Администрирование Windows

1. Краткая теоретическая информация

В операционной системе Windows 10 существует 2 группы пользователей:

- *локальные учетные записи;*

- *учетные записи Microsoft.*

Первая группа называется локальной, потому что аутентификация происходит на локальном компьютере. Все необходимые для этого учетные данные (имя пользователя, пароль и настройки учетной записи) хранятся в нем.

При работе с учетной записью Microsoft аутентификация пользователя происходит на сетевом сервере, то есть удаленно. Преимущество этого метода в том, что любой сотрудник предприятия может получить доступ к сети с любого компьютера, а не только с того, который ему выделен. Сервер хранит все параметры пользователя, а также, при необходимости, документы, с которыми работает пользователь. Однако второй тип пользователя имеет свой недостаток — если нет подключения к Интернету или модемного соединения (не установлено автоматически), аутентификация будет невозможна.

Локальные учетные записи бывают трех типов:

- *учетная запись администратора*, созданная во время установки системы и используемая при изменении настроек системы;

- *пользовательская учетная запись*, позволяющая использовать программы, установленные администратором из внешних источников, и изменять настройки персонализации;

- гостевой учетной записи.

Microsoft Management Console (MMC) — это компонент операционных систем семейства Windows, предоставляющий администраторам графический интерфейс для настройки системных приложений и прикладных программ.

Snap-in — это компонент для MMC, который включает набор параметров для любого модуля операционной системы (файловая система, управление пользователями и т. д.) или приложения.

Набор параметров для прикладных программ может быть добавлен в snap-in с помощью административных шаблонов — специально структурированных файлов с расширением *.adm.

Групповая политика — это набор правил или настроек, в соответствии с которыми настраивается операционная среда Windows.

1.1. Управление локальными учетными записями пользователей

Рассмотрим механизм работы с учетными записями пользователей, предлагаемый Windows 10. Для этого через меню «Пуск» перейдите в настройки системы (рис. 1).

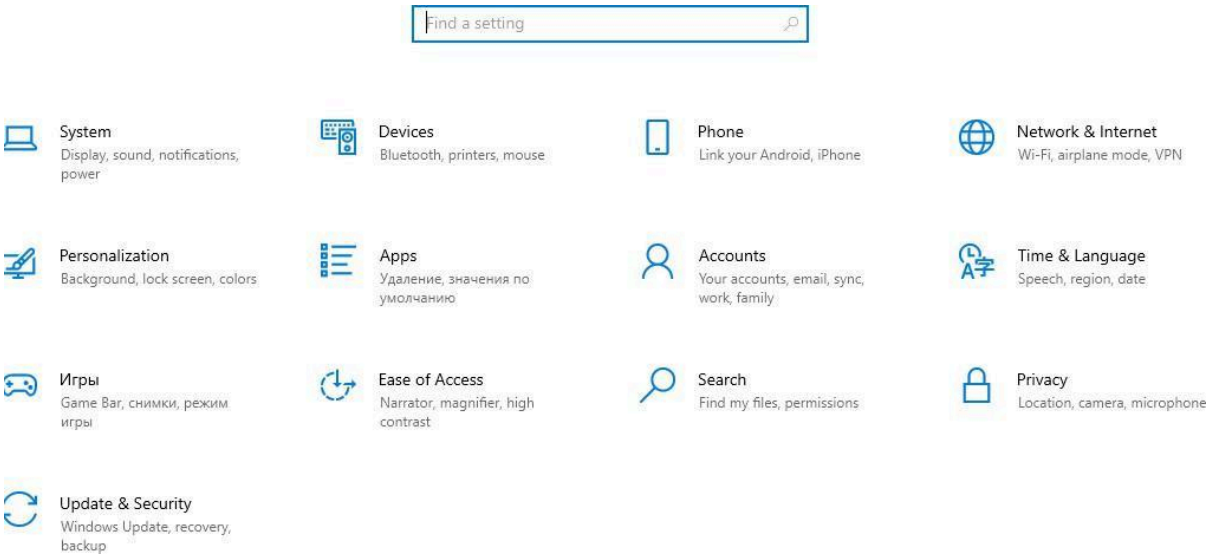


Рис. 1. Настройки Windows

Перейдите в раздел «Учетные записи». В этом разделе будет представлена информация о том, какая учетная запись была использована для аутентификации, будут представлены функции для изменения параметров входа, будут представлены учетные записи на этом компьютере (если они есть) и будет предложено создание новых пользователей (рис. 2).

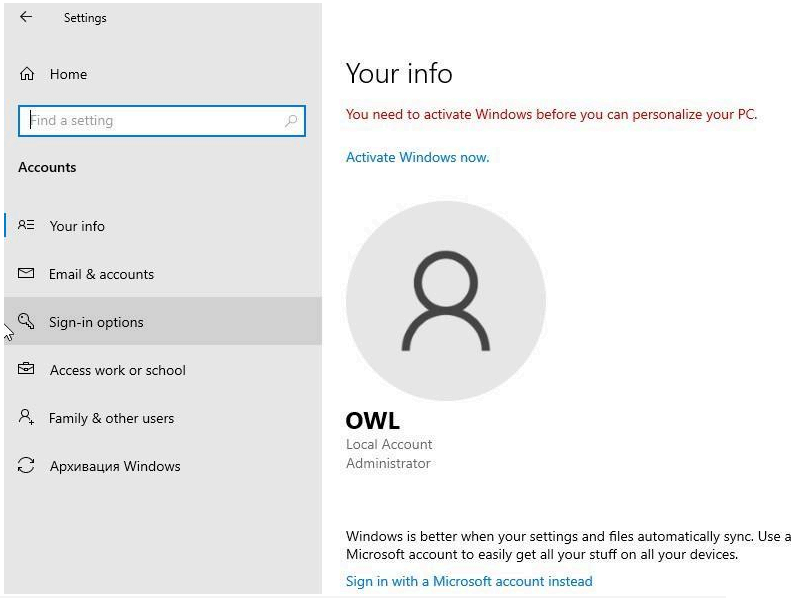


Рис. 2. Вкладка управления пользователями.

Перейдите на вкладку «Семья и другие люди», нажмите «Добавить нового пользователя для этого компьютера». В результате вам будет предложено ввести адрес электронной почты или номер телефона для авторизации. Чтобы добавить локального пользователя, нажмите «У меня нет данных об этом человеке» (рис. 3).

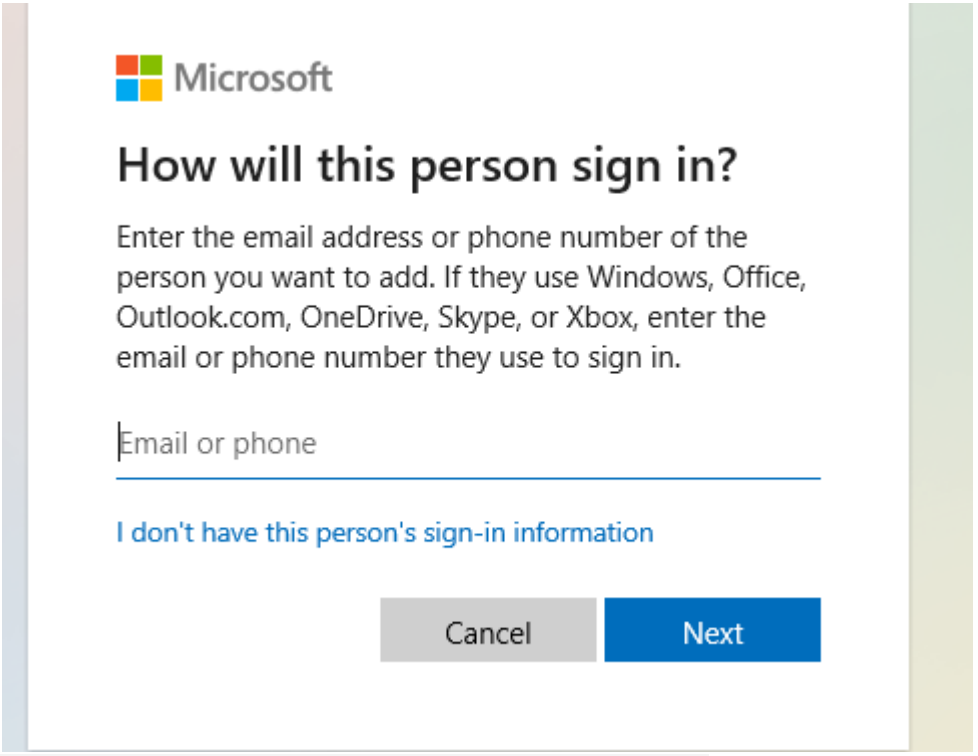


Рис. 3. Выбор метода подключения

Затем нажмите на надпись: «Добавить пользователя без учетной записи» (рис. 4).

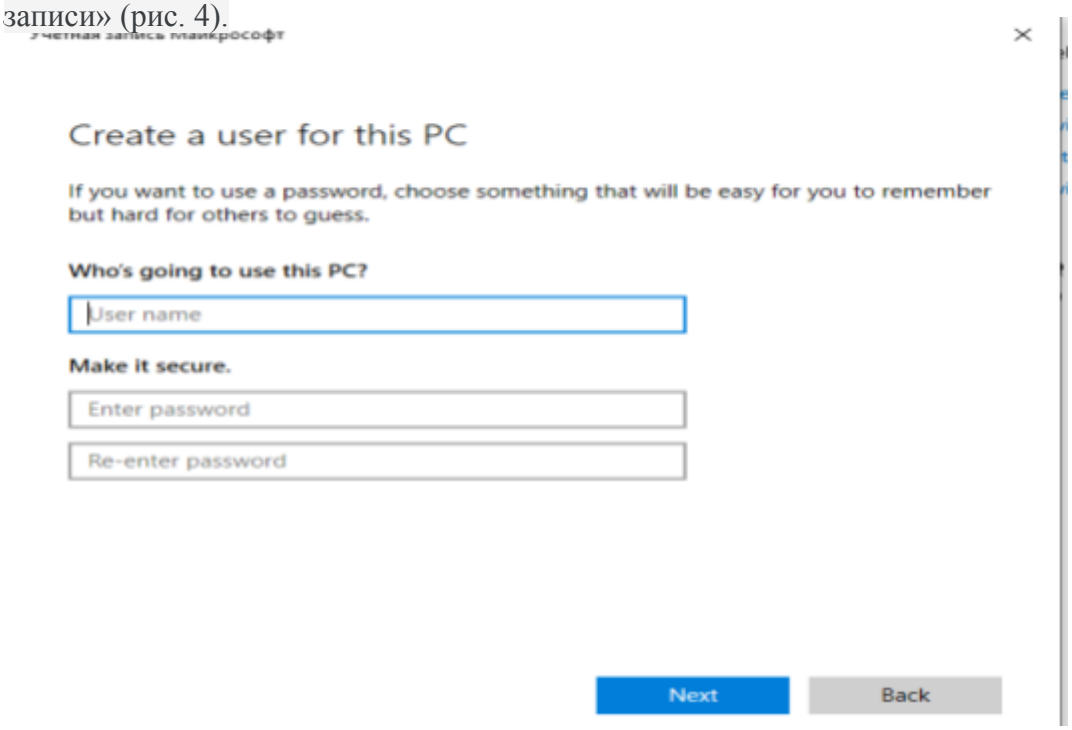


Рис. 4. Добавление локального пользователя

После этого вам нужно будет установить имя пользователя и пароль для него, а также подсказку для пароля. После завершения создания пользователя соответствующая запись появится в списке учетных записей на этом компьютере.

Запустите Microsoft Management Console (MMC), компонент Windows, который позволяет управлять системой. Откройте меню «Пуск → Выполнить → mmc». Чтобы добавить необходимый набор оснавок, выберите «Файл → Добавить или удалить оснавки» в меню консоли. В результате будет предложен список, из которого пользователь может выбрать один или несколько snap-in.

Нажмите «Файл» и перейдите в «Параметры». Здесь можно выбрать режим пользователя для работы с этой консолью: режим автора, который предоставляет пользователю полный доступ ко всем функциям MMC, и режим пользователя.

Существует три типа пользовательского режима:

- *полный доступ (full access)* предоставляет пользователю доступ ко всем командам MMC, но не позволяет добавлять или удалять оснастки или изменять свойства консоли;

- ограниченный доступ, несколько окон (Limited Access Multiple Windows) позволяет пользователю получать доступ только к тем областям дерева консоли, которые были отображены при сохранении консоли, а также открывать новые окна;

- ограниченный доступ, одно окно (Limited Access Single Window) работает так же, как ограниченный доступ с несколькими окнами, с той разницей, что пользователь не может открывать новые окна. Сохраните консоль в режимах «автор» и «пользователь» (рис. 5). Определите различия в работе консоли в разных режимах.

