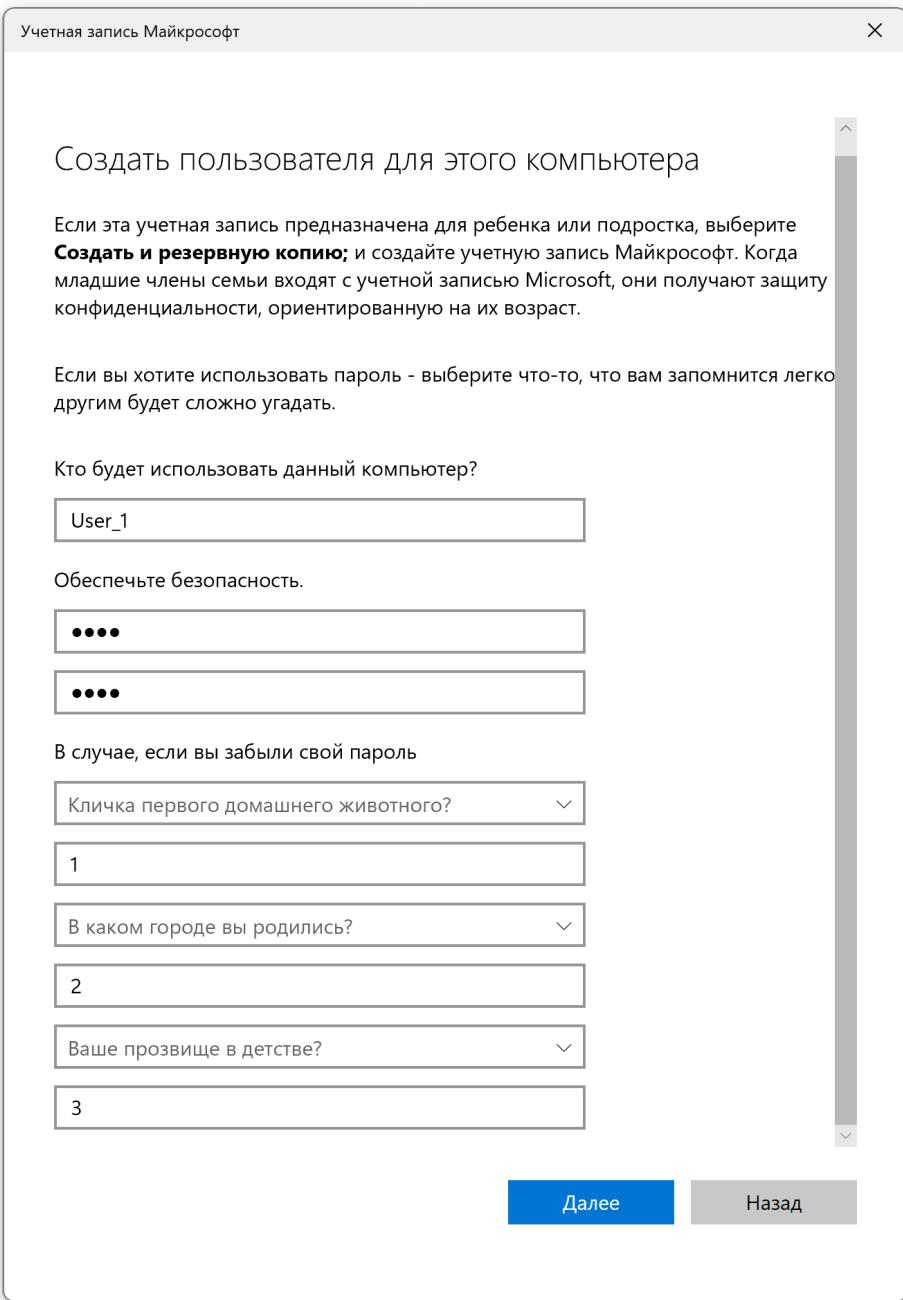


Рис. 6: Создание пользователя

6. Пользователь создан.

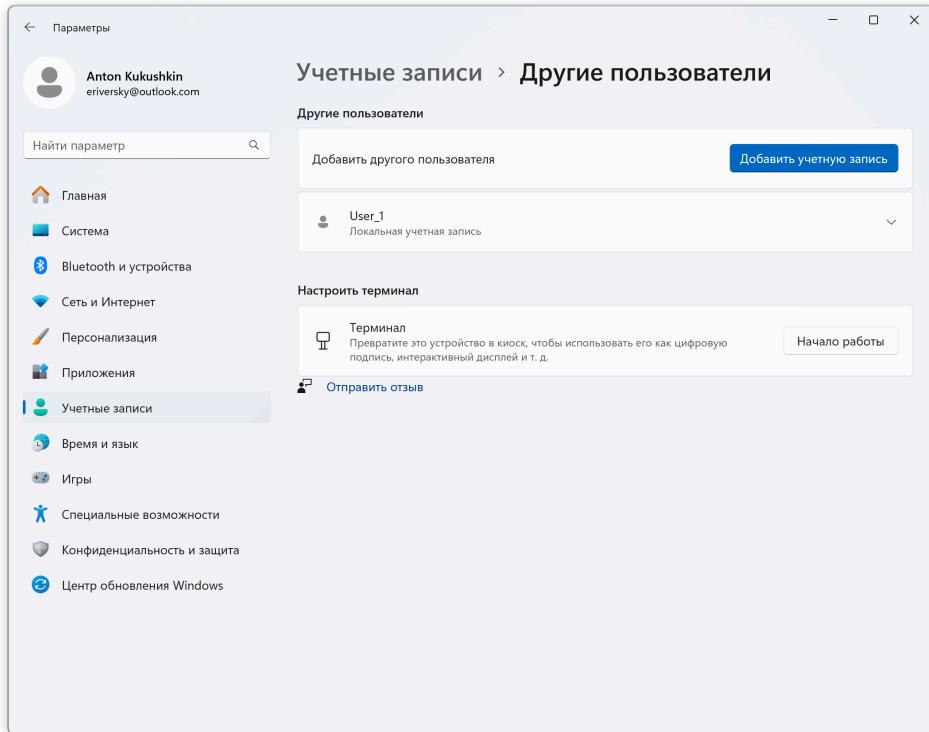


Рис. 7: Пользователь создан

### Вариант 2. Создание нового пользователя в Панели управления

- Переходим в Панель управления > Изменение типа учетной записи > Управление учетными записями > Добавить нового пользователя в окне "Параметры компьютера".

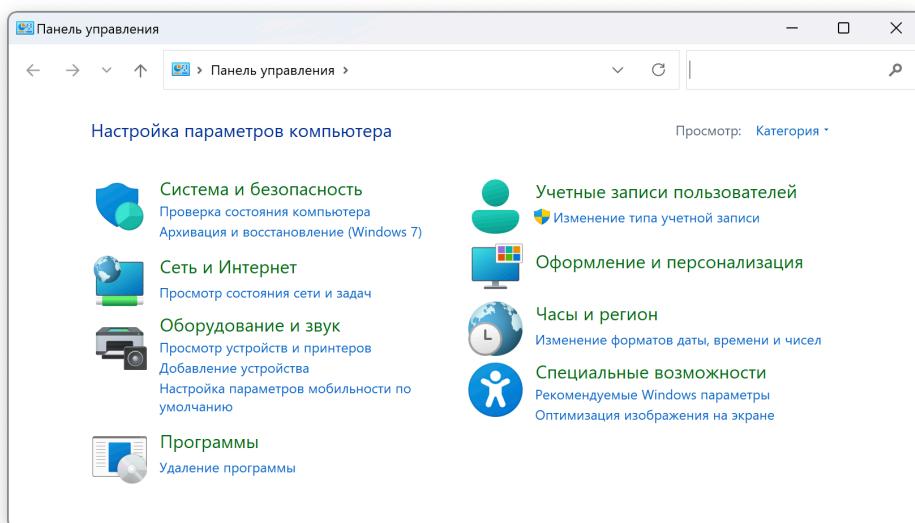


Рис. 8: Панель управления

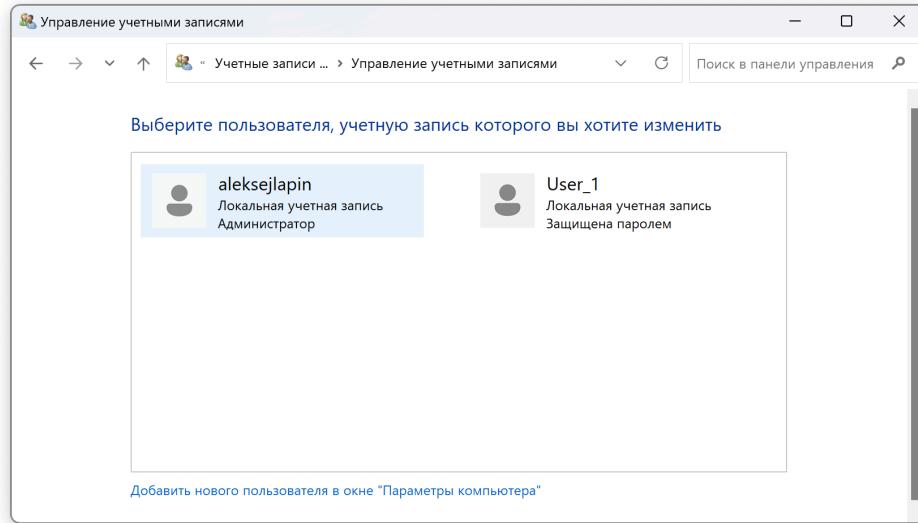


Рис. 9: Управление учетными записями

2. Дальше все действия аналогичны варианту 1.

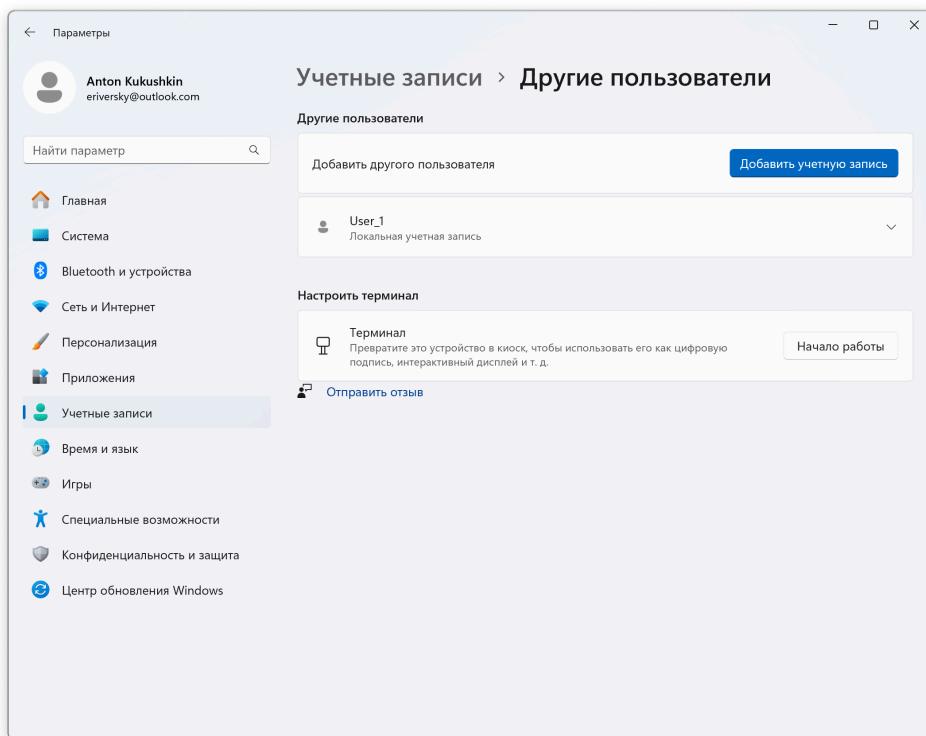


Рис. 10: Другие пользователи

### **Вариант 3. Создание пользователя в окне управления учетными записями пользователей**

1. Нажмите **Ctrl + R**, введите **control userpasswords2** и нажмите **Enter**.