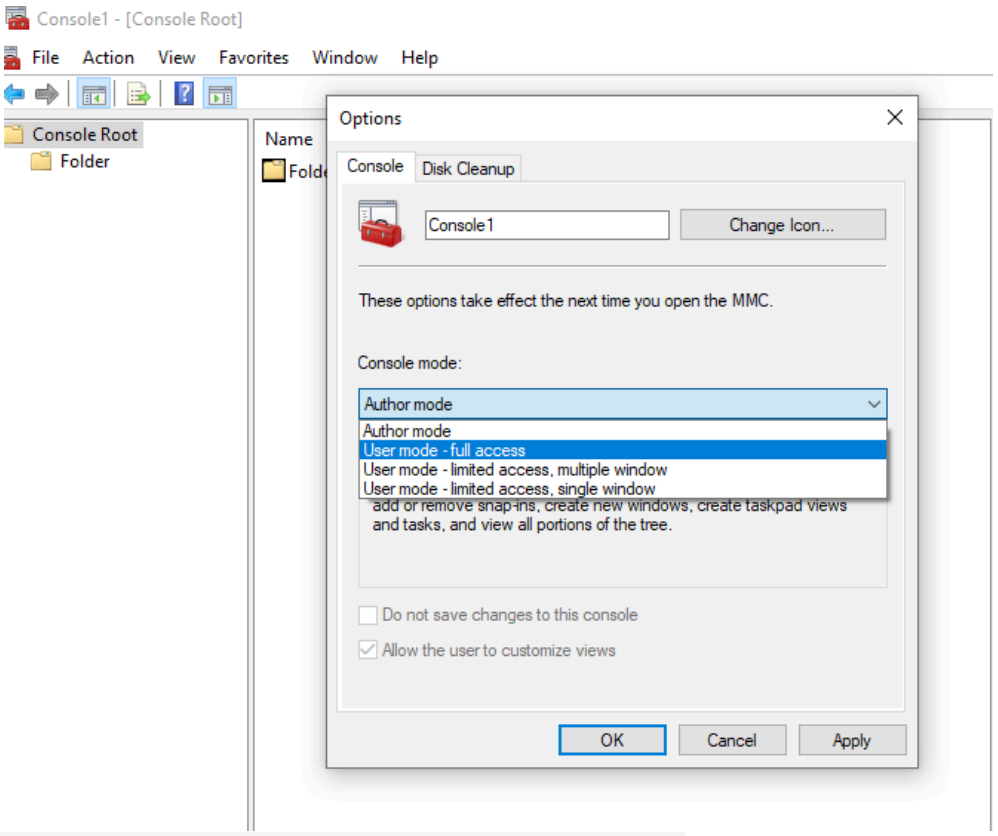


Рис. 5. Параметры режима консоли

С помощью элемента «Добавить или удалить оснастку» добавьте «Локальные пользователи и группы» (рис. 6).

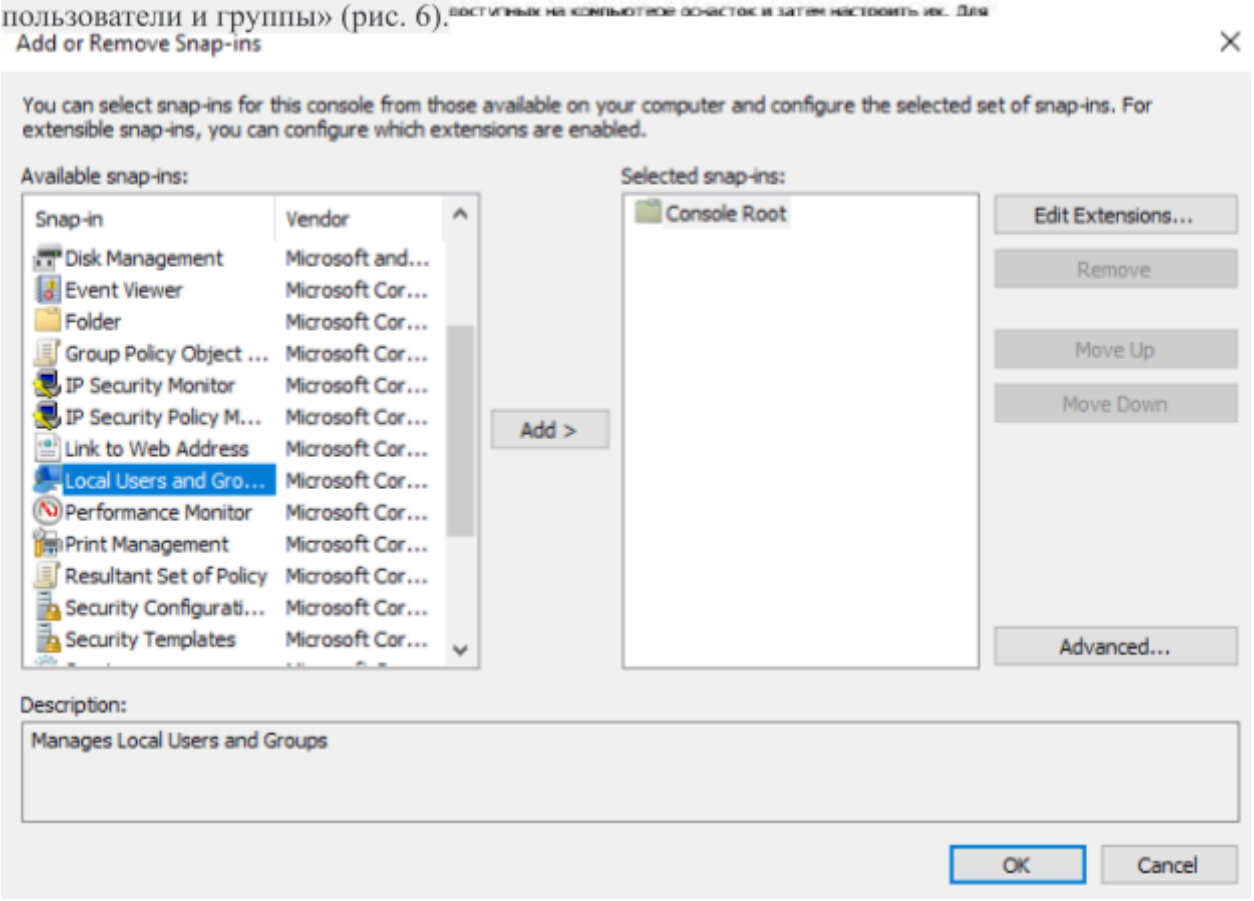


Рис. 6. Добавление оснастки

С помощью этого оснастки также можно добавить нового пользователя (рис. 7).

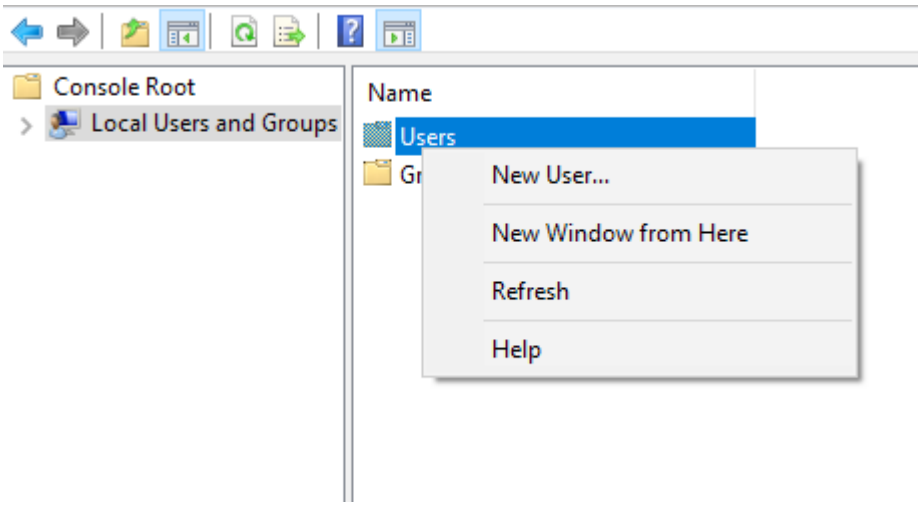


Рис. 7. Добавление пользователя через оснастку

В появившемся окне (рис. 8) введите имя учетной записи, а также пароль и его подтверждение. Если администратор устанавливает временный пароль для пользователя, то для запроса смены пароля необходимо активировать опцию «Запросить смену пароля при следующем входе в систему». Сразу после успешной аутентификации пользователь получает запрос на смену пароля, в ответ на который необходимо установить новый пароль. Этот

подход следует использовать в тех случаях, когда системный администратор не должен знать пароли пользователей.

Если пользователь забыл свой пароль, член группы «Администраторы» может сбросить его старый пароль с помощью функции «Установить пароль», доступной в контекстном меню этого учетной записи пользователя (рис. 8). Измените пароль для созданной учетной записи.

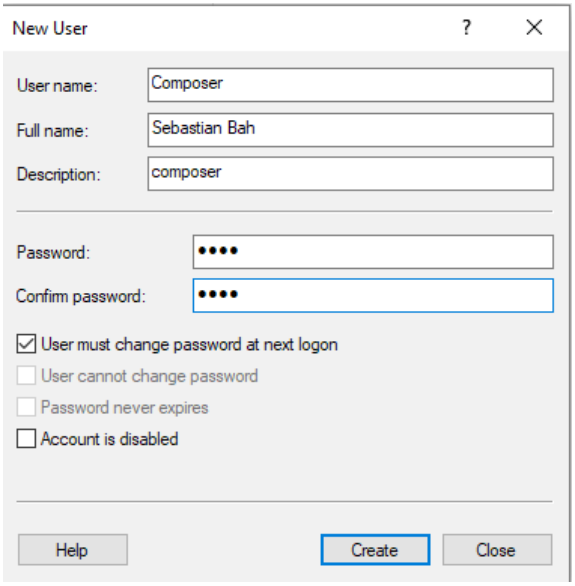


Рис. 8. Настройка параметров учетной записи при ее создании

В данный момент учетная запись «Администратор» заблокирована (рис. 10). Разблокируйте ее, выбрав соответствующий элемент в свойствах учетной записи. Посмотрите, какие еще параметры можно настроить в свойствах.

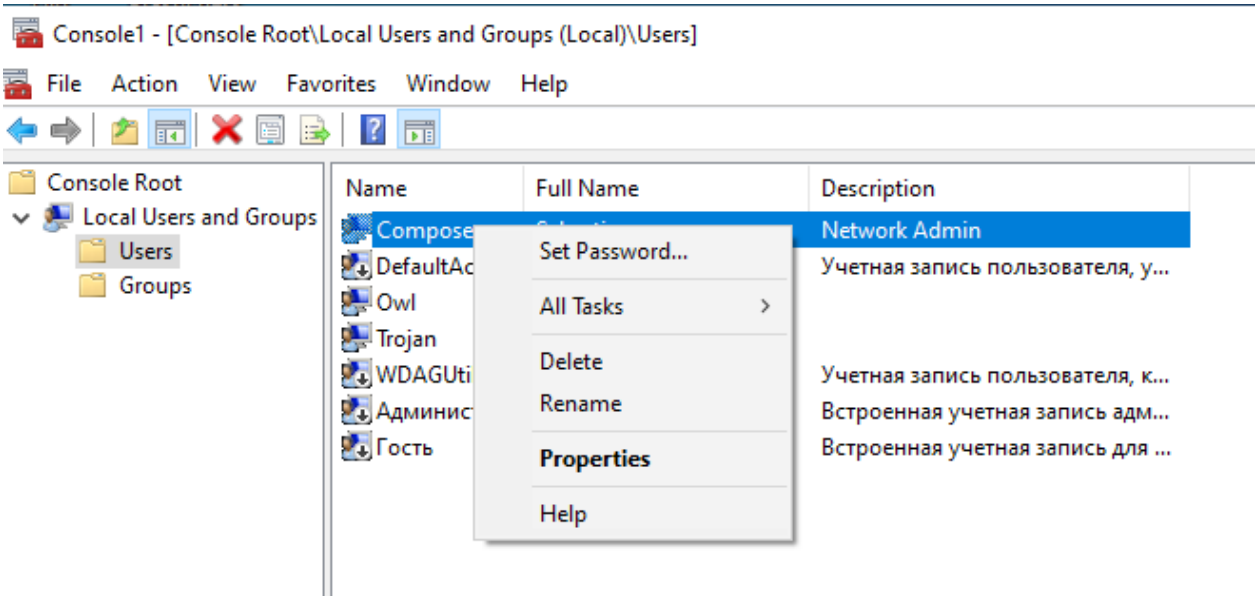


Рис. 9. Установка пароля пользователя администратором

Войдите в систему, используя созданную вами учетную запись. При первом входе в систему пользователю будет предложено ввести пароль и окно для смены пароля. Измените пароль созданной учетной записи. Здесь подтверждение действий осуществляется нажатием клавиши «Enter».

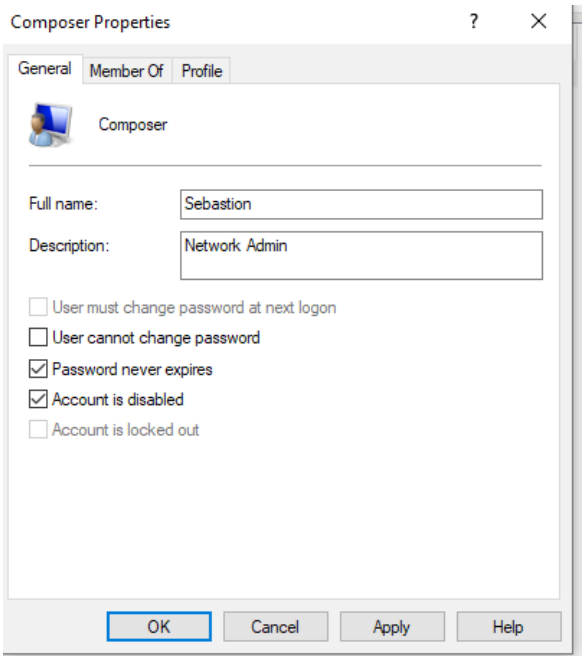


Рис. 10. Изменение свойств администратора

Чтобы применить набор прав и ограничений к пользователю, можно включить его учетную запись в группу пользователей с соответствующим набором прав и ограничений.

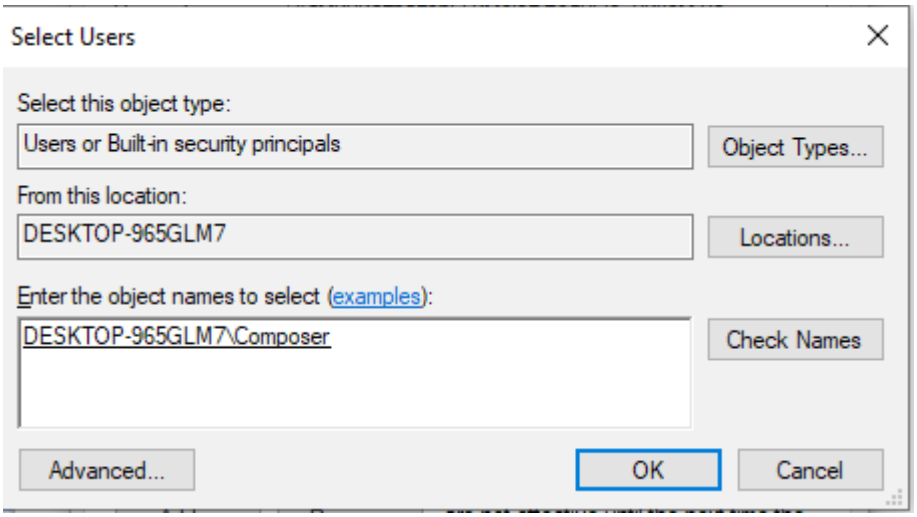


Рис. 11. Добавление группы

Войдите в систему, используя учетную запись «Администратор». Откройте «Свойства» созданной учетной записи. На вкладке «Группа членов» добавьте пользователя в группу «Power Users» (рис. 11). Вы можете ввести название группы самостоятельно или выбрать его из предложенного списка, последовательно нажав кнопки «Дополнительно» и «Поиск».

В разделе «Группы» откройте «Свойства» группы «Power Users» и убедитесь, что учетная запись была добавлена в группу. Создайте новую группу и добавьте в нее того же пользователя.

Откройте командную строку и выполните команду «net user». Консоль отобразит список всех доступных учетных записей (рис. 14).

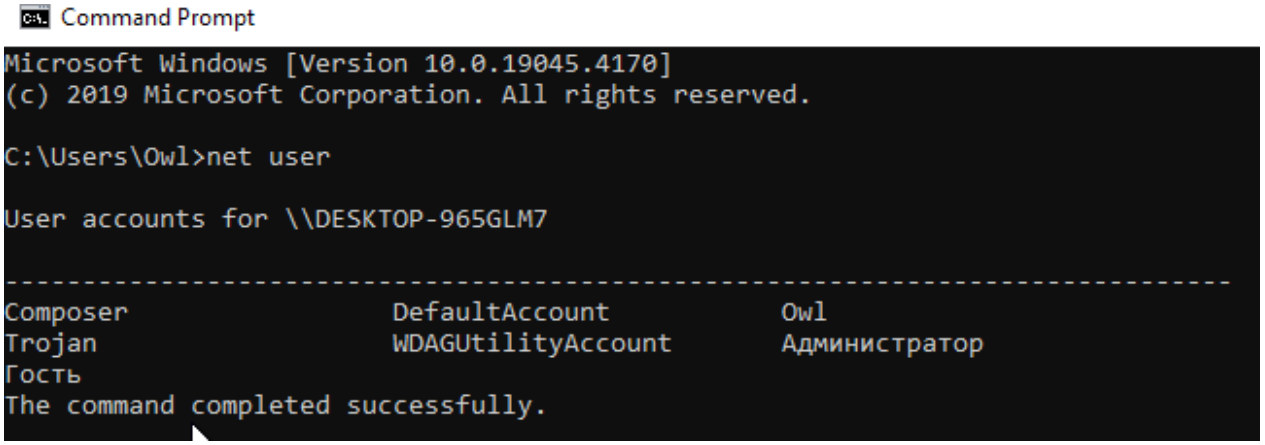


Рис. 14.

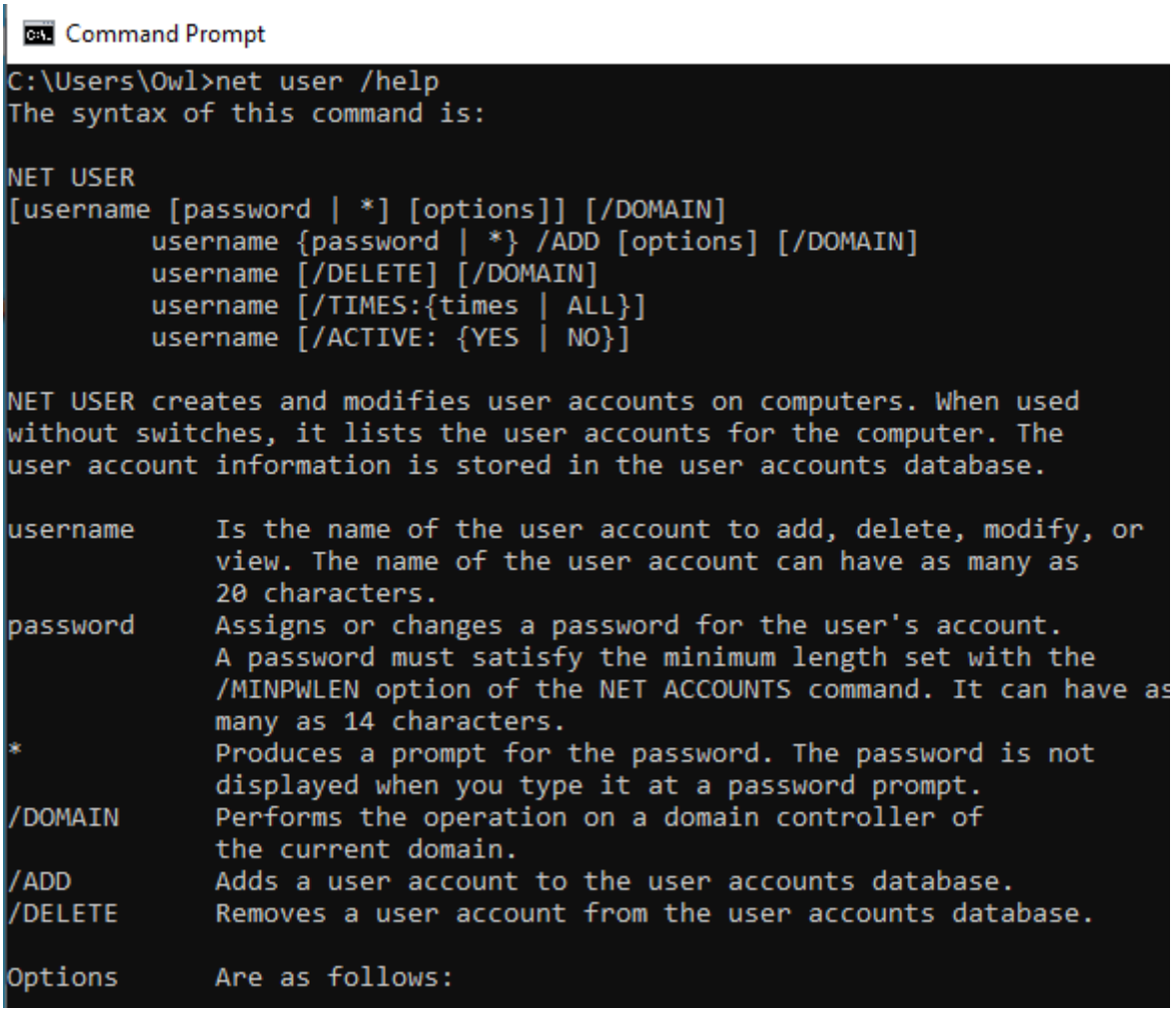


Рис. 15. Справка по команде Net user

Создайте учетную запись пользователя с именем, соответствующим вашему имени в сети кафедр, явно указав пароль. При создании, помимо аутентификации, укажите полное имя пользователя.

Синтаксис команды Net user при создании учетной записи пользователя:

Net user имя_пользователя {пароль | *} /ADD [параметры].

Чтобы добавить полное имя пользователя, введите в качестве параметра:

/FULLNAME: «имя».

C:\Users\Admin>net user XXX 12345 /add /fullname:"XXX YYY"

Проверьте наличие созданной учетной записи в списке пользователей с

помощью команды Net user. Команда

Net user имя_пользователя,

введенная без параметров, позволяет просматривать информацию об указанном пользователе. Просмотрите информацию об учетной записи, которую вы создали.

Можно ввести пароль, не отображая его на экране — для этого введите «*» вместо пароля. Измените пароль созданного пользователя с помощью команды:

Net user username *

C:\Users\ Admin >net user sdv *

Введите пароль для пользователя:
Введите пароль еще раз для подтверждения:
Команда выполнена успешно. Пароль пользователя успешно изменен.
Можно установить временные ограничения для работы пользователя в операционной системе. Для этого используйте /TIMES:{ интервал | ВСЕ}. Значение ALL означает, что пользователь может авторизоваться в любое время, а пустое значение означает, что пользователь не может авторизоваться никогда. Ограничьте время работы созданного пользователя рабочими часами (рис. 18). Установите часы на время вне рабочих часов и проверьте возможность пользователя авторизоваться в операционной системе.

C:\Users\Admin>net user XXX /times:Понедельник-Пятница,09:00-18:00

Команда выполнена успешно. Настройка срока действия учетной записи.

При необходимости администратор может заблокировать учетную запись пользователя. Заблокируйте созданную учетную запись пользователя с помощью /ACTIVE:{YES | NO}

C:\Users\Admin>net user XXX /active:no

Команда выполнена успешно. Блокировка учетной

записи. Проверьте, заблокирована ли учетная запись, с

помощью команды

Net user username

В предоставленной информации о пользователе есть столбец «Учетная запись активна», который показывает состояние учетной записи, которая заблокирована. Разблокируйте учетную запись пользователя.

Если пользователь временно работает в организации, администратор может ограничить срок действия учетной записи пользователя. Для этого используйте параметр:

/EXPIRES:{дата | NEVER}.

Если значение NEVER не используется, то учетная запись не имеет ограничений по сроку действия. Ограничьте срок действия созданной учетной записи пользователя. Установите

системное время на более позднюю дату

установите ограничение.

C:\Users\Admin >net user XXX /expires:24.09.2024

Команда выполнена успешно. Ограничение по времени для учетной записи.

Попробуйте войти в систему с помощью этой учетной записи — операционная система выдаст ошибку при попытке войти с просроченной учетной записью.

Команда

Net localgroup

используется для создания и управления локальными группами. При использовании этой команды без указания параметров отображается список групп пользователей, существующих в операционной системе (рис. 16). Выведите список всех существующих групп.