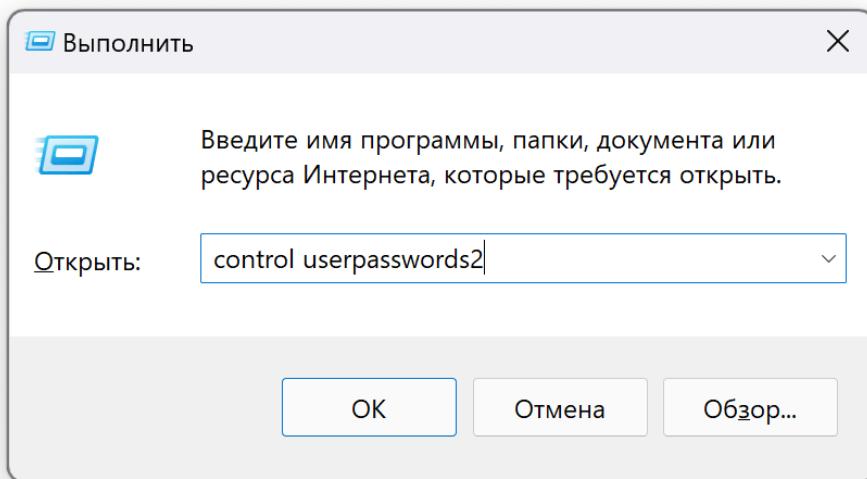


Рис. 11: Выполнение команды

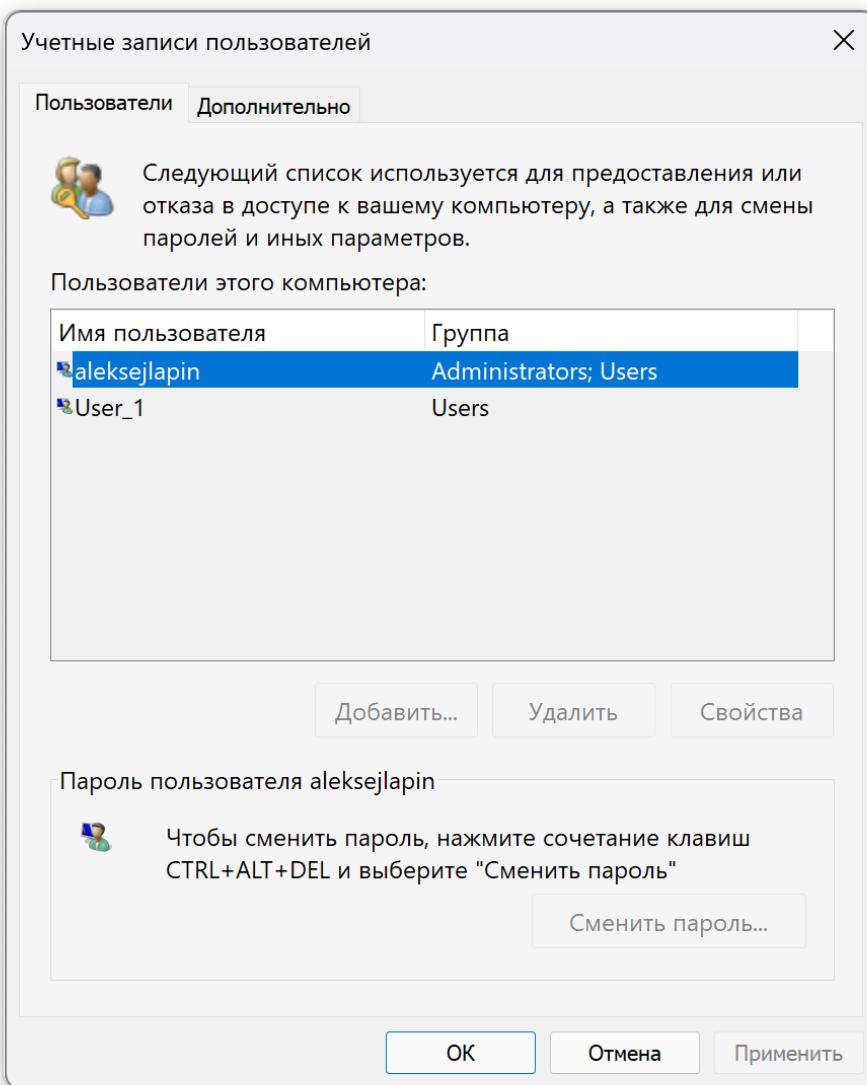


Рис. 12: Управление учетными записями пользователей

2. Переходим в раздел «Дополнительно».

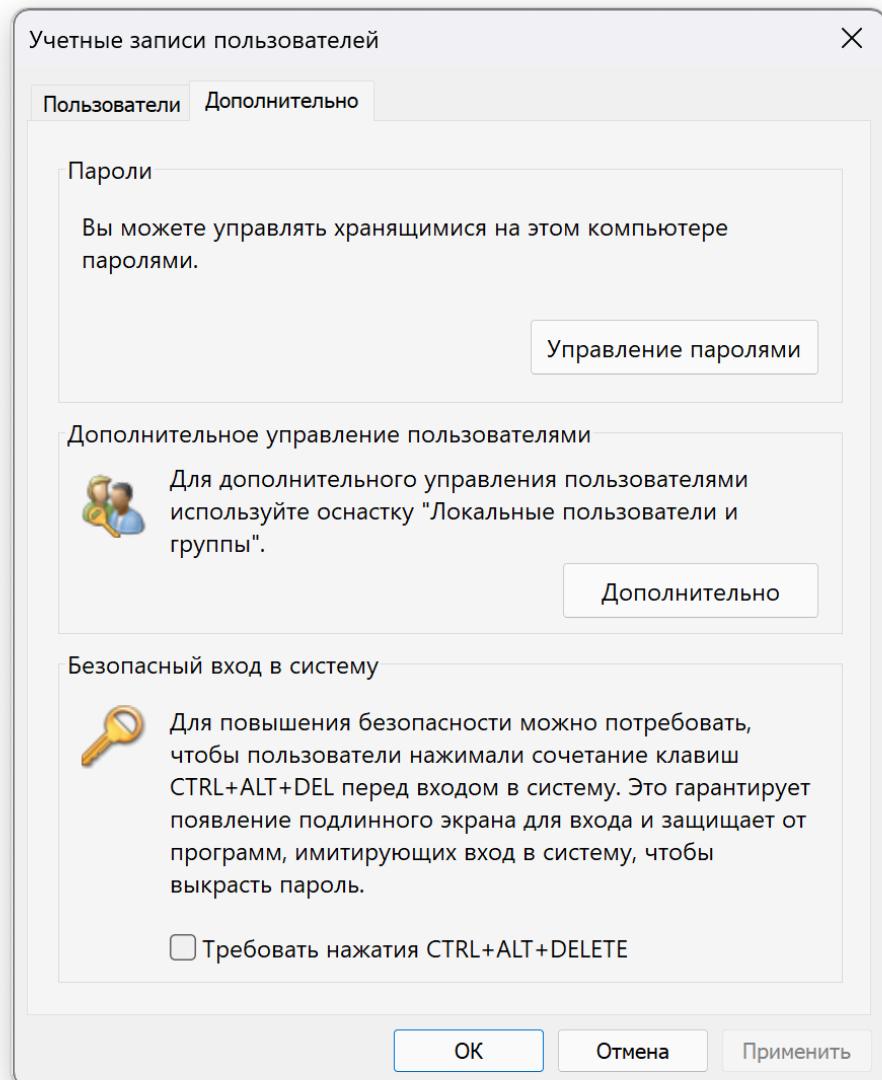


Рис. 13: Управление учетными записями пользователей (дополнительные параметры)

3. Открывается окно управления локальными пользователями и группами.

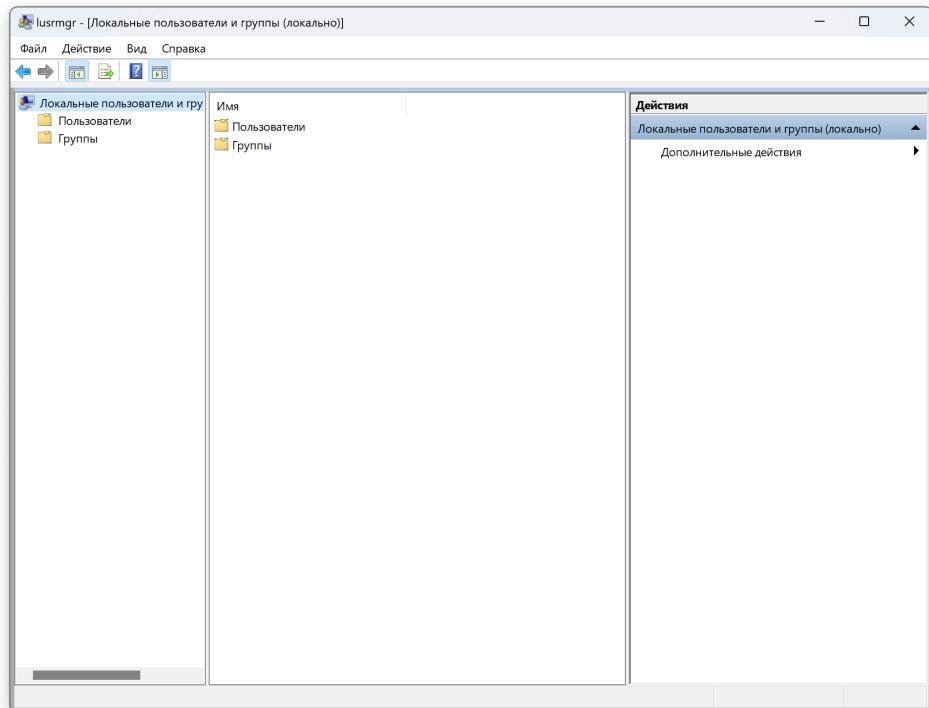


Рис. 14: Управление локальными пользователями и группами

4. Нажимаем правой кнопкой мыши на «Пользователи» и выбираем «Новый пользователь...»