Синтаксис команды при создании локальной группы:

Net localgroup group_name {/ADD }

Для создания локальной группы Students используем команду

C:\Users\Admin>net localgroup Students /add

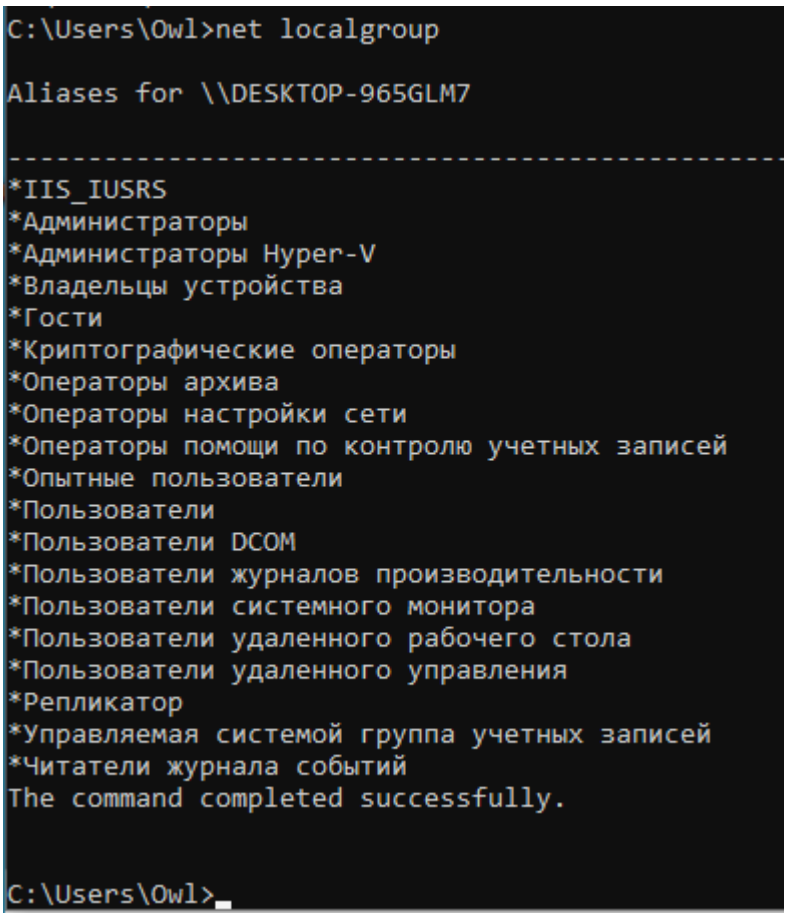


Рис. 16. Список групп

Добавление пользователей в группу осуществляется с помощью

команды

Net localgroup group_name name [...] {/ADD },

где **name [...]** — имя одного или нескольких пользователей (имена разделяются пробелами).

Добавьте ранее созданного пользователя в группу Students. Команда ***Net localgroup group_name*** отображает список пользователей, являющихся членами указанной группы. Отображает список пользователей группы Students (рис. 17).

```
C:\Users\Owl>net localgroup Администраторы
Alias name     Администраторы
Comment        Администраторы имеют полные, ничем не ограниченные права доступа к компьютеру или домену

Members

-------------------------------------------------------------------------------
Composer
Owl
Администратор
The command completed successfully.
```

Рис. 17. Просмотр списка пользователей определенной

группы Чтобы удалить пользователя из группы, используйте команду

Net localgroup group_name user_name {/DELETE}

Удалите из группы Students пользователя XXX с помощью команды:

C:\Users\Admin>net localgroup Sstudents XXX /DELETE

Удалите группу Students с помощью команды:

C:\Users\Admin>net localgroup Students /DELETE

Проверьте, что группа Studenți отсутствует, с помощью команды ***Net localgroup***

1.2. Настройка политики учетной записи

Откройте «Локальная политика безопасности», активировав запрос **secpol.msc** в меню «Пуск». Главное окно «Локальная политика безопасности» представлено на рисунке 18. Значения параметров, указанных при установке политики, будут применяться ко всем пользователям локального компьютера.

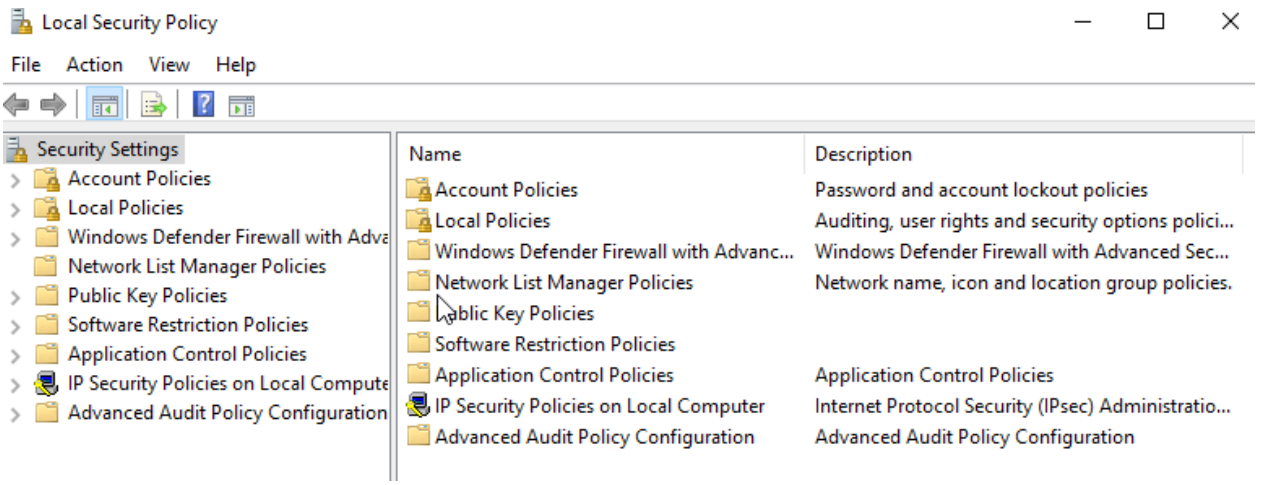


Рис. 18. Локальная политика безопасности

Раздел «Политики учетных записей» в «Локальной политике безопасности» содержит настройки, которые применяются к паролям пользователей.

Выберите раздел «Политика паролей» («Настройки безопасности → Политики учетных записей → Политика паролей»). Настройки, включенные в раздел «Политика паролей», представлены на рис. 19.

Выполните следующие задачи:

- установите максимальный срок действия пароля — 30 дней;

- установите минимальную длину пароля 10 символов;

- для параметра «Вести журнал паролей» установите значение 3 сохраненных пароля, что означает, что новый пароль должен отличаться от последних 3 паролей пользователя;

- активируйте опцию «Пароль должен соответствовать требованиям сложности».

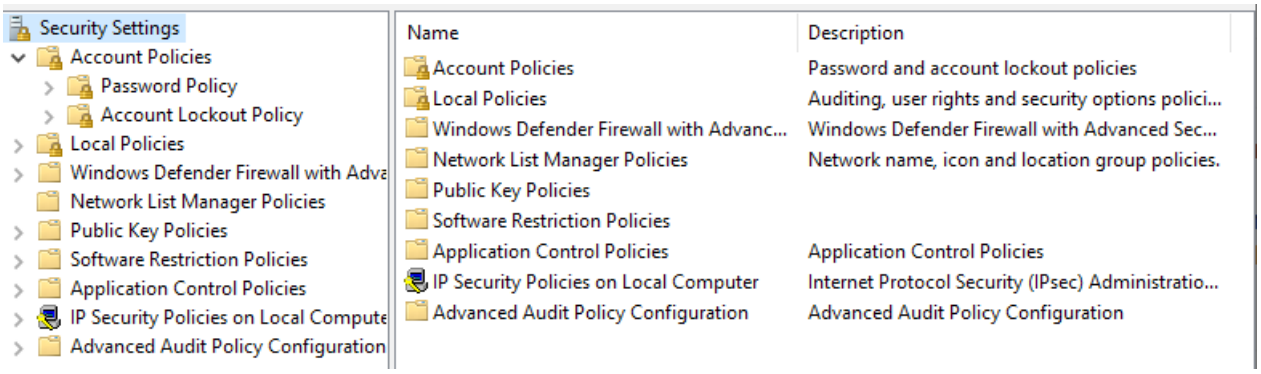


Рис. 19. Политика паролей

Настройка «Пароль должен соответствовать требованиям сложности» определяет требования к сложности паролей. Если эта политика включена, пароли должны соответствовать следующим минимальным требованиям:

- пароль не может содержать имя учетной записи пользователя или любую его часть;

- пароль должен содержать не менее шести символов;

- пароль должен содержать символы из трех категорий из следующих четырех:

a) заглавные буквы английского алфавита от A до Z; b) строчные буквы английского алфавита от a до z;

c) десятичные цифры (от 0 до 9);

d) неалфавитные символы (например, !, $, #, %).

Соблюдение этих требований проверяется при изменении или создании паролей. Используя этот параметр, вы можете избавиться от легко угадываемых паролей.

Убедитесь, что у пользователя не включена опция «Пароль никогда не истекает» в оснастке «Локальные пользователи и группы». Установите системное время на более чем 30 дней вперед. Попробуйте войти в систему, используя созданную вами учетную запись. Пользователю будет сообщено, что срок действия пароля истек. При смене пароля попробуйте заменить его на более простой (например, abc12345 или пароль, включающий имя учетной записи). В этом случае пользователь получит сообщение об ошибке при смене пароля. Введите пароль, соответствующий указанным выше требованиям.

Войдите в систему, используя учетную запись «Admin». Сбросьте системное время до исходного состояния. Выберите раздел «Политика блокировки учетной записи» («Настройки безопасности → Политики учетной записи → Политика блокировки учетной

записи»). Настройки, включенные в раздел «Политика блокировки учетной записи», представлены на рис. 20.

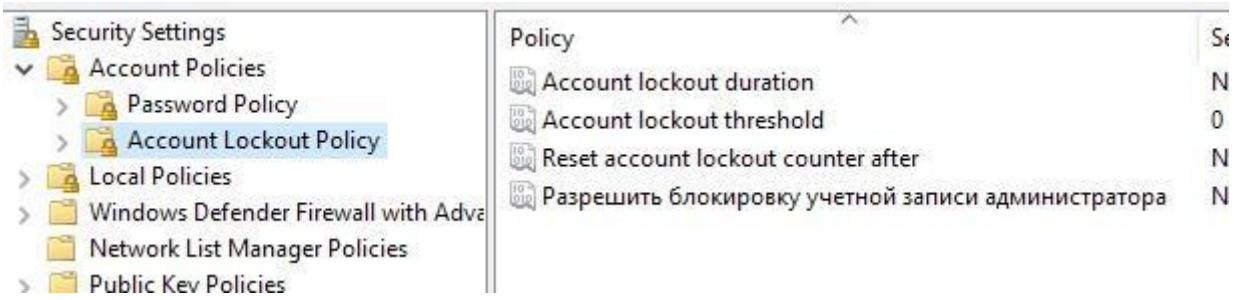


Рис. 20. Политика блокировки учетной

записи Настройте параметры следующим образом:

- установите порог блокировки равным 3 ошибкам входа (после 3 неудачных попыток входа аккаунт блокируется);

- установите продолжительность блокировки в параметре «Блокировка учетной записи на» на 30 минут (значение 0 означает, что только администратор может снять блокировку);

- установите сброс счетчика блокировки через 15 минут. Если в течение указанного времени произошло 3 неудачных попытки входа, учетная запись блокируется. Если в течение установленного времени произошло меньше неудачных попыток, то снова допускается 3 неудачных попытки (значение этого параметра не должно превышать продолжительность блокировки учетной записи).

Выйдите из учетной записи администратора. При входе в систему с помощью созданной учетной записи три раза введите неверный пароль. При следующей попытке входа вы получите сообщение о том, что созданная учетная запись заблокирована.

Войдите в систему, используя учетную запись «Администратор». Разблокируйте созданную учетную запись. Для этого в окне «Свойства» этой учетной записи отключите настройку «Блокировка учетной записи».

Откройте командную строку. **Net accounts** используется для обновления базы данных входа в систему и изменения настроек входа (LOGON) и требований к паролю для всех входов. При использовании этой команды без указания параметров отображаются текущие значения параметров, контролирующих требования к паролю и другие настройки. Отобразите текущие параметры входа в систему (рис. 21).

Установите следующие требования к паролю:

- минимальная длина — 6 символов;

- максимальный срок действия пароля — 40 дней;

- запрет на использование последних 3 паролей пользователя.

```
C:\Users\Owl>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        WORKSTATION
The command completed successfully.
```

Рис. 21. Просмотр информации о требованиях к качеству пароля

Эти требования применяются с помощью следующих параметров команды **Net accounts**:

/MINPWLEN: минимальная_длина /MAXPWAGE: дней /UNIQUEPW:

количество_паролей C:\UsGrs\Admin>net accounts /minpwlen:6 /maxpwage:40

/uniquepw:3

1.3. Групповые политики

Откройте оснастку «Групповая политика» (Пуск → Выполнить → **gpedit.msc**). Оснастка «Групповая политика» состоит из двух основных частей: настройки компьютера и настройки пользователя (рис. 22).

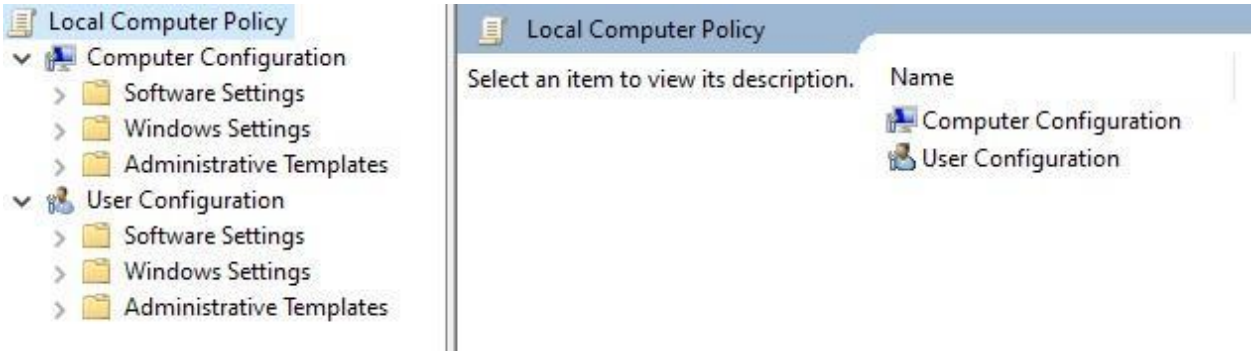


Рис. 22. Редактор групповых политик

Настройка компьютера используется для установки политик, которые применяются к компьютерам, независимо от того, какой пользователь их запускает. Настройка пользователя используется для установки политик, которые применяются к пользователям, независимо от того, какой компьютер они используют для входа в систему.

Созданная групповая политика может быть экспортирована на другой локальный компьютер. Для экспорта данных необходимо выбрать нужный узел в оснастке «Групповая политика» и выбрать «Экспорт списка» на вкладке «Действие». В появившемся окне выберите путь для сохранения и укажите имя файла.

«Конфигурация компьютера» по умолчанию состоит из следующих разделов: конфигурация программы, конфигурация Windows и административные шаблоны (рис. 23).

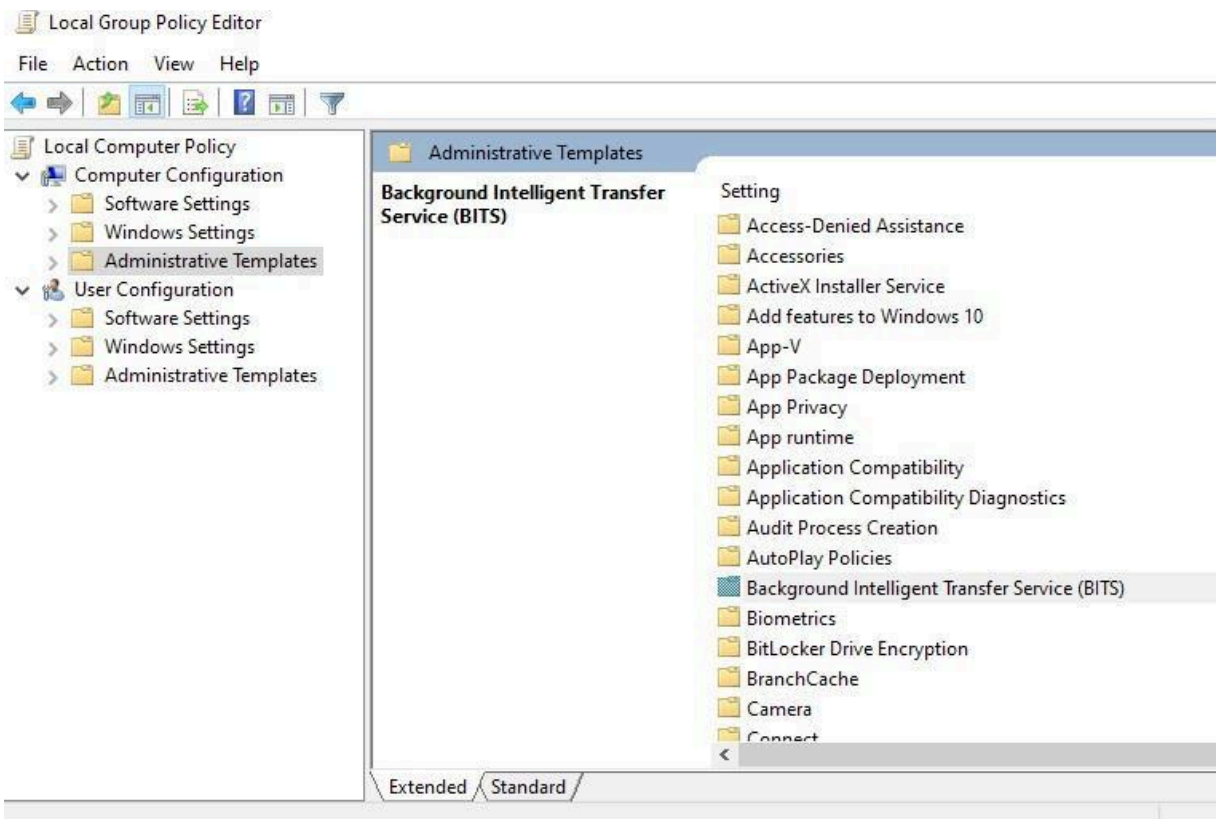

Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Administrative Templates
Background Intelligent Transfer Service (BITS)
Setting
Access-Denied Assistance
Accessories
ActiveX Installer Service
Add features to Windows 10
App-V
App Package Deployment
App Privacy
App runtime
Application Compatibility
Application Compatibility Diagnostics
Audit Process Creation
AutoPlay Policies
Background Intelligent Transfer Service (BITS)
Biometrics
BitLocker Drive Encryption
BranchCache
Camera
Extended
Standard

Рис. 23. Раздел «Административные шаблоны»

В разделе «Система» откройте подраздел «Аутентификация» и выберите опцию «Запускать эти программы при входе в систему». Активируйте эту опцию и добавьте несколько программ, которые будут запускаться при входе пользователя в систему (рис. 24).

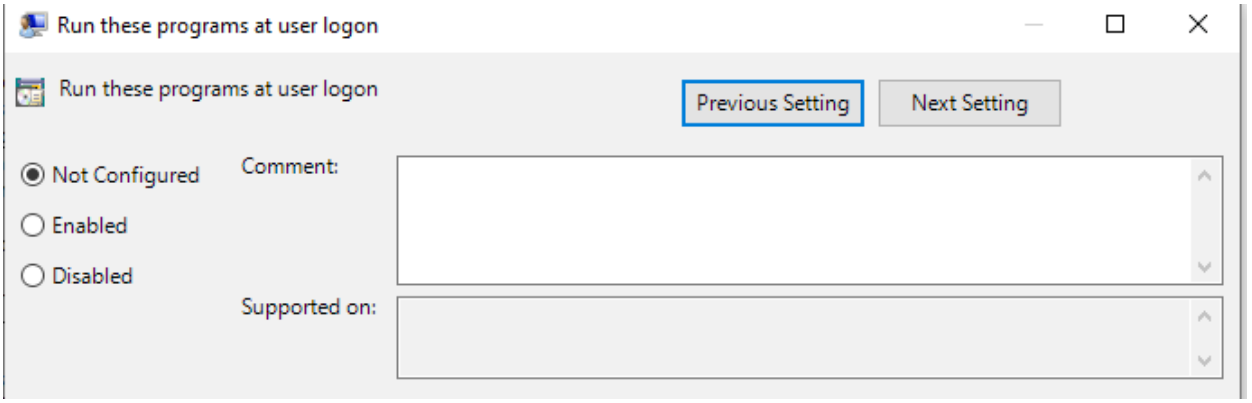


Рис. 24. Активация программ

Добавленные программы будут запускаться каждый раз при входе пользователя в систему. Пожалуйста, войдите в систему еще раз, чтобы проверить.

«Конфигурация пользователя» по умолчанию состоит из тех же разделов, что и «Конфигурация компьютера». Используя настройки групповой политики, можно ограничить доступ пользователей к логическим дискам. Вы можете скрыть выбранный диск в Проводнике, а также запретить доступ к нему.

Выберите опцию «Запретить доступ к дискам через мой компьютер», расположенную в подразделе
«Компоненты Windows → Проводник» и запретите доступ к логическому диску C:\ (рис. 25).

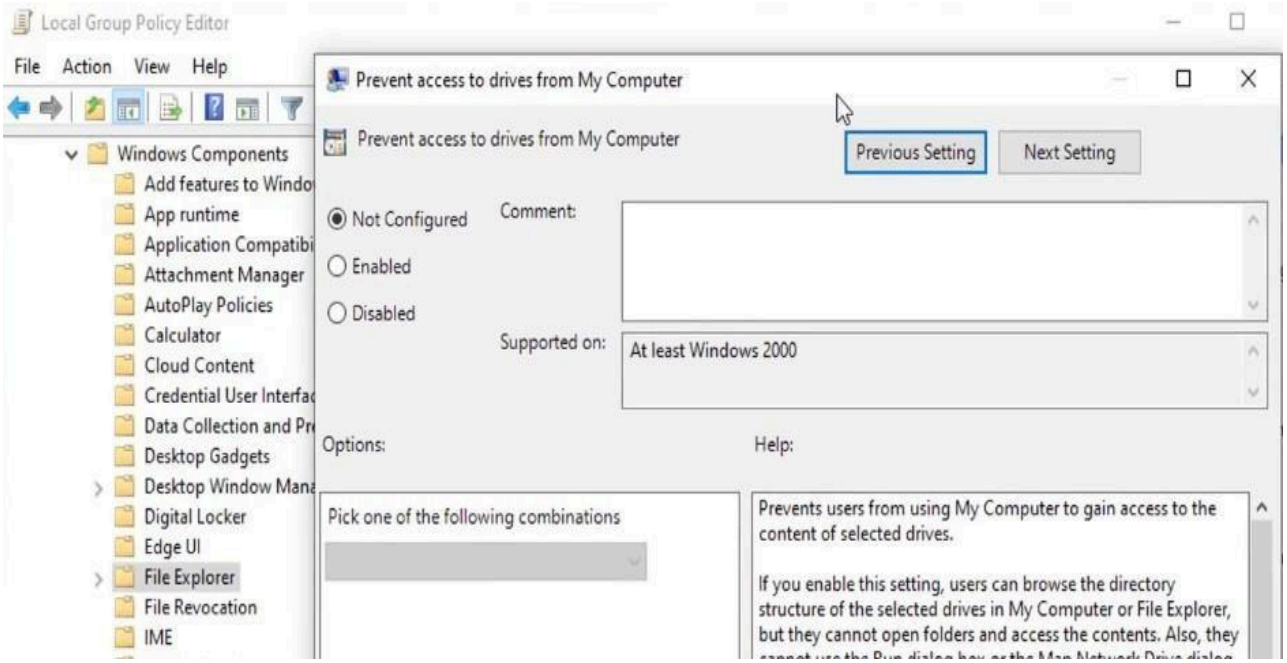


Рис. 25. Активация ограничений доступа для управления C

Попробуйте открыть диск C:\ через «Мой компьютер» и командную строку.

C:\Users\Admin>C:

В первом случае система откажет в доступе, а во втором — доступ будет предоставлен (поскольку доступ запрещен только через Explorer).

Ограничение доступа к инструментам администрирования возможно путем запрета доступа к панели управления. Активируйте опцию «Запретить доступ к панели управления», находящуюся в подразделе «Панель управления». Попробуйте открыть **cmd.exe**.

Кроме того, в подразделе «Система» вы можете отключить использование Редактора реестра. Для этого необходимо активировать опцию «Сделать инструменты редактирования реестра недоступными». Активируйте эту опцию и попробуйте запустить Редактор реестра

C:\Windows\regedit.exe.

Добавление и удаление шаблонов можно выполнить через контекстное меню раздела «Административные шаблоны» (рис. 26). В появившемся контекстном меню выберите «Добавить» или «Удалить шаблоны». В появившемся окне вы можете удалить любой шаблон, а также добавить новый шаблон политики.

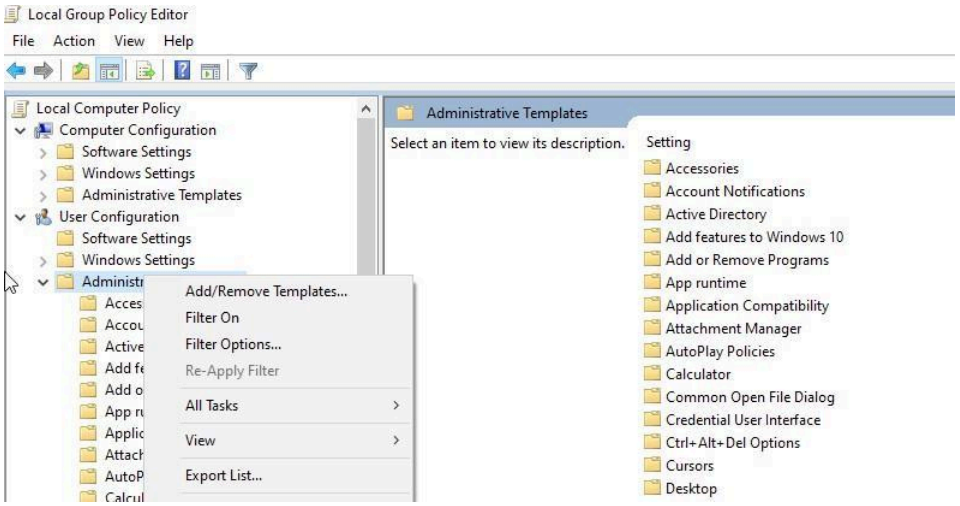


Рис. 26. Контекстное меню «Административные шаблоны»

2. Редактор реестра в Windows 10

Большинство настроек Windows хранятся в его реестре — базе данных с ключами и значениями, которая позволяет операционной системе Windows знать, какие настройки использовать для приложений, функций, драйверов, аппаратных устройств и т. д.