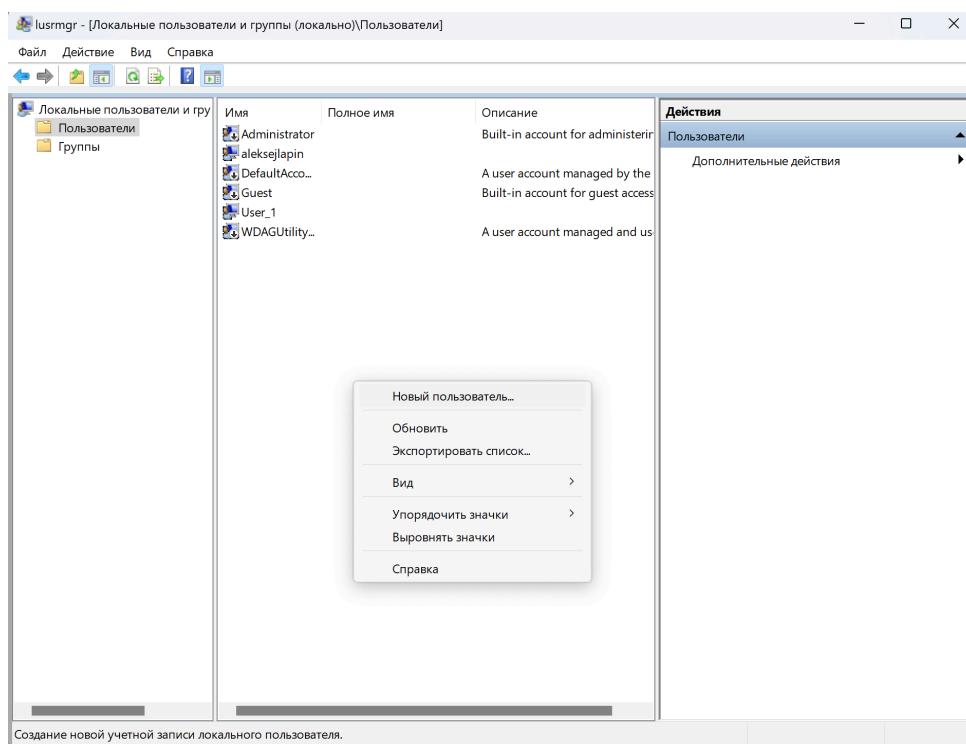


Рис. 15: Управление локальными пользователями и группами (пользователи)

5. Вводим имя пользователя, полное имя и пароль.

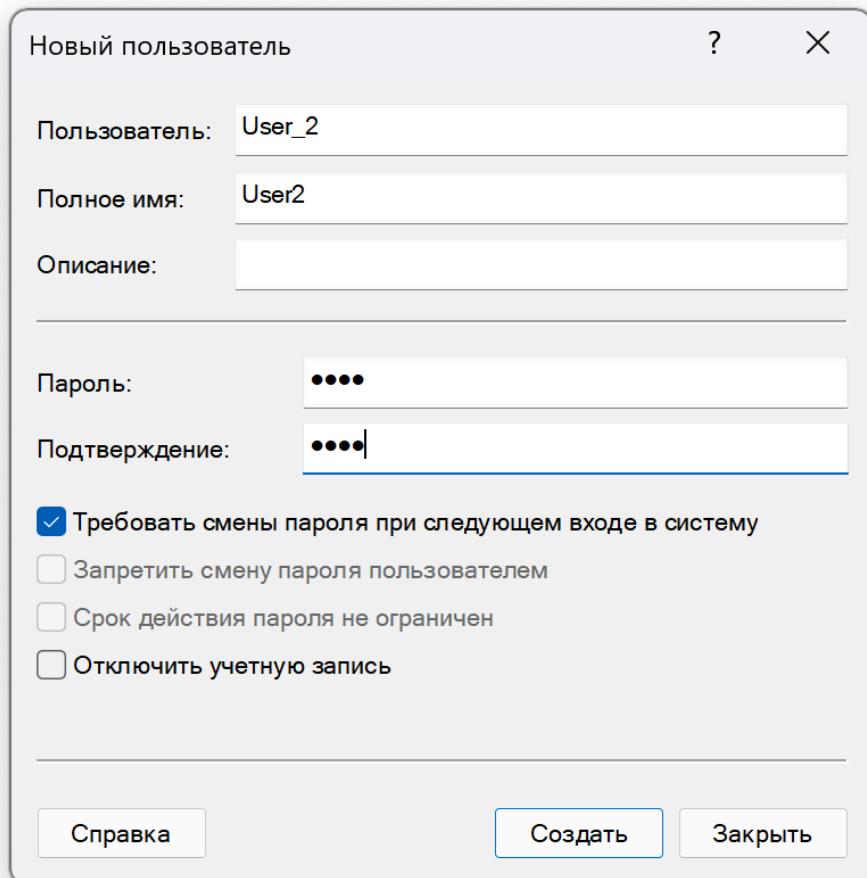


Рис. 16: Создание нового пользователя

6. Новый пользователь создан.

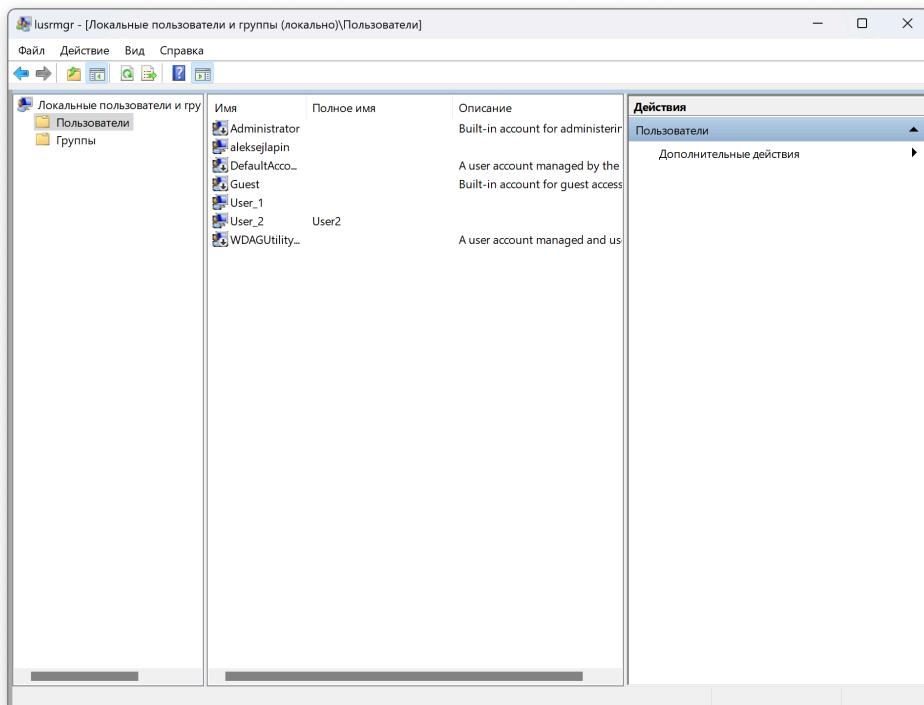


Рис. 17: Новый пользователь

#### Вариант 4. Создание пользователя с помощью командной строки

1. Откроем командную строку от имени администратора.

2. Введем команду `net user <имя пользователя> <пароль> /add`
3. Если пользователь создан, то появится сообщение: Команда выполнена успешно.

```

Administrator: Командная строка
Microsoft Windows [Version 10.0.22631.3374]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Windows\System32>net user User_3 1234 /add
Команда выполнена успешно.

C:\Windows\System32>

```

Рис. 18: Создание пользователя с помощью командной строки

#### 4. Описание команды NET USER

- (a) Команда NET USER предназначена для добавления, редактирования или просмотра учетных записей пользователей на компьютерах. При выполнении команды в командной строке без параметров отображается список учетных записей пользователей Windows, присутствующих на компьютере.
- (b) **Возможности команды Net User**
  - Добавить учетную запись;
  - Добавить пароль учетной записи;
  - Изменить пароль учетной записи;
  - Отключить учетную запись;
  - Удалить учетную запись.

#### Вариант 5. Создание пользователя с помощью PowerShell

1. Откроем PowerShell от имени администратора.
2. Введем команду `New-LocalUser`
3. Введем имя пользователя и пароль.
4. Если пользователь создан, то появится сообщение: `True`
5. Пользователь создан.

```

Administrator: Windows PowerShell
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Установите последнюю версию PowerShell для новых функций и улучшения! https://aka.ms/PSWindows

PS C:\Windows\system32> New-LocalUser

Командлет New-LocalUser в конвейере команд в позиции 1
Укажите значения для следующих параметров:
Name: User_4
Password: ****

Name   Enabled Description
----   ----- -----
User_4 True

PS C:\Windows\system32>

```

Рис. 19: Создание пользователя с помощью PowerShell

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

- Пользователь может менять настройки региона и языка.

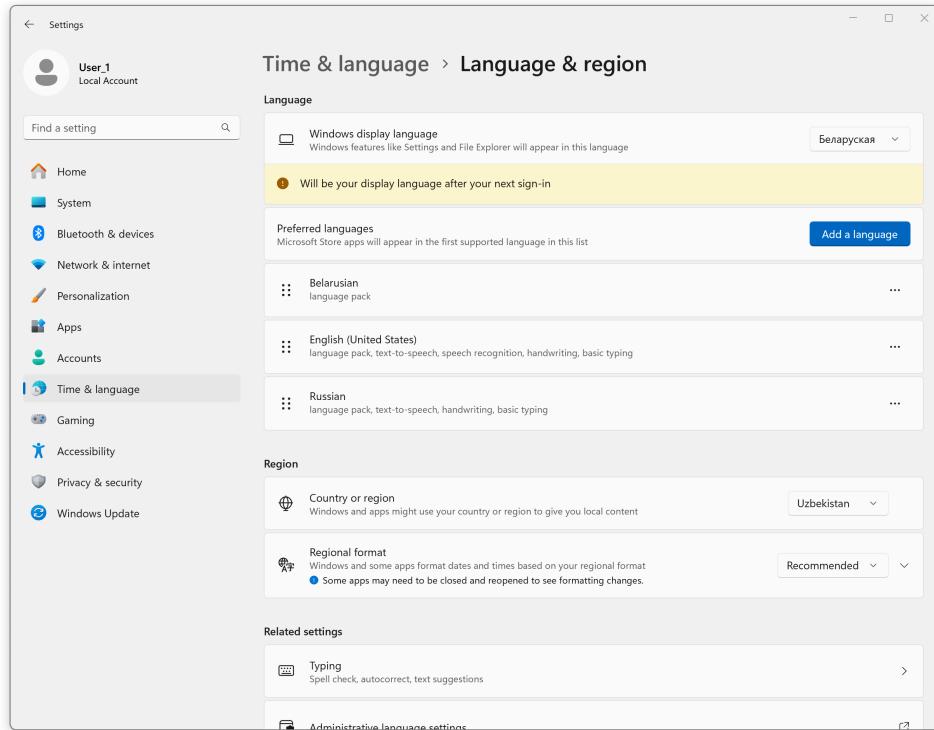


Рис. 20: Настройки региона и языка

- Пользователь может менять параметры персонализации. Например изменить тему оформления.