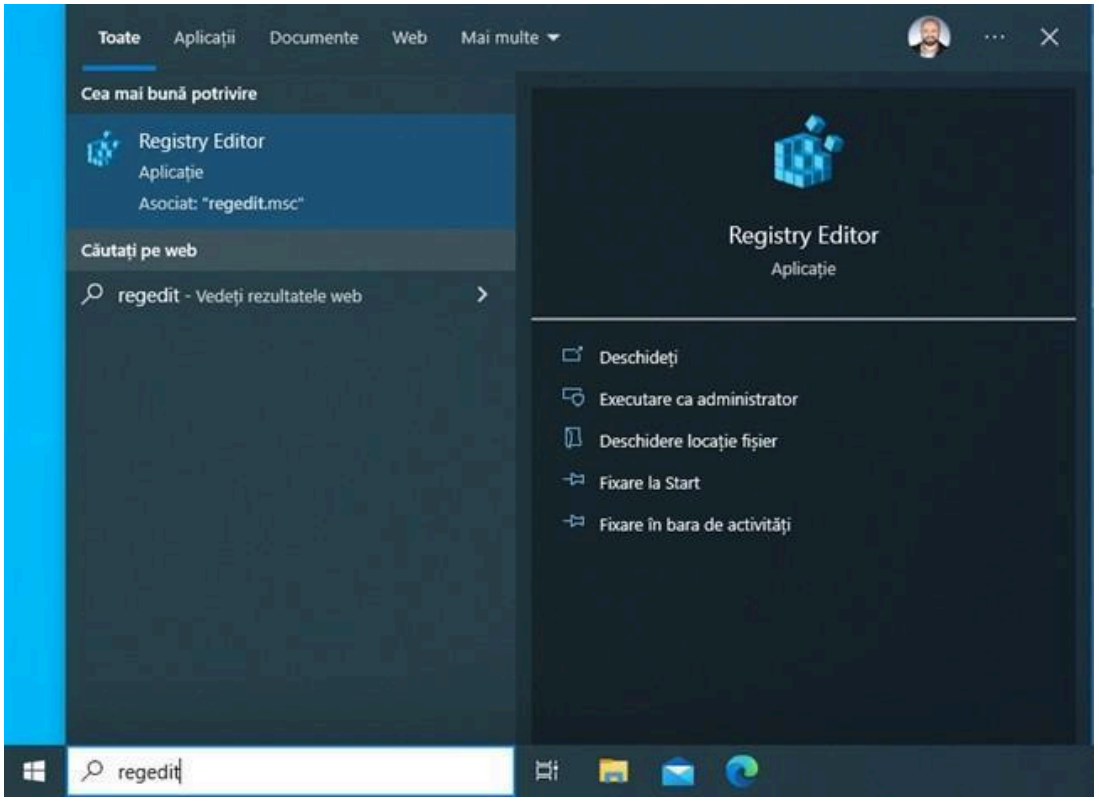
2.1.Как открыть редактор реестра с помощью поиска

Один из самых быстрых способов открыть любое приложение — использовать *Поиск*. Это также применимо к открытию приложения *Редактор реестра* от имени администратора. Вот как это работает:

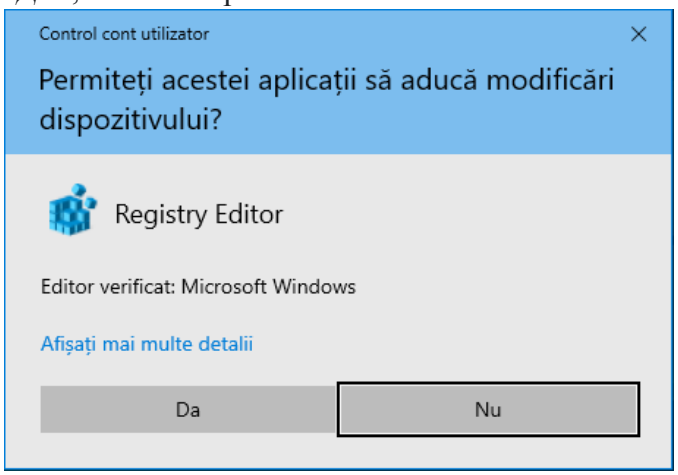
2.2. Найдите regedit в Windows 10

Если вы используете Windows 10, нажмите на поле *поиска* на панели задач и введите *regedit*.

Когда появится список результатов поиска, нажмите *Enter* на клавиатуре или щелкните *Registry Editor*.

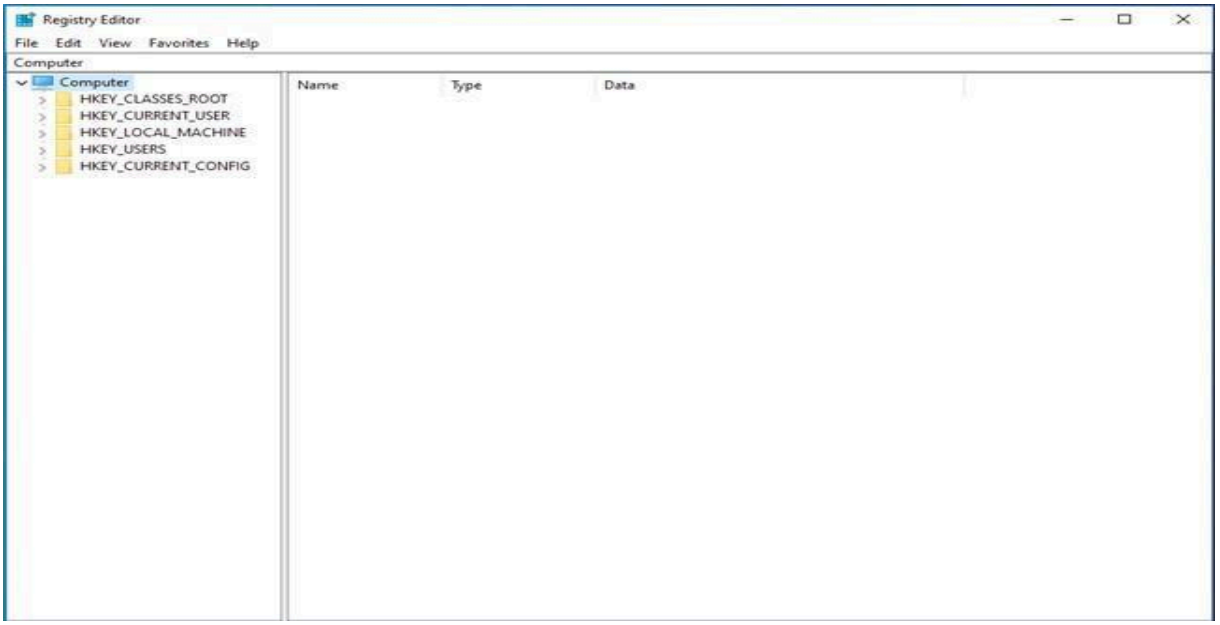


Перед открытием *Registry Editor* появится запрос *CCU*, который потребует подтверждения для запуска этого приложения, поскольку оно требует прав администратора. Нажмите *«Да»*, чтобы открыть его.



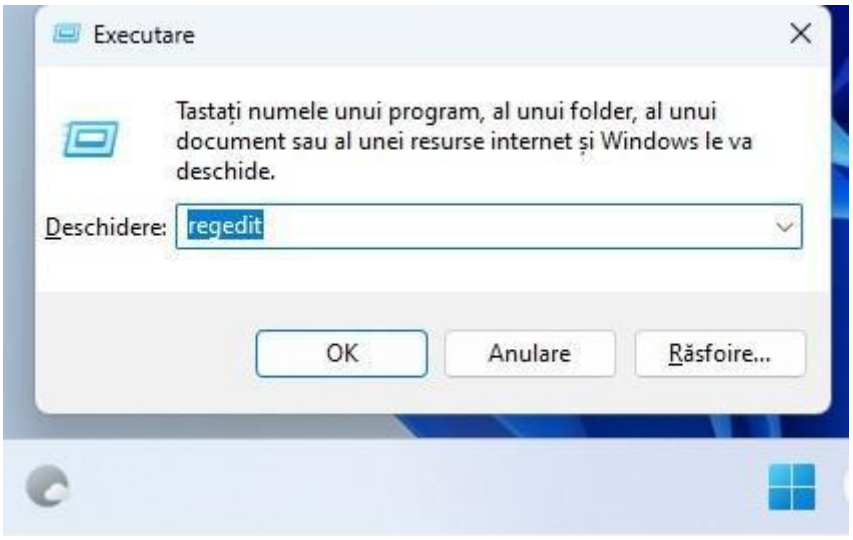
CCU запрашивает подтверждение для запуска regedit

Теперь появится окно *Registry Editor*, похожее на то, что показано на изображении ниже, и вы сможете редактировать или просматривать реестр Windows 10.



2.3. Как открыть Registry Editor с помощью окна «Выполнить»

Еще один быстрый способ открыть *Registry Editor* — ввести команду в окне *«Выполнить»*. Нажмите *Windows + R* на клавиатуре, чтобы открыть окно *«Выполнить»*. Затем введите эту команду, чтобы запустить *Registry Editor*:

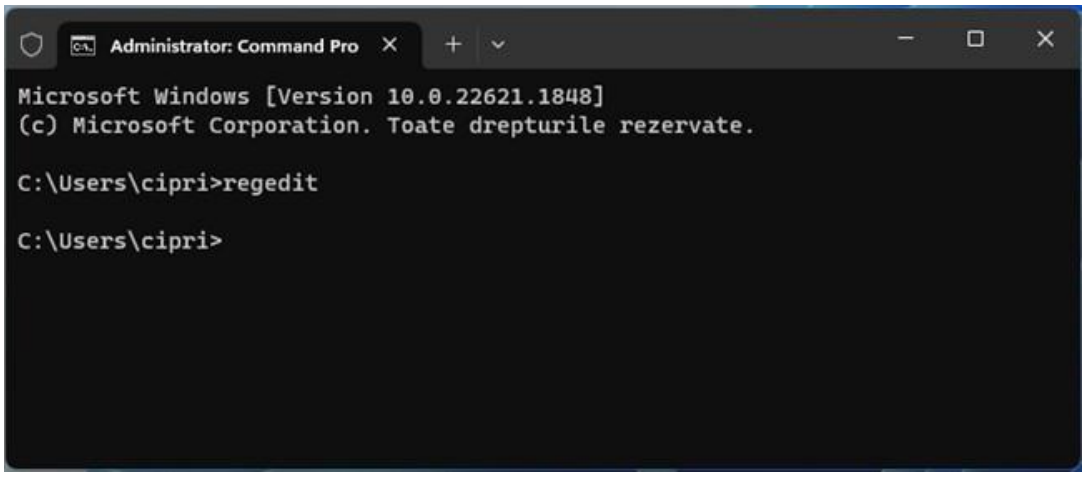


Команда для открытия **Registry Editor**

Нажмите *OK* или *Enter* на клавиатуре, чтобы запустить эту команду.