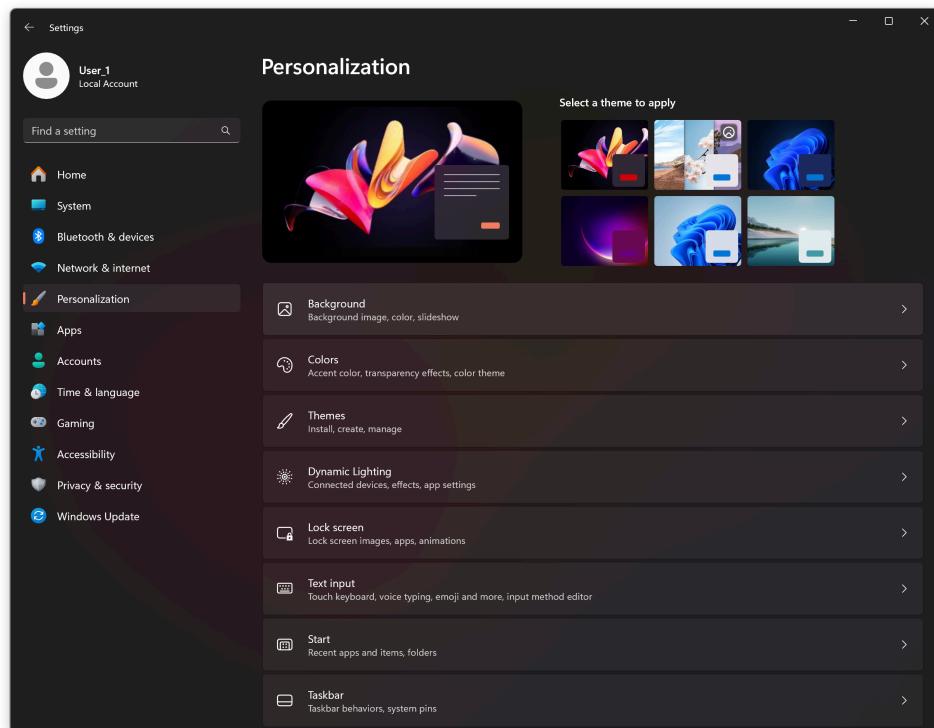


Рис. 21: Персонализация

- Пользователь может изменять параметры Accessibility. Например увеличить шрифт.

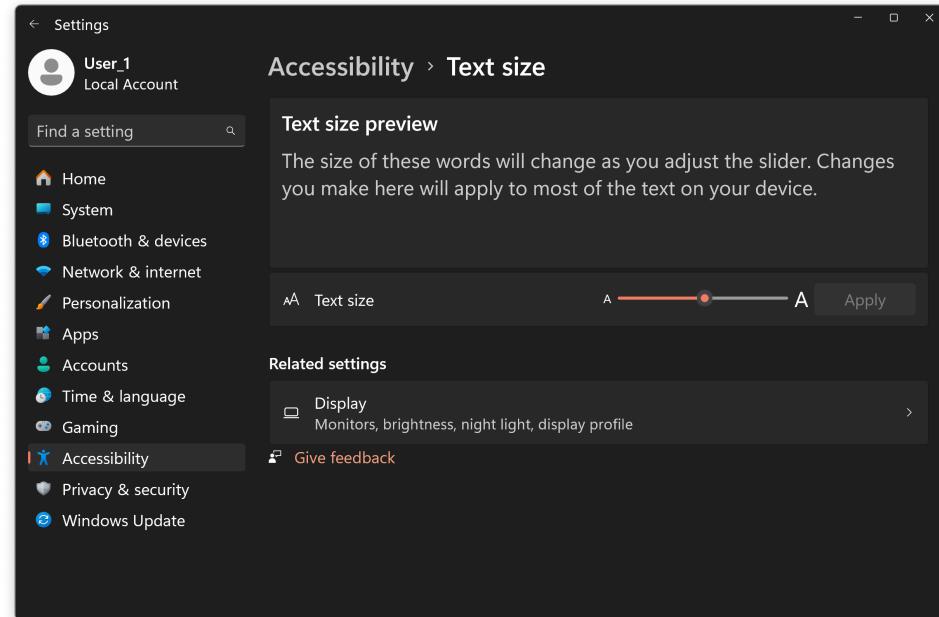


Рис. 22: Accessibility

4. Пользователь может удалять приложения, установленные на компьютере.

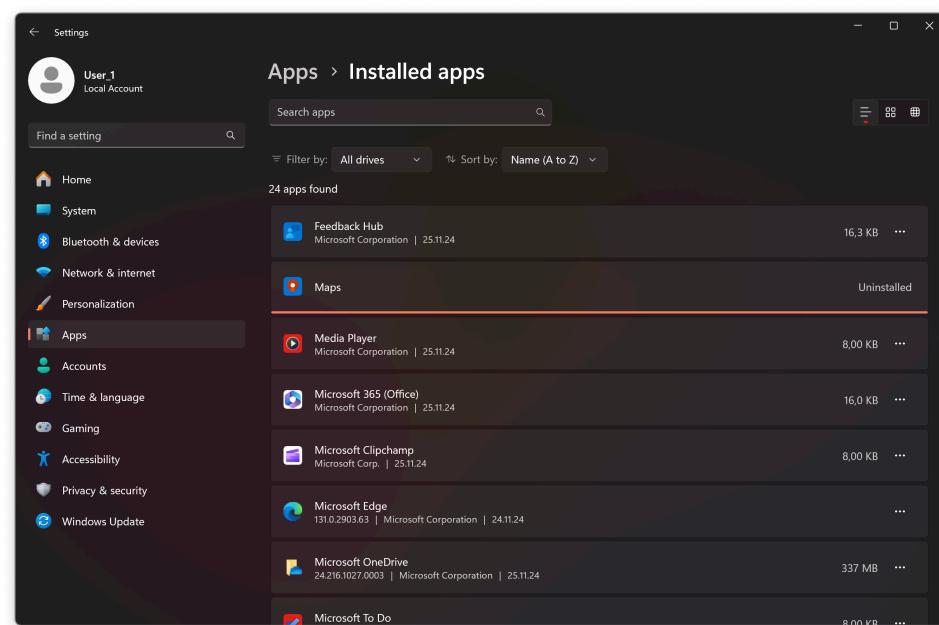


Рис. 23: Удаление приложения

Однако, пользователь не может удалять приложения, требующие выполнения скриптов.

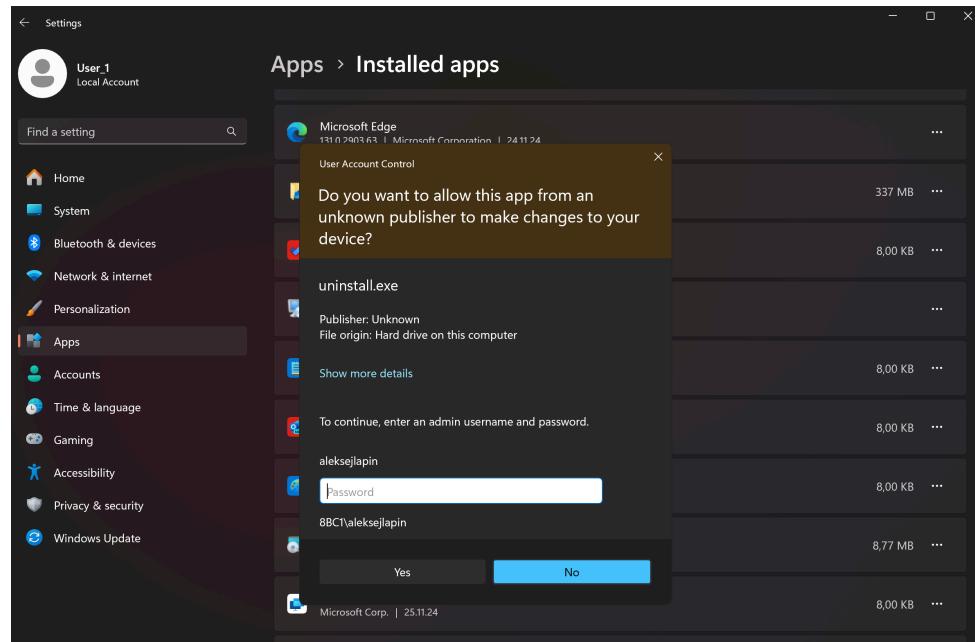


Рис. 24: Удаление приложения, требующего выполнения скриптов

Также, пользователь не может получить доступ к папкам, других пользователей.

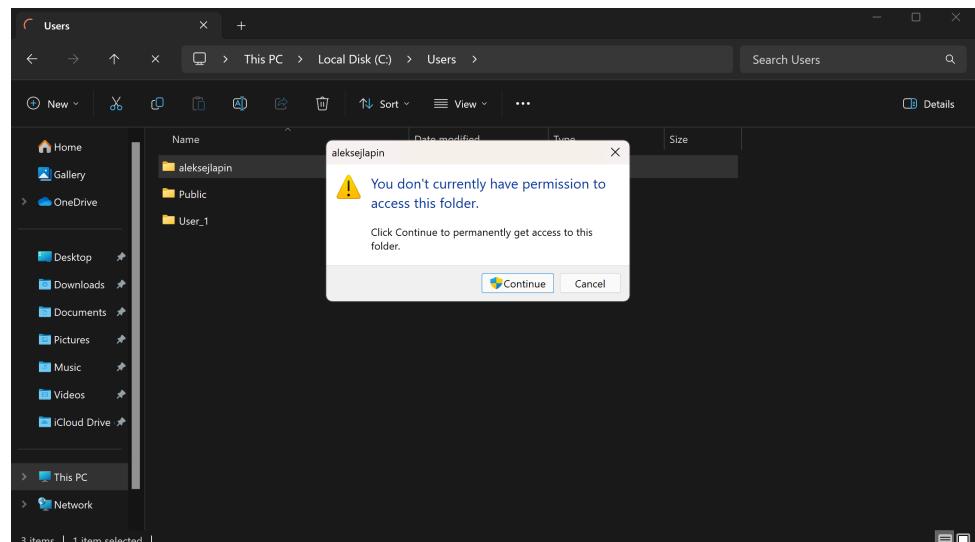


Рис. 25: Доступ к папкам других пользователей

Также, пользователь не может получить доступ к некоторым системным папкам.

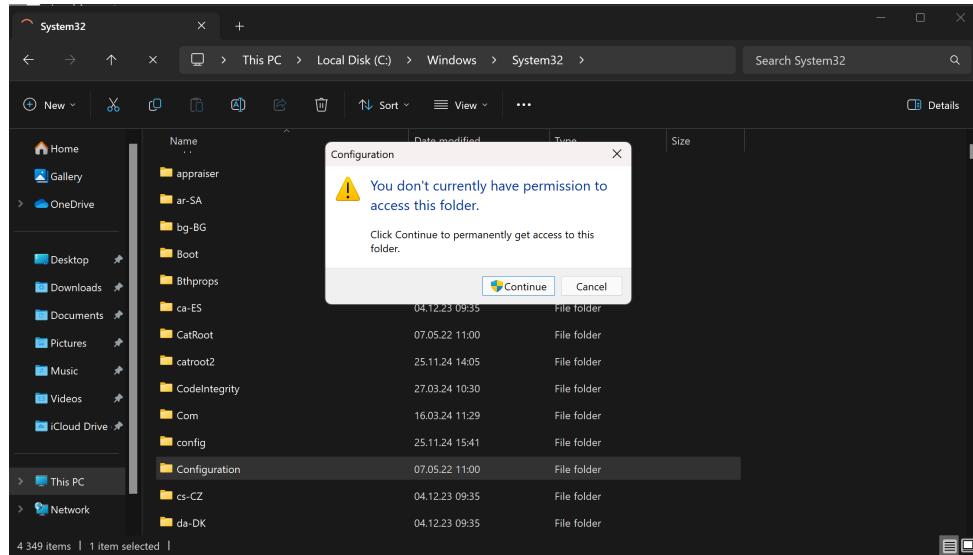


Рис. 26: Доступ к системной папке

### 3 Создание администратора

#### Вариант 1. Создание администратора в Параметрах Windows 11

1. Создадим нового пользователя аналогично варианту 1 из предыдущего пункта.
2. Нажмем правой кнопкой мыши на пользователя и выберем "Изменить учетную запись".
3. Выберем "Администратор".