2.4. Как запустить Regedit от имени администратора с помощью CMD, PowerShell или Windows Terminal

Другой способ открыть *редактор реестра* — использовать команду *regedit* в командной строке, например в *PowerShell*, *командной строке* или *Windows Terminal*. Например, можно открыть *CMD* от имени администратора, ввести следующую команду и нажать клавишу *Enter*, чтобы ее выполнить:



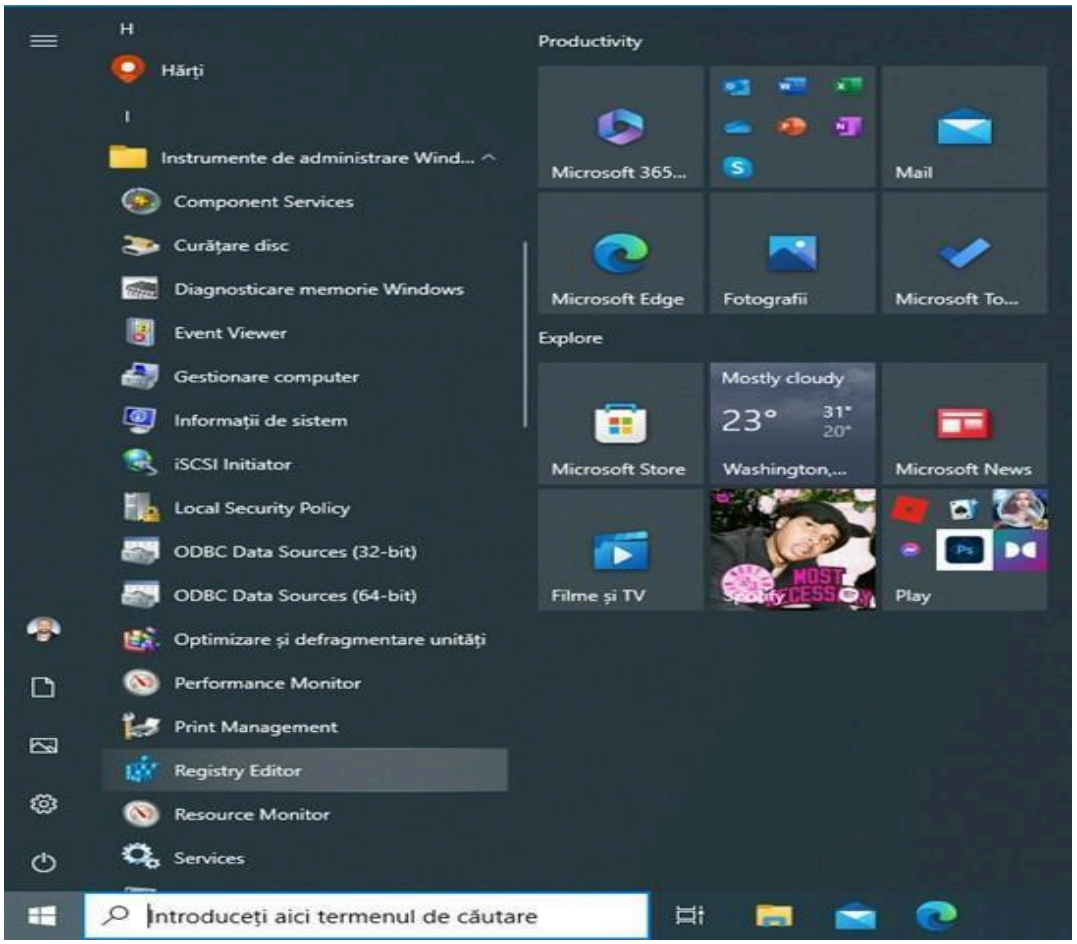
Запустите regedit в CMD, Power Shell или Windows Terminal

2.5.Как получить доступ к редактору реестра из меню «Пуск»

Меню «Пуск» содержит ярлык для *Registry Editor*, но его трудно найти, если не знать, где искать.

2.5.1. Где найти ярлык Registry Editor в меню «Пуск» Windows 10

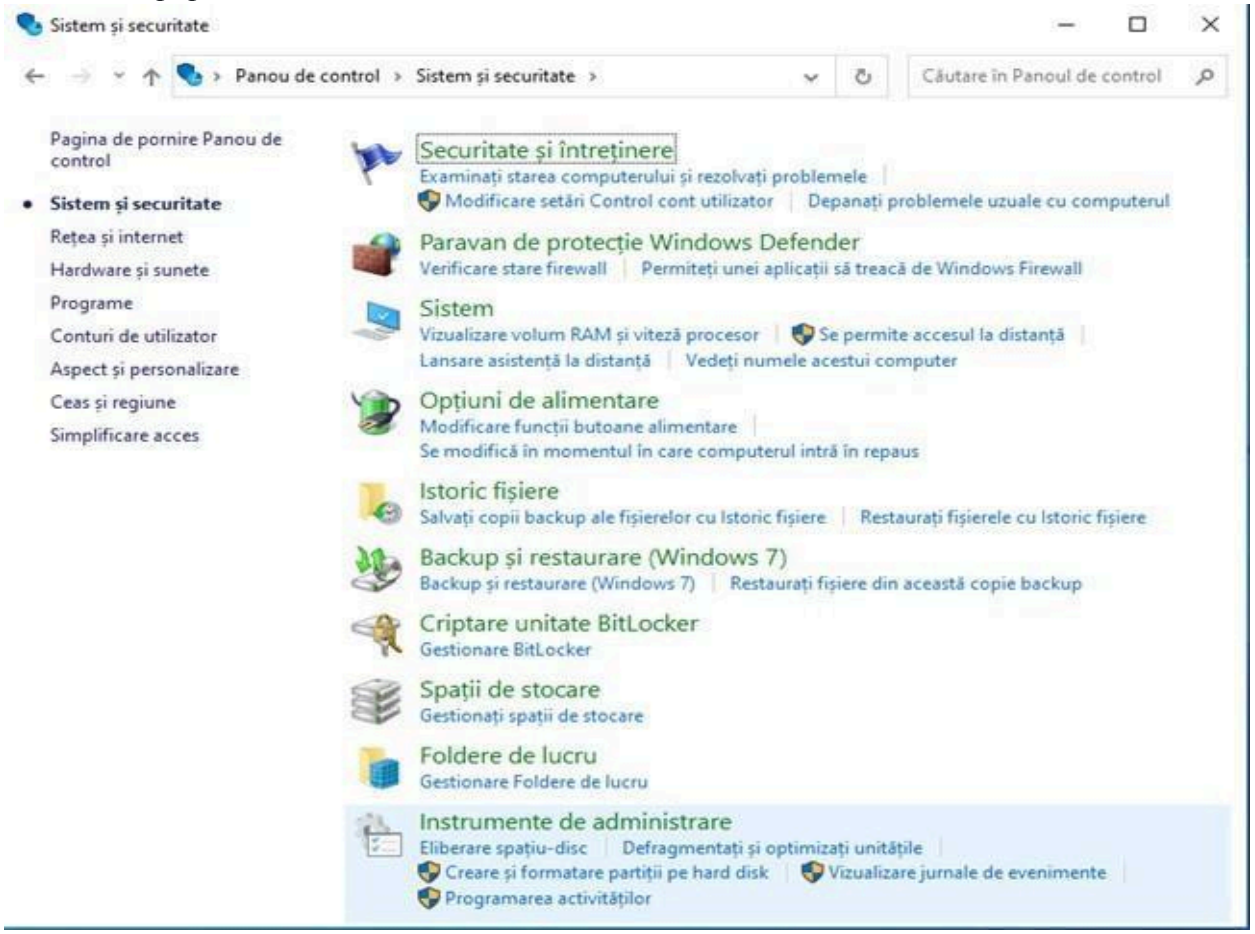
В Windows 10 нажмите на логотип *Windows* на панели задач, чтобы открыть *меню «Пуск»*. В списке приложений прокрутите до тех, которые начинаются с буквы *I*, и откройте папку *«Администрирование Windows»*. Найдите в ней ярлык *«Редактор реестра»* и нажмите на него.



Ярлык Registry Editor в меню «Пуск»

2.5.2. Как открыть редактор реестра в панели управления

Другой способ заключается в открытии *панели управления*. Затем перейдите в *раздел «Система и безопасность»*. Если вы используете Windows 10, нажмите *«Администрирование»*.



В открывшемся окне появится несколько ярлыков инструментов Windows. Найдите *Registry Editor* и дважды щелкните по его ярлыку.

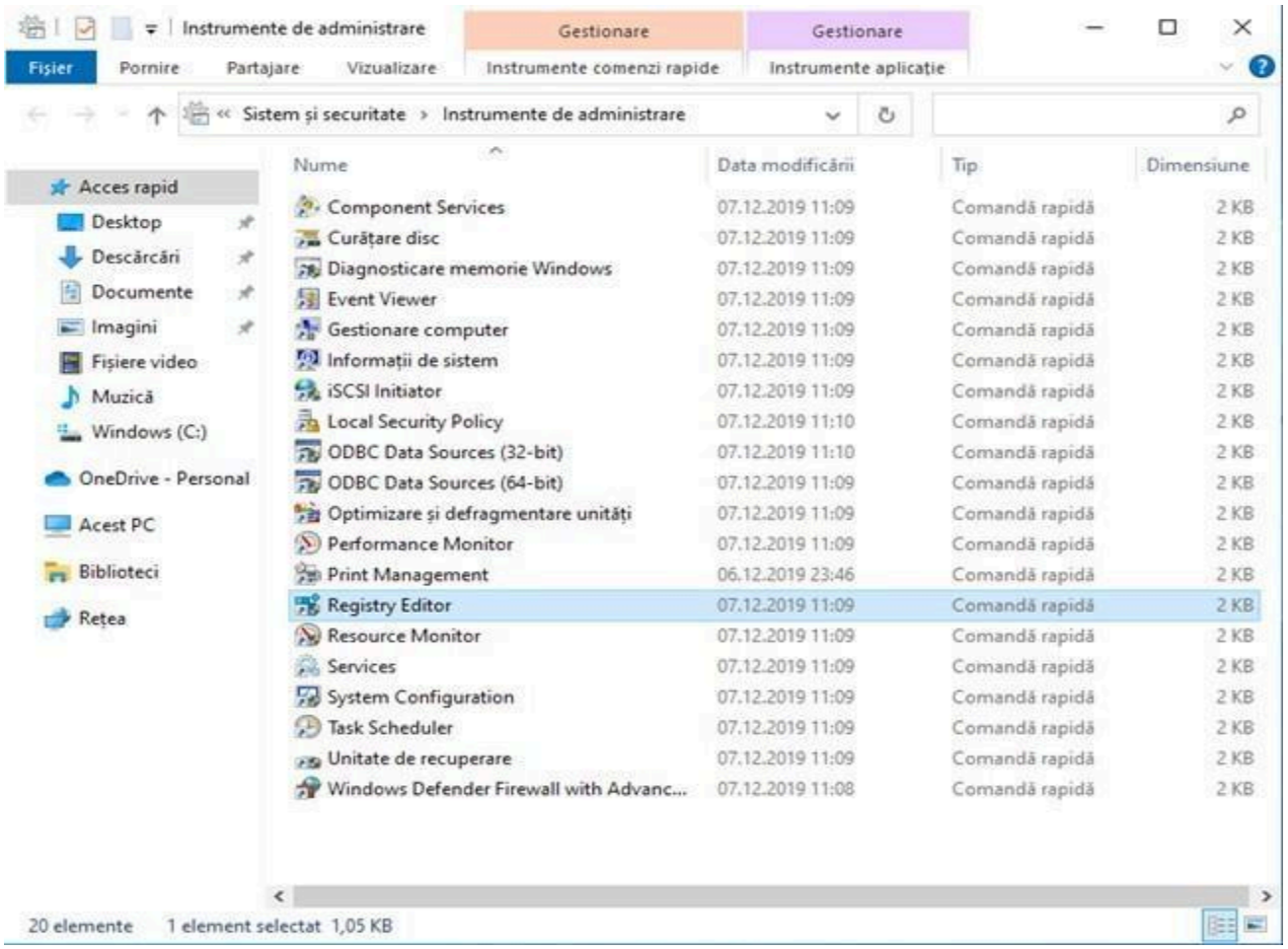
Дважды щелкните ярлык «Редактор реестра»

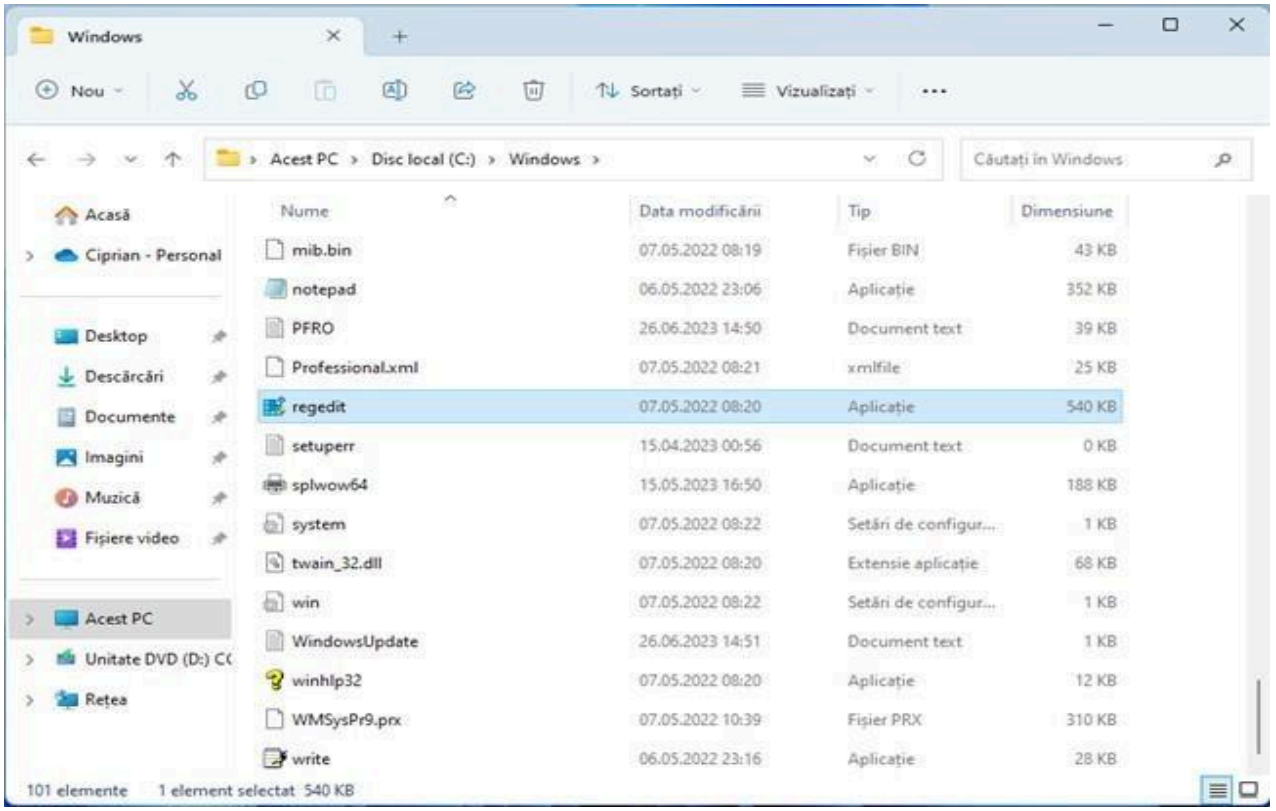
Нажмите *«Да»*, когда увидите запрос *CCU*.