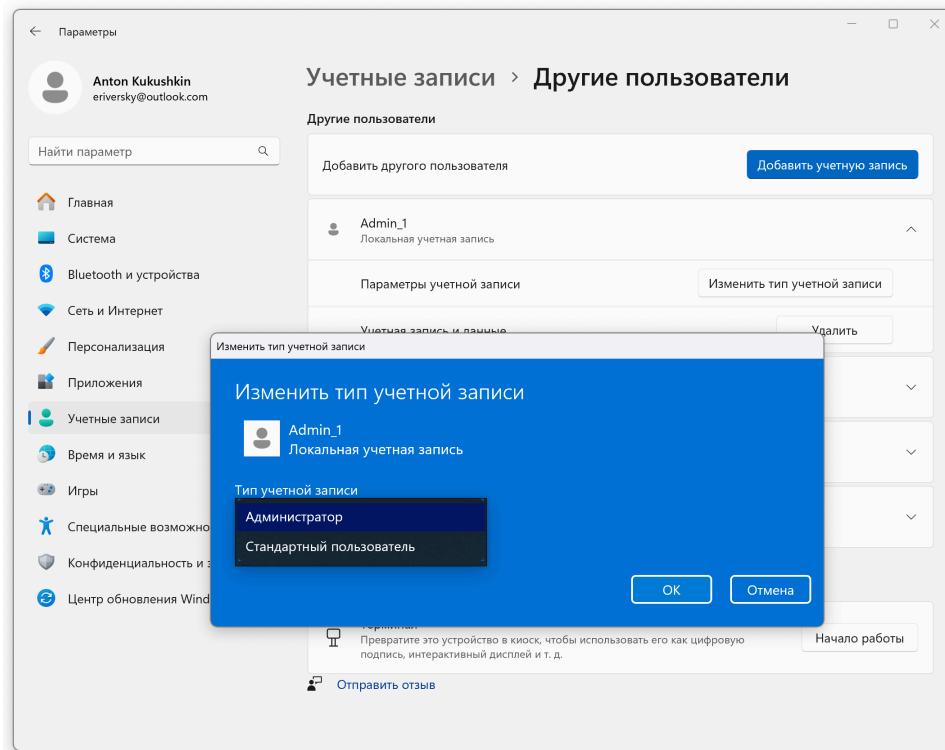


Рис. 27: Создание администратора

#### Вариант 2. Создание администратора в Управлении учетными записями пользователей

1. Создадим нового пользователя аналогично варианту 3 из предыдущего пункта.
2. Переходим в раздел «Группы».
3. Нажмем правой кнопкой мыши на группу «Администраторы» и выберем "Добавить в группу".

4. Выберем «Добавить»

5. Введем имя пользователя и нажмем «OK».

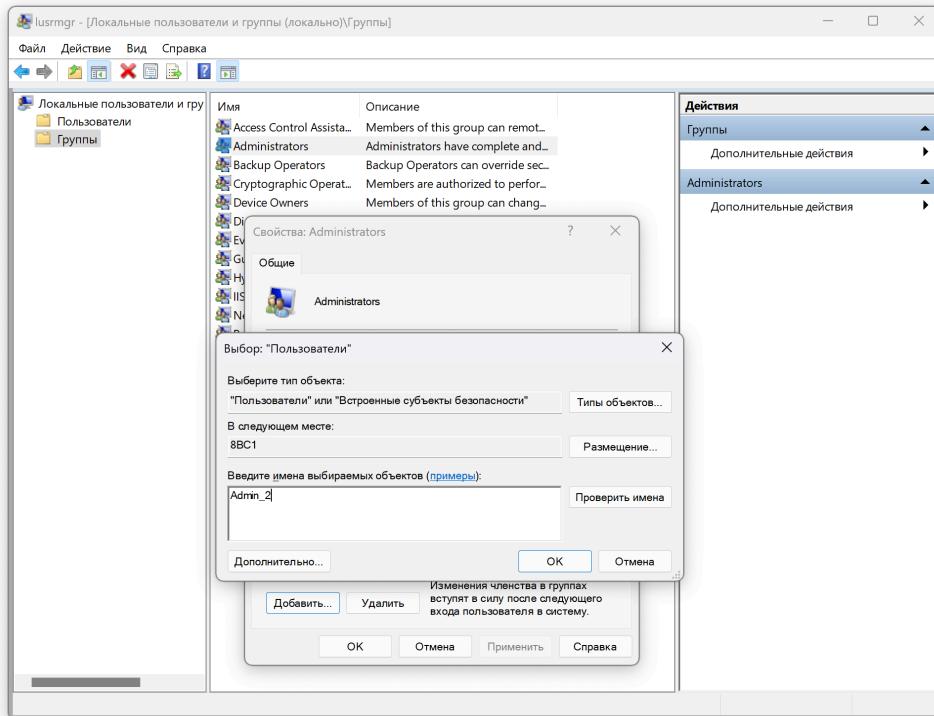


Рис. 28: Создание администратора

### Вариант 3. Создание администратора с помощью командной строки

1. Откроем командную строку от имени администратора.
2. Введем команду `net user <имя пользователя> /add`
3. Введем команду `net localgroup`, чтобы посмотреть доступные группы.
4. Введем команду `net localgroup "Administrators" <имя пользователя> /add`

```
Выбрать Администратор: Командная строка
Microsoft Windows [Version 10.0.22631.3374]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Windows\System32>net user Admin_3 /add
Команда выполнена успешно.

C:\Windows\System32>net localgroup
Псевдонимы для \\8BC1

-----
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Power Users
*Remote Desktop Users
*Remote Management Users
*Replicator
*System Managed Accounts Group
*Users
Команда выполнена успешно.

C:\Windows\System32>net localgroup "Administrators" Admin_3 /add
Команда выполнена успешно.

C:\Windows\System32>
```

Рис. 29: Создание администратора с помощью командной строки

5.

## Ограничения администратора по конфигурации системы

1. Администратор может не может удалять некоторые системные приложения.

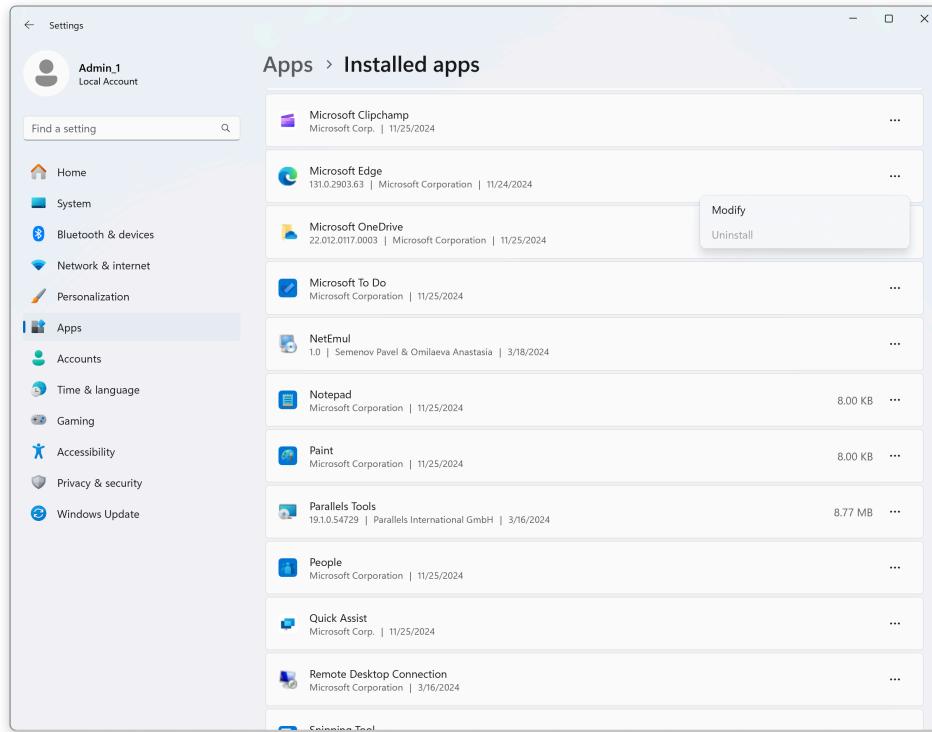


Рис. 30: Удаление «важного» системного приложения

2. Администратор не может удалять встроенные группы. К примеру, группу «Guests».

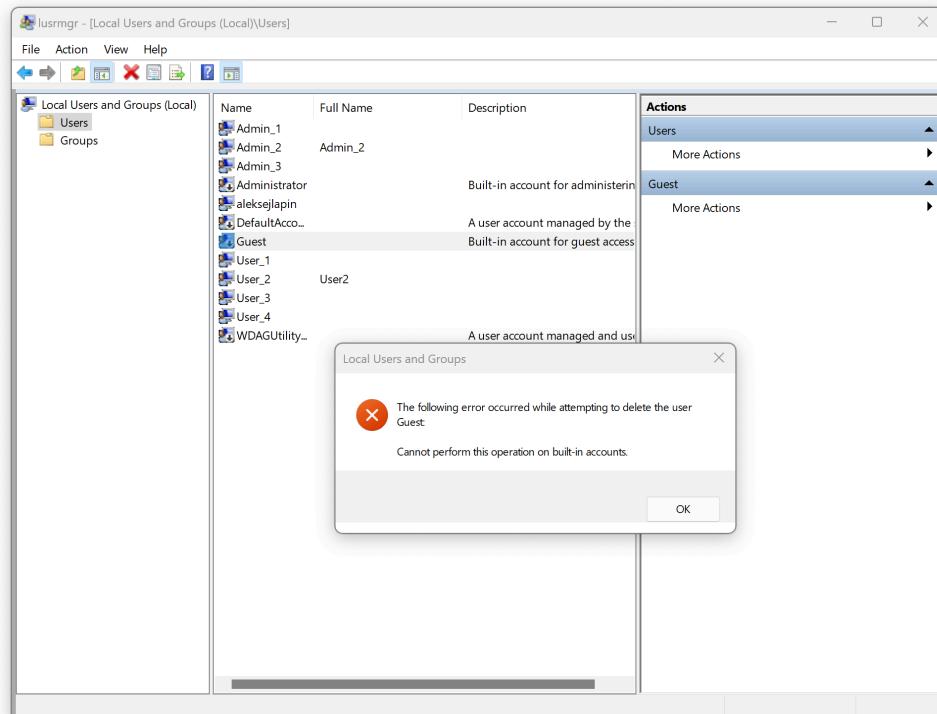


Рис. 31: Удаление встроенной группы

3. Администратор не может получить доступ к важным системным папкам.

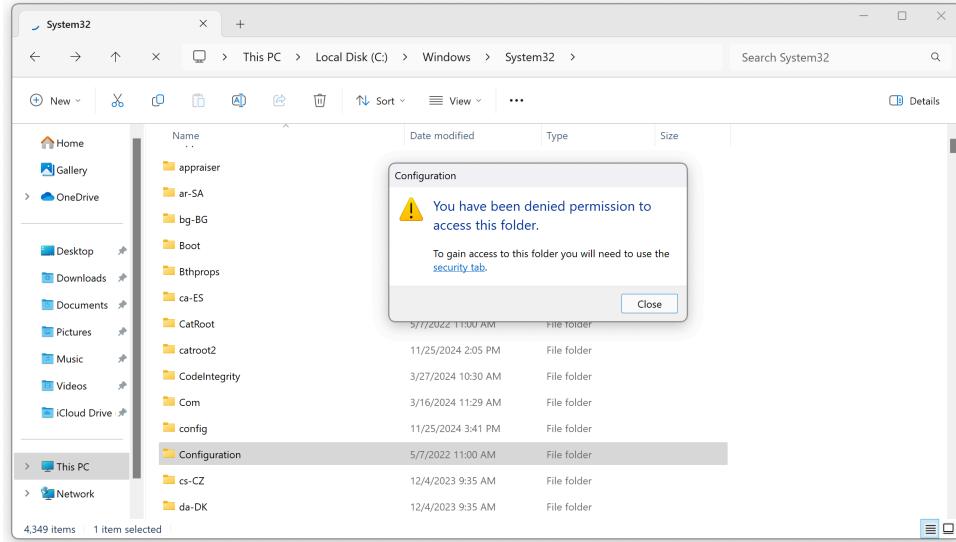


Рис. 32: Доступ к важной системной папке

#### 4. Администратор не может изменять параметры автозапуска некоторых служб.

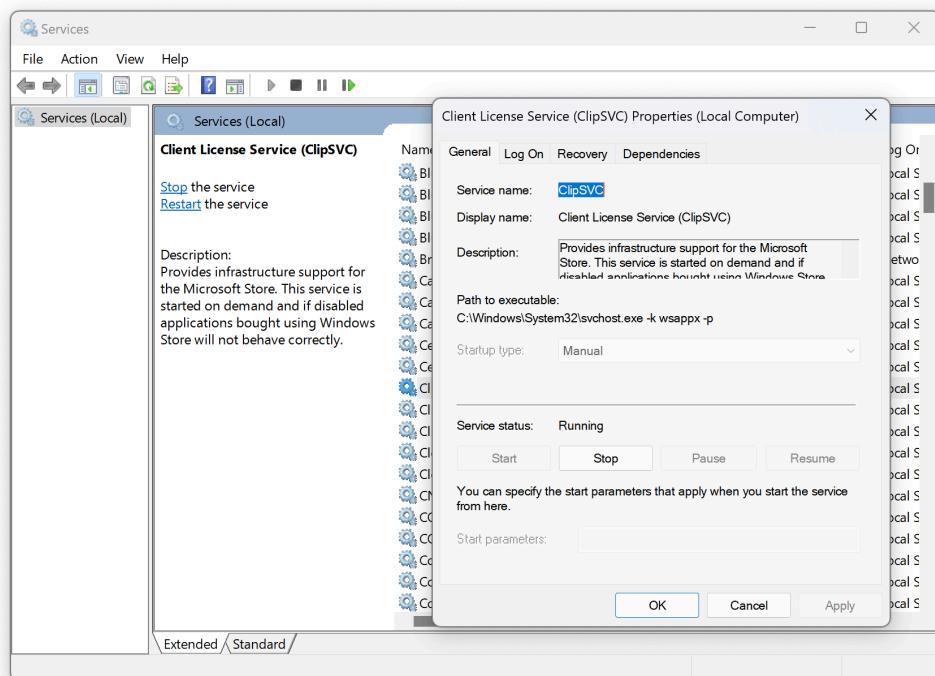


Рис. 33: Изменение параметров автозапуска службы Client License Service

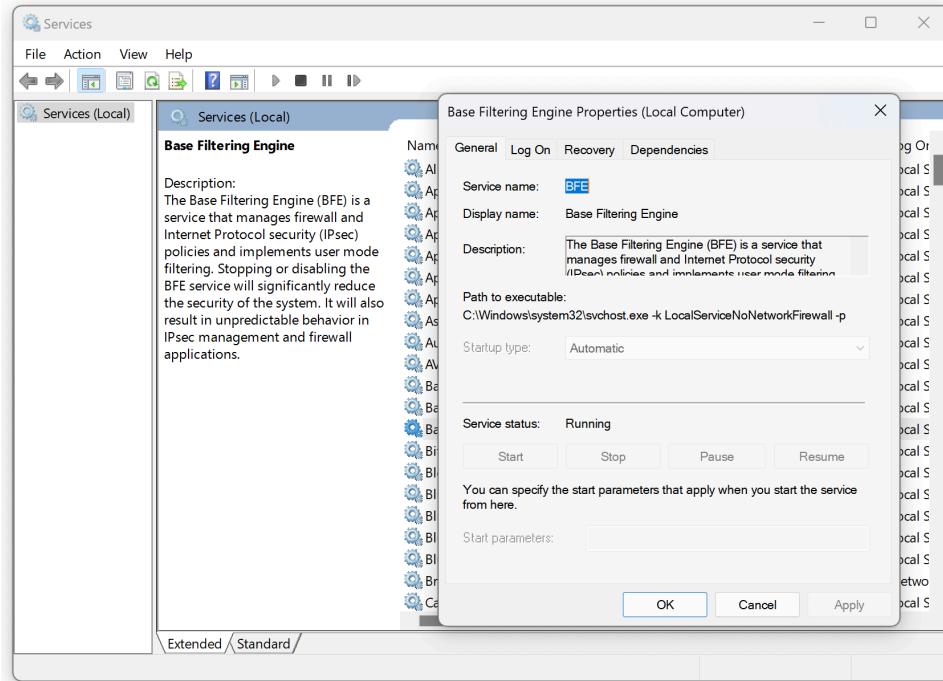


Рис. 34: Изменение параметров автозапуска службы Base Filtering Engine

## 4 Параметры контроля учетных записей пользователей (UAC)

UAC (User Account Control или контроль учетных записей) важный компонент системы защиты Windows. При запуске любого приложения или процесса, который требует прав администратора, пытается изменить системные настройки, ветки реестра или файлы, компонент контроля учетных записей UAC переключает рабочий стол в защищенный режим и запрашивает подтверждение этих действий у администратора. Тем самым UAC позволяет предотвратить запуск процессов и вредоносных программ, которые потенциально могут нанести вред вашему компьютеру.

### Ползунок User Account Control

В Windows 7 (и выше) настройки UAC на компьютере управляются с помощью специального ползунка (вызывается через панель управления или файлом UserAccountControlSettings.exe). С помощью ползунка вы можете выбрать один из четырех предопределенных уровней защиты UAC.

- Всегда уведомлять в следующих случаях
  - Когда приложения пытаются установить программное обеспечение или изменить параметры компьютера
  - Когда я изменяю параметры Windows
- !** Рекомендуется при частой установке нового программного обеспечения и посещении незнакомых веб-сайтов.
- Уведомлять только при попытках приложений внести изменения в компьютер (по умолчанию)
  - Не уведомлять при изменении параметров Windows пользователем
- !** Рекомендуется при использовании знакомых приложений и посещении знакомых веб-сайтов.
- Уведомлять только при попытках приложений внести изменения в компьютер (не затенять рабочий стол)
  - Не уведомлять, когда я изменяю параметры Windows
- !** Не рекомендуется. Выбирайте этот вариант, только если затенение рабочего стола компьютера занимает много времени.

- Не уведомлять меня:
  - Когда приложения пытаются установить программное обеспечение или изменить параметры компьютера
  - Когда я изменяю параметры Windows

 Не рекомендуется.

По умолчанию в Windows 11 выбран 3 уровень защиты UAC, который выводит уведомление только при попытке изменить системные файлы или параметры.

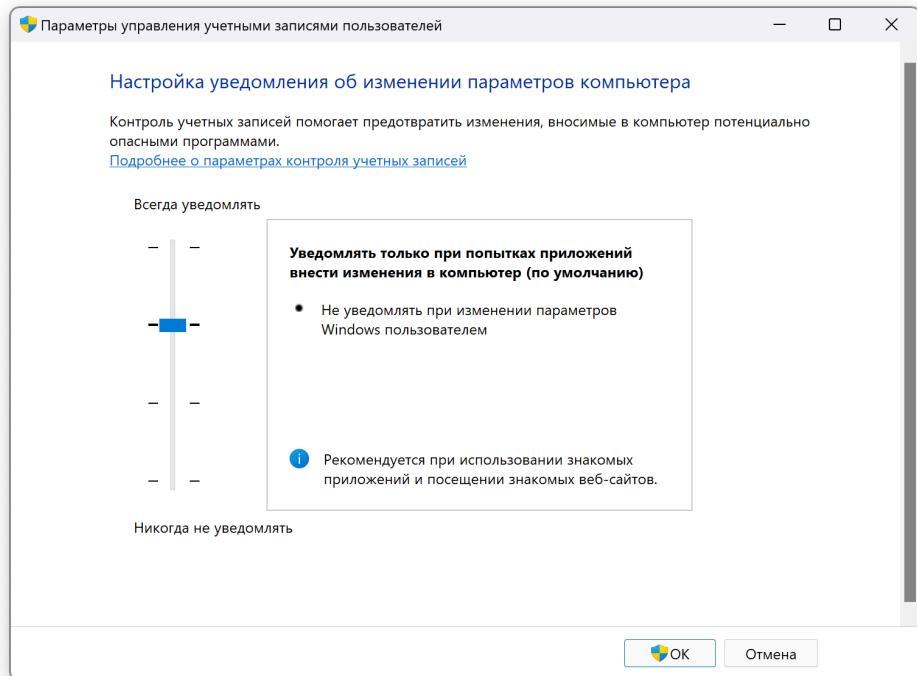


Рис. 35: Уровень защиты UAC

## 5 Выполнить настройки механизмов защиты ОС Windows в соответствии с вариантом

### Вариант 1

Настроить вход пользователя в систему по паролю.

Рассмотреть и реализовать возможные способы усиления парольной защиты.

В процессе создания пользователей был установлен пароль для входа в систему. По умолчанию нет ограничений по сложности пароля.

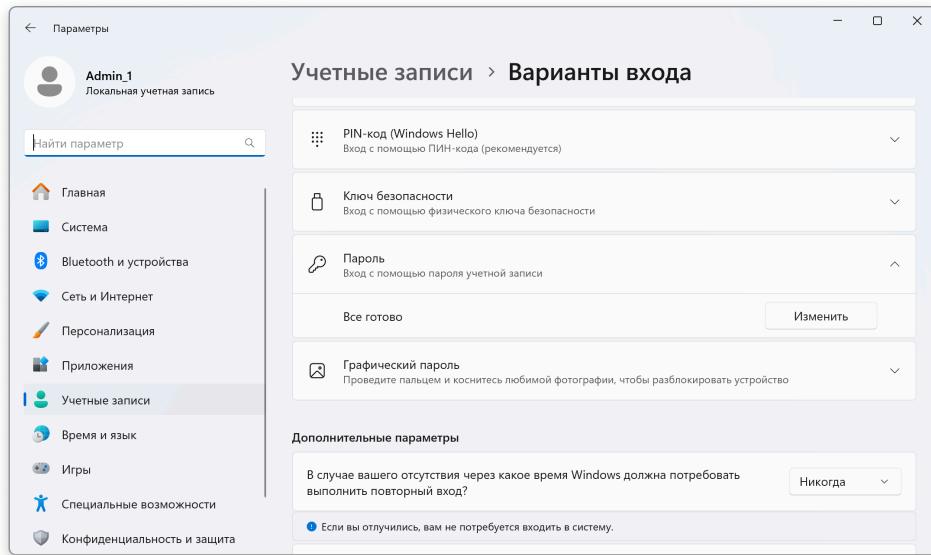


Рис. 36: Пароль пользователя

### **Меры по усилению парольной защиты.**

Для усиления парольной защиты в Windows 11 можно использовать групповые политики безопасности:

1. Открываем редактор локальной групповой политики с помощью команды `gpedit.msc`
2. Переходим в раздел Конфигурация компьютера > Конфигурация Windows > Параметры безопасности > Политики учетных записей > Политика паролей
3. Можем настроить следующие параметры:
  - Аудит минимальной длины пароля
    - Позволяет отслеживать попытки создания паролей короче минимальной длины
    - События записываются в журнал безопасности Windows
    - Помогает выявить пользователей, пытающихся обойти политику безопасности
  - Вести журнал паролей
    - Хранит историю использованных паролей
    - Предотвращает повторное использование старых паролей
    - Повышает безопасность, заставляя создавать новые пароли
  - Максимальный срок действия пароля
    - Определяет период, после которого пароль должен быть изменен
    - Снижает риск компрометации при длительном использовании одного пароля
    - Рекомендуется устанавливать 60-90 дней
  - Минимальная длина пароля
    - Задает минимальное количество символов в пароле
    - Длинные пароли сложнее подобрать
    - Рекомендуется минимум 8-12 символов
  - Минимальный срок действия пароля
    - Определяет период, в течение которого нельзя изменить пароль
    - Предотвращает немедленную смену пароля обратно на старый
    - Усиливает эффективность журнала паролей
  - Ослабить ограничение минимальной длины пароля
    - Позволяет создавать пароли короче установленной минимальной длины

- Не рекомендуется включать
- Используется только в особых случаях для совместимости
- Пароль должен отвечать требованиям сложности
  - Требует использования разных типов символов
  - Увеличивает энтропию пароля
  - Делает пароль более устойчивым к подбору
- Хранить пароли, используя обратимое шифрование
  - Позволяет восстановить исходный пароль
  - Снижает безопасность системы
  - Включается только если требуется протоколами или приложениями

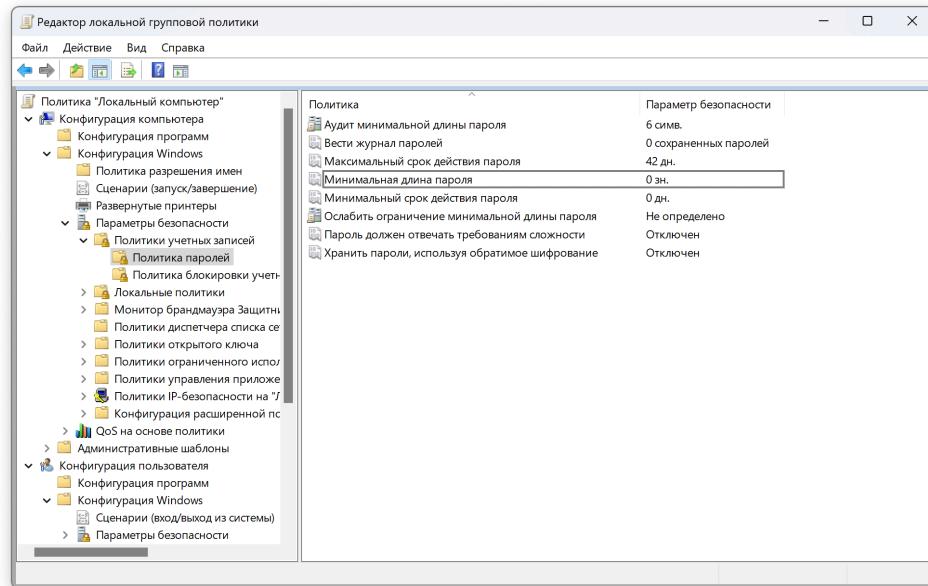


Рис. 37: Политика паролей

## **Меры по усилению парольной защиты с помощью политик блокировки учетной записи в Windows**

11

### **1. Настройка политики блокировки учетных записей:**

- Откройте редактор локальной групповой политики, введя команду `gpedit.msc` в диалоговом окне "Выполнить" (Win + R).
- Перейдите в раздел Конфигурация компьютера > Параметры Windows > Параметры безопасности > Политики учетных записей > Политика блокировки учетных записей.

### **2. Параметры политики блокировки и их назначение:**

- **Время до сброса счетчика блокировки:**
  - Определяет время в минутах до обнуления счетчика неудачных попыток входа
  - Предотвращает атаки перебором, растянутые во времени
  - Позволяет легитимным пользователям повторить попытку входа после периода ожидания
- **Пороговое значение блокировки:**
  - Задает количество неудачных попыток входа до блокировки учетной записи
  - Защищает от автоматизированного подбора паролей
  - Предотвращает атаки методом "грубой силы"
- **Продолжительность блокировки учетной записи:**

- Устанавливает время, на которое блокируется учетная запись
  - Предотвращает немедленные повторные попытки взлома
  - Дает время администраторам для реагирования на подозрительную активность
- **Разрешить блокировку учетной записи администратора:**
    - Определяет, применяются ли правила блокировки к учетной записи администратора
    - Повышает безопасность, но может создать риск полной блокировки системы
    - Требует наличия резервной административной учетной записи

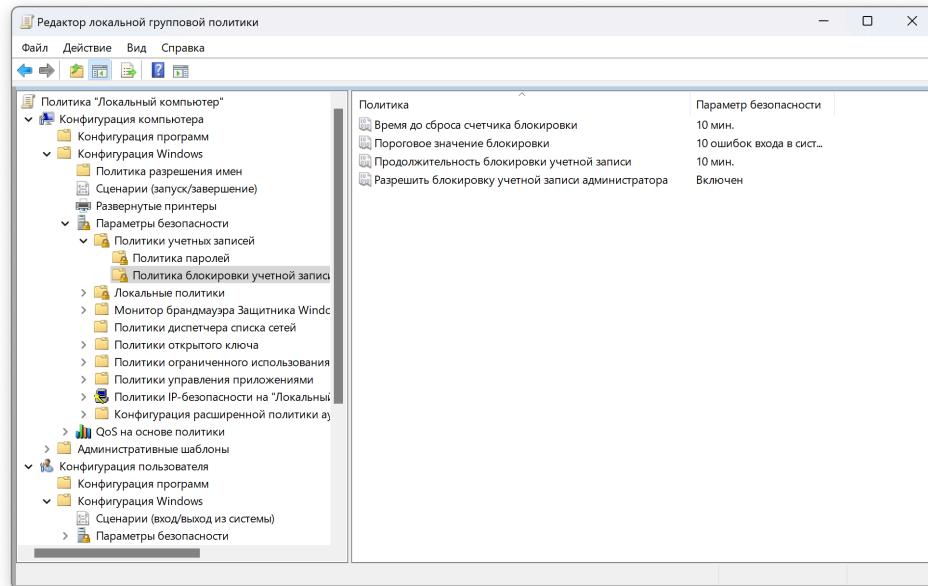


Рис. 38: Политика блокировки учетных записей

### Меры по усилению парольной защиты с помощью команды Net Accounts

Команда Net Accounts используется для задания параметров политики на локальном компьютере, таких как политики учетных записей и политики паролей.

1. Откроем командную строку от имени администратора.
2. Введем команду `net accounts`
3. Вы увидите параметры политики блокировки учетных записей по умолчанию и политики паролей на локальном компьютере, как показано ниже.

```
C:\Windows\System32>net accounts
Приударительный выход по истечении времени через: Никогда
Минимальный срок действия пароля (дней): 0
Максимальный срок действия пароля (дней): 42
Минимальная длина пароля: 0
Хранение неповторяющихся паролей: Нет
Блокировка после ошибок ввода пароля: 10
Длительность блокировки (минут): 10
Сброс счетчика блокировок через (минут): 10
Роль компьютера: РАБОЧАЯ СТАНЦИЯ
Команда выполнена успешно.

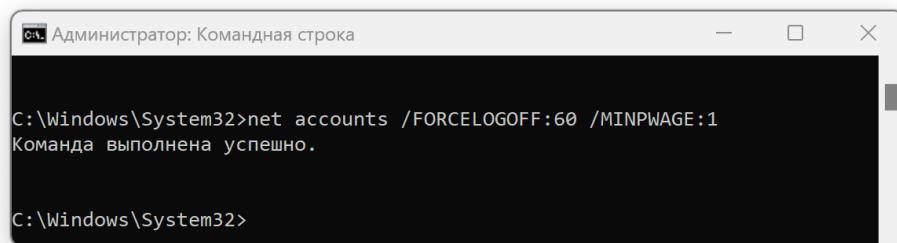
C:\Windows\System32>
```

Рис. 39: Параметры политики блокировки учетных записей и паролей

4. Приведенные выше параметры отображаются в качестве роли компьютера. Если компьютер присоединен к домену, параметры домена вступают в силу, и будут отображаться только параметры, поступающие из домена. Остальные параметры будут локальными параметрами, если он не поступает из объекта групповой политики домена.

5. Вы можете изменить следующие параметры в параметрах Net Accounts:

- **/FORCELOGOFF:minutes | NO**: Задает количество минут, когда срок действия учетной записи истекает или истекает срок действия допустимого срока входа. Нет, значение по умолчанию предотвращает принудительный выход.
- **/MINPWLEN:length**: Задает минимальное количество символов для пароля. Диапазон равен 0–14 символам; Значение по умолчанию — шесть символов.
- **/MAXPWAGE:days | UNLIMITED**: Задает максимальное количество дней, в течение которых пароль действителен. Ограничение не указано с помощью UNLIMITED. Значение /MAXPWAGE не может быть меньше /MINPWAGE. Диапазон равен 1–999; Значение по умолчанию — 90 дней.
- **/MINPWAGE:days**: Задает минимальное количество дней, которые должны пройти, прежде чем пользователь сможет изменить пароль. Значение нуля не задает минимальное время. Диапазон равен 0–999; значение по умолчанию равно нулю дней. /MINPWAGE не может быть больше /MAXPWAGE.
- **/UNIQUEPW:number**: Задает количество уникальных паролей, которые должны быть использованы перед повторным использованием одного и того же пароля. Максимальное значение равно 24.
- **/DOMAIN**: Выполняет операцию на контроллере домена текущего домена. В противном случае операция выполняется на локальном компьютере.
- **net help accounts**: Отображение справки для указанной команды net.



```
C:\Windows\System32>net accounts /FORCELOGOFF:60 /MINPWAGE:1
Команда выполнена успешно.

C:\Windows\System32>
```

Рис. 40: Пример команды Net Accounts

Мои действия по настройке механизма защиты, включающие установку пароля для пользователя, не соответствуют ряду требований, указанных в руководящих документах. В частности, они не удовлетворяют требованиям «Очистка памяти», «Дискреционный принцип контроля доступа» и «Руководство для пользователя». Это связано с тем, что функциональность, о которой идёт речь, относится непосредственно к операционной системе Windows 10. Настройка входа по паролю направлена на выполнение требований идентификации и аутентификации.

## 6 Анализ реализации механизма защиты в ОС Windows

С апреля 2022 года ФСТЭК приостановил действие сертификатов на все программное обеспечение Microsoft (как и многих других иностранных вендоров). До этого момента, последняя версия Windows, которая имела сертификат ФСТЭК, была Windows 10. 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). 6 это минимальный уровень доверия к системе. Средства,

соответствующие 6 уровню доверия, применяются в значимых объектах критической информационной инфраструктуры 3 категории, в государственных информационных системах 3 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровня защищенности персональных данных. Что говорит о том, что Windows 10 не может быть использован для большинства критических объектов, но подходит для использования на персональных компьютерах, без критических данных.

## **6.1 Анализ соответствия механизма защиты ОС Windows 11 классу защищенности 1Г**

В соответствии с положениями руководящего документа «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.», операционная система Windows 11 относится к классу систем 1Г.

### **Соответствие подсистемы управления доступом**

#### **1. Идентификация и проверка подлинности субъектов доступа:**

- Windows 11 поддерживает идентификацию пользователей через уникальные идентификаторы (логины) и пароли, соответствующие требованиям длины не менее шести буквенно-цифровых символов. Кроме того, поддерживаются многофакторная аутентификация (MFA) для усиления безопасности.

#### **2. Идентификация терминалов, ЭВМ и других объектов по логическим именам:**

- В Windows 11 каждый терминал и устройство в сети могут быть идентифицированы по уникальным именам (например, NetBIOS или DNS имена), что соответствует требованиям класса 1Г.

#### **3. Идентификация программ и файлов по именам:**

- Операционная система обеспечивает идентификацию программ, томов, каталогов, файлов и других объектов по их именам через файловую систему NTFS и механизмы разрешений.

#### **4. Контроль доступа в соответствии с матрицей доступа:**

- Windows 11 использует контроль доступа на основе списков контроля доступа (ACL), которые позволяют управлять правами доступа субъектов к различным ресурсам системы. Это позволяет реализовать матрицу доступа, определяющую права каждого пользователя.

### **Соответствие подсистемы регистрации и учета**

#### **1. Регистрация входа и выхода субъектов доступа:**

- Windows 11 ведет журналы безопасности (Security Logs) через журнал событий Windows, регистрируя успешные и неуспешные попытки входа пользователей, а также загрузку и останов системы.

#### **2. Регистрация выдачи печатных документов:**

- Система может регистрировать события печати через журналы событий, фиксируя дату, время, устройство вывода и пользователя, инициировавшего печать.

#### **3. Регистрация запуска и завершения программ и процессов:**

- Windows 11 регистрирует запуск и завершение процессов через журнал событий, включая информацию о времени, имени процесса и пользователе, инициировавшем действие.

#### **4. Регистрация попыток доступа к защищаемым файлам и объектам:**

- Система фиксирует попытки доступа к файлам и другим объектам в журнале безопасности, включая результат попытки, идентификатор пользователя и спецификацию объекта.

##### **5. Учет защищаемых носителей информации:**

- Windows 11 поддерживает шифрование данных на накопителях (BitLocker).

##### **6. Очистка освобождаемых областей памяти:**

- Операционная система обеспечивает базовую очистку оперативной памяти при закрытии процессов. Однако для выполнения требований класса 1Г, связанных с очисткой и перезаписью данных, могут потребоваться специализированные программные средства.

#### **Соответствие подсистемы обеспечения целостности**

##### **1. Целостность программных средств СЗИ НСД:**

- Windows 11 использует цифровые подписи и проверки целостности системных файлов через механизмы защиты, такие как Windows Defender и механизмы Secure Boot, что способствует обеспечению целостности системных компонентов.

##### **2. Трансляция программной среды:**

- Использование современных компиляторов и защищенных сред разработки помогает поддерживать неизменность объектного кода программ при обработке и хранении защищаемой информации.

##### **3. Физическая охрана СВТ:**

- Физическая безопасность устройств и носителей информации зависит от инфраструктуры организации. Windows 11 предоставляет инструменты для управления доступом, но физическая охрана реализуется на уровне организации.

##### **4. Периодическое тестирование функций СЗИ НСД:**

- Windows 11 регулярно получает обновления безопасности и рекомендации по тестированию через Microsoft Security Compliance Toolkit. Однако организациям необходимо самостоятельно проводить тестирования с использованием специализированных тестовых программ.

##### **5. Средства восстановления СЗИ НСД:**

- Операционная система поддерживает функции восстановления и резервного копирования, однако для выполнения требований класса 1Г по ведению двух копий программных средств необходимо использовать дополнительные решения для резервного копирования и восстановления.

##### **6. Использование сертифицированных средств защиты:**

- Windows 11 сертифицирована по различным стандартам безопасности, включая FIPS 140-2 для криптографических модулей. Однако, для выполнения требований класса 1Г, связанных с использованием сертифицированных средств защиты, могут потребоваться специализированные программные средства сертифицированные ФСТЭК.

#### **Вывод**

Windows 11 обладает множеством встроенных функций безопасности, позволяющих удовлетворить основные требования класса защищенности 1Г, такие как идентификация и аутентификация пользователей, контроль доступа, регистрация событий безопасности и обеспечение целостности системных компонентов. Однако некоторые специфические требования класса 1Г, например, очистка с перезаписью оперативной памяти, требуют дополнительной настройки или использования специализированного программного обеспечения. В целом, при правильной конфигурации и применении дополнительных мер, Windows 11 может

соответствовать требованиям класса защищенности 1Г для использования в менее критических информационных системах. Отсутствие автоматической маркировки печатных документов и многократной очистки оперативной памяти и других требований не позволяет отнести Windows 11 к более высокому классу защищенности.

## 6.2 Анализ соответствия защиты Windows 11 классу защищенности 6

В соответствии с руководящим документом «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», Windows 11 относится к шестому классу защиты.

В данном разделе рассматривается соответствие защиты операционной системы Windows 11 требованиям класса защищенности 6, исходя из установленных критериев.

### Дискреционный принцип контроля доступа (ПРД)

#### Требования класса 6:

- Контролировать доступ именованных субъектов к именованным объектам с явным перечислением допустимых типов доступа
- Механизм обеспечения дискреционных правил разграничения доступа
- Возможность санкционированного изменения ПРД

**Анализ:** Windows 11 реализует дискреционный контроль доступа через систему разрешений файловой системы NTFS, позволяющую управлять доступом пользователей и групп к файлам и папкам. Пользователи могут назначать права чтения, записи, выполнения и изменения для различных объектов. Также доступно управление списками контроля доступа (ACL), что соответствует требованию явного перечисления допустимых типов доступа.

Возможность санкционированного изменения ПРД ограничена правами администраторов, что соответствует требованиям класса 6.

### Идентификация и аутентификация

#### Требования класса 6:

- Требование идентификации пользователей при запросах доступа
- Аутентификация подлинности идентификации
- Хранение необходимых данных для идентификации и аутентификации
- Препятствование доступу неидентифицированных или неаутентифицированных пользователей

**Анализ:** Windows 11 поддерживает различные методы аутентификации, включая:

- Пароли
- PIN-коды
- Биометрические данные (Windows Hello)
- Многофакторная аутентификация

Система проверяет подлинность учетных данных перед предоставлением доступа к защищаемым ресурсам. Реализованы механизмы блокировки учетной записи после нескольких неудачных попыток входа, что предотвращает неавторизованный доступ.

## **Тестирование**

### **Требования класса 6:**

- Тестирование реализации дискреционных ПРД
- Тестирование механизмов идентификации и аутентификации

**Анализ:** Microsoft регулярно проводит внутренние и внешние аудиты безопасности Windows 11, включая тестирование механизмов контроля доступа и аутентификации. Система также проходит программы Bug Bounty, позволяющие выявлять и устранять уязвимости.

## **Документация**

### **Требования класса 6:**

- Руководство для пользователя
- Руководство по КСЗ (Контроль системы защиты)

**Анализ:** Windows 11 поставляется с обширной документацией для пользователей, включая справочные материалы и руководства по использованию встроенных средств безопасности. Для администраторов доступны специальные руководства по настройке и управлению средствами безопасности, таким как Group Policy, BitLocker и другими инструментами.

## **Тестовая и проектная документация**

### **Требования класса 6:**

- Описание тестов и результатов тестирования
- Конструкторская (проектная) документация, включая общую схему КСЗ и описание механизмов идентификации и аутентификации

**Анализ:** Конкретные детали тестовой и проектной документации Windows 11 недоступны для общественности, однако Microsoft предоставляет общую информацию о архитектуре безопасности и реализованных механизмах через официальные документы и технические статьи.

## **6.3 Заключение**

Windows 11 обладает многими характеристиками, соответствующими требованиям класса защищенности 6:

- **Дискреционный контроль доступа** реализован через гибкую систему разрешений и ACL
- **Идентификация и аутентификация** обеспечиваются современными методами, включая многофакторную аутентификацию
- **Тестирование** проводится регулярно с участием как внутренних, так и внешних экспертов
- **Документация** доступна как для пользователей, так и для администраторов

Однако необходимо учитывать, что соответствие конкретным стандартам класса защищенности 6 может требовать дополнительных настроек и конфигураций, а также соблюдения организационных процессов безопасности, которые выходят за рамки возможностей самой операционной системы.

## 6.4 Ключевые выводы

- **Сильные стороны Windows 11:** Гибкая система контроля доступа, поддержка современных методов аутентификации, регулярное тестирование безопасности и наличие обширной документации
- **Возможные области улучшения:** Специальные настройки и дополнительные меры безопасности могут потребоваться для полного соответствия специфическим требованиям класса защищенности 6

Таким образом, **защита Windows 11 частично соответствует классу защищенности 6**, однако окончательное соответствие зависит от конкретных требований и условий эксплуатации, а также от дополнительных мер по настройке и управлению безопасностью.

## 7 Анализ результатов выполнения лабораторной работы

В ходе выполнения лабораторной работы были достигнуты поставленные цели, связанные с изучением и применением методов управления учетными записями пользователей и настройками безопасности в операционной системе Windows 11.

### 7.1 Создание пользователей и администраторов

Были рассмотрены и реализованы различные методы создания пользователей, включая использование графического интерфейса через Параметры Windows, Панель управления, командную строку и PowerShell. Это позволило освоить гибкость инструментов Windows для управления учетными записями и выбрать наиболее удобный способ в зависимости от конкретных задач.

### 7.2 Усиление парольной защиты

Настройки политик паролей и блокировки учетных записей продемонстрировали важность комплексного подхода к обеспечению безопасности. Применение групповых политик и командных утилит позволило настроить параметры сложности паролей, сроки их действия и механизмы блокировки, что существенно повышает защиту системы от несанкционированного доступа.

### 7.3 Настройка контроля учетных записей пользователей (UAC)

Изучение и настройка UAC обеспечили понимание механизмов защиты Windows от запуска потенциально вредоносных приложений и изменений системных настроек без явного разрешения администратора. Регулировка уровней уведомлений позволила сбалансировать безопасность и удобство использования системы.

### 7.4 Анализ соответствия механизма защиты ОС Windows

Проведенный анализ показал, что Windows 11 обладает значительными возможностями для обеспечения безопасности, включая гибкую систему контроля доступа, поддержку многофакторной аутентификации и регулярные обновления безопасности. Однако, для полного соответствия высоким классам защищенности, требуется дополнительная настройка и использование специализированных средств защиты.

### 7.5 Заключение

Лабораторная работа позволила на практике изучить и применить механизмы управления учетными записями и настройками безопасности в ОС Windows 11. Полученные результаты демонстрируют эффективность встроенных инструментов для обеспечения безопасности системы, а также подчеркивают необходимость комплексного подхода и дополнительной настройки для соответствия высоким стандартам защищенности.