2.6. Как запустить Редактор реестра из Проводника

Другой способ запустить *Редактор реестра* — открыть *Проводник* (*Windows + E*). Затем перейдите в следующее место:

```
C:\Windows\regedit.exe
```


Instrumente de administrare
Gestionare
Gestionare
Fișier
Pornire
Partajare
Vizualizare
Instrumente comenzi rapide
Instrumente aplicație
« Sistem și securitate › Instrumente de administrare
Acces rapid
Desktop
Descărcări
Documente
Imagini
Fișiere video
Muzică
Windows (C:)
OneDrive - Personal
Acest PC
Biblioteci
Rețea
Nume
Data modificării
Tip
Dimensiune
Component Services 07.12.2019 11:09 Comandă rapidă 2 KB
Curățare disc 07.12.2019 11:09 Comandă rapidă 2 KB
Diagnosticare memorie Windows 07.12.2019 11:09 Comandă rapidă 2 KB
Event Viewer 07.12.2019 11:09 Comandă rapidă 2 KB
Gestionare computer 07.12.2019 11:09 Comandă rapidă 2 KB
Informații de sistem 07.12.2019 11:09 Comandă rapidă 2 KB
iSCSI Initiator 07.12.2019 11:09 Comandă rapidă 2 KB
Local Security Policy 07.12.2019 11:10 Comandă rapidă 2 KB
ODBC Data Sources (32-bit) 07.12.2019 11:10 Comandă rapidă 2 KB
ODBC Data Sources (64-bit) 07.12.2019 11:09 Comandă rapidă 2 KB
Optimizare și defragmentare unități 07.12.2019 11:09 Comandă rapidă 2 KB
Performance Monitor 07.12.2019 11:09 Comandă rapidă 2 KB
Print Management 06.12.2019 23:46 Comandă rapidă 2 KB
Registry Editor 07.12.2019 11:09 Comandă rapidă 2 KB
Resource Monitor 07.12.2019 11:09 Comandă rapidă 2 KB
Services 07.12.2019 11:09 Comandă rapidă 2 KB
System Configuration 07.12.2019 11:09 Comandă rapidă 2 KB
Task Scheduler 07.12.2019 11:09 Comandă rapidă 2 KB
Unitate de recuperare 07.12.2019 11:09 Comandă rapidă 2 KB
Windows Defender Firewall with Advanc... 07.12.2019 11:08 Comandă rapidă 2 KB
20 elemente
1 element selectat 1,05 KB

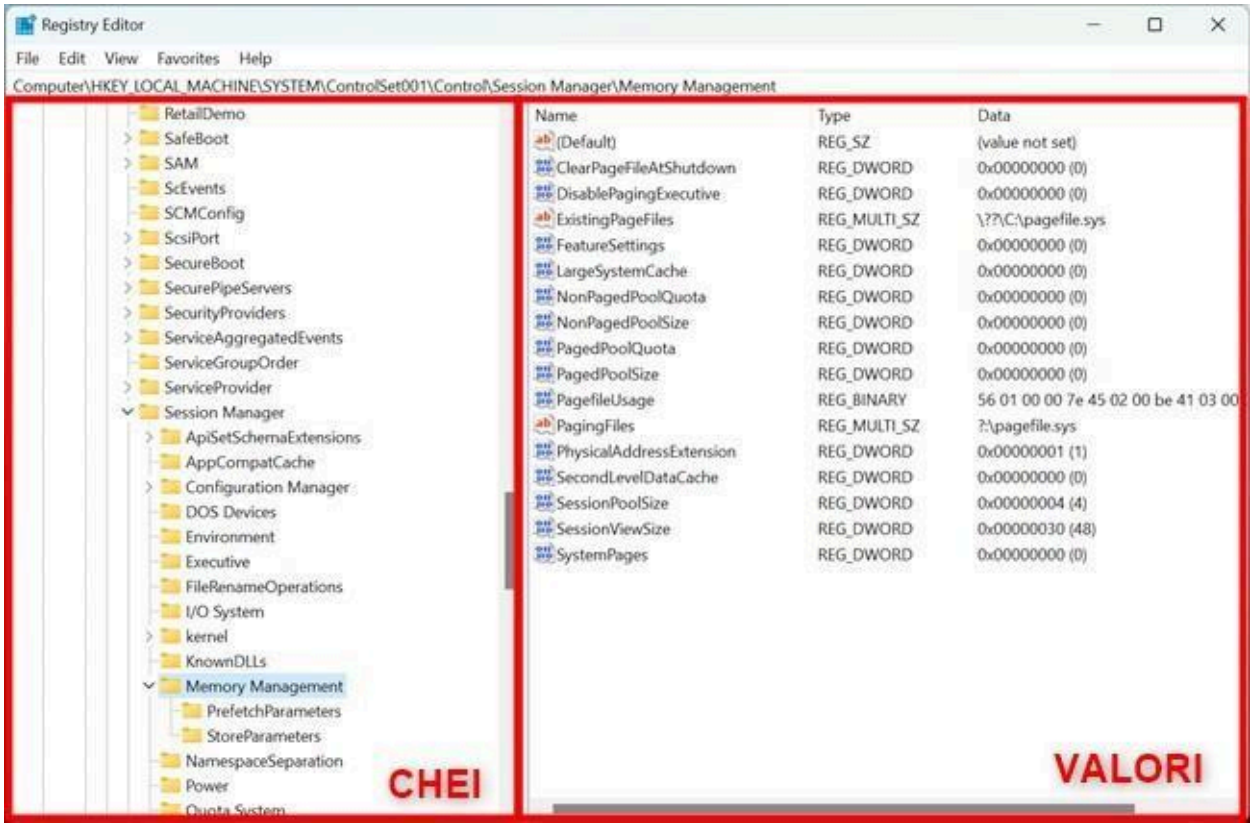

Windows
Nou
Sortați
Vizualizați
Acest PC › Disc local (C:) › Windows ›
Căutați în Windows
Acasă
Ciprian - Personal
Desktop
Descărcări
Documente
Imagini
Muzică
Fișiere video
Acest PC
Unitate DVD (D:) CC
Rețea
Nume
Data modificării
Tip
Dimensiune
mib.bin 07.05.2022 08:19 Fișier BIN 43 KB
notepad 06.05.2022 23:06 Aplicație 352 KB
PFRO 26.06.2023 14:50 Document text 39 KB
Professional.xml 07.05.2022 08:21 xmlfile 25 KB
regedit 07.05.2022 08:20 Aplicație 540 KB
setuperr 15.04.2023 00:56 Document text 0 KB
splwow64 15.05.2023 16:50 Aplicație 188 KB
system 07.05.2022 08:22 Setări de configur... 1 KB
twain_32.dll 07.05.2022 08:20 Extensie aplicație 68 KB
win 07.05.2022 08:22 Setări de configur... 1 KB
WindowsUpdate 26.06.2023 14:51 Document text 1 KB
winhlp32 07.05.2022 08:20 Aplicație 12 KB
WMSysPr9.prx 07.05.2022 10:39 Fișier PRX 310 KB
write 06.05.2022 23:16 Aplicație 28 KB
101 elemente
1 element selectat 540 KB

Запуск regedit.exe из Проводника

Вы также можете ввести команду *regedit* в адресной строке *File Explorer* и нажать *Enter* на клавиатуре.

2.7. Как редактировать редактор реестра

Открыв приложение *Registry Editor*, вы увидите, что оно разделено на две панели. Левая панель окна показывает иерархическое представление ключей *реестра Windows*. В правой панели вы можете просматривать и работать со значениями ключей, выбранных в левой панели.

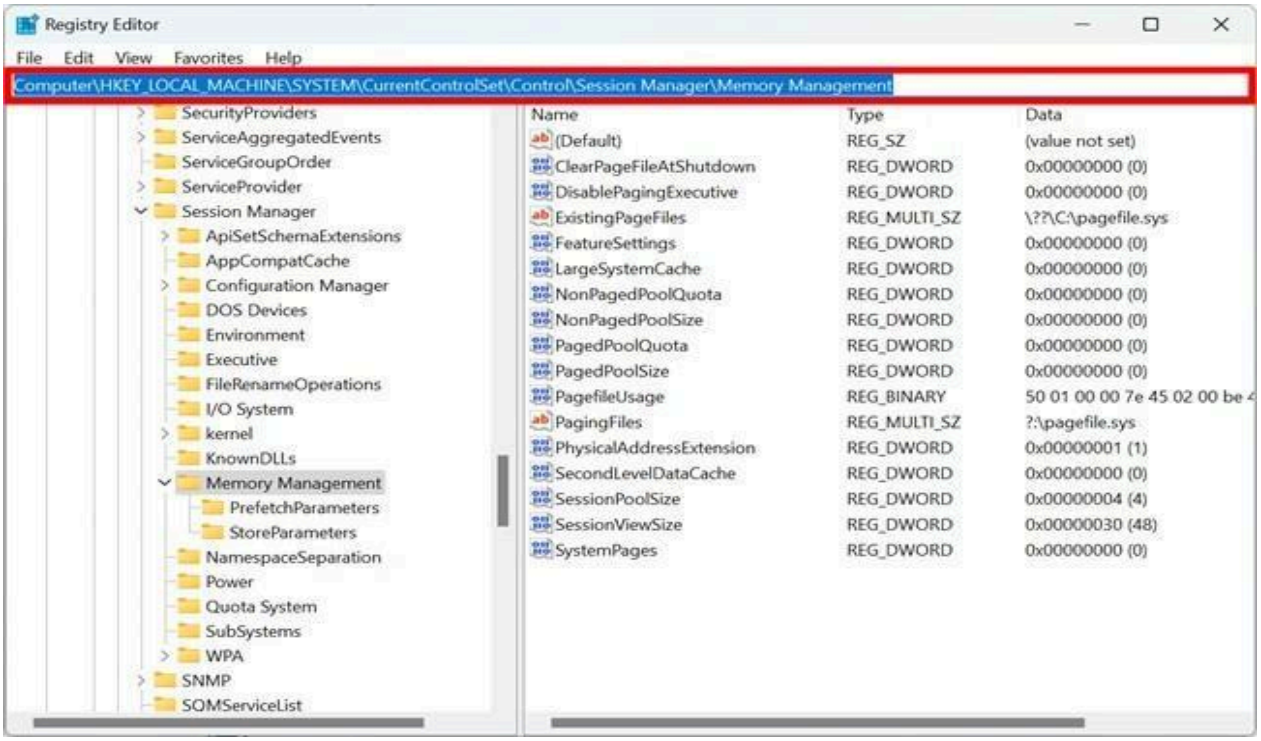


Редактор реестра содержит ключи и значения

Хотя *Registry Editor* позволяет создавать новые ключи и значения и даже удалять их, большинство пользователей используют его для редактирования ключей и значений, уже находящихся в *реестре Windows*. К сожалению, почти все ключи и значения в *реестре Windows* имеют загадочные названия и обычно спрятаны под множеством родительских ключей. Поэтому я рекомендую вам найти в Интернете то, что вы хотите изменить в *реестре Windows*, прежде чем вносить изменения.

Адрес ключа в Registry Editpr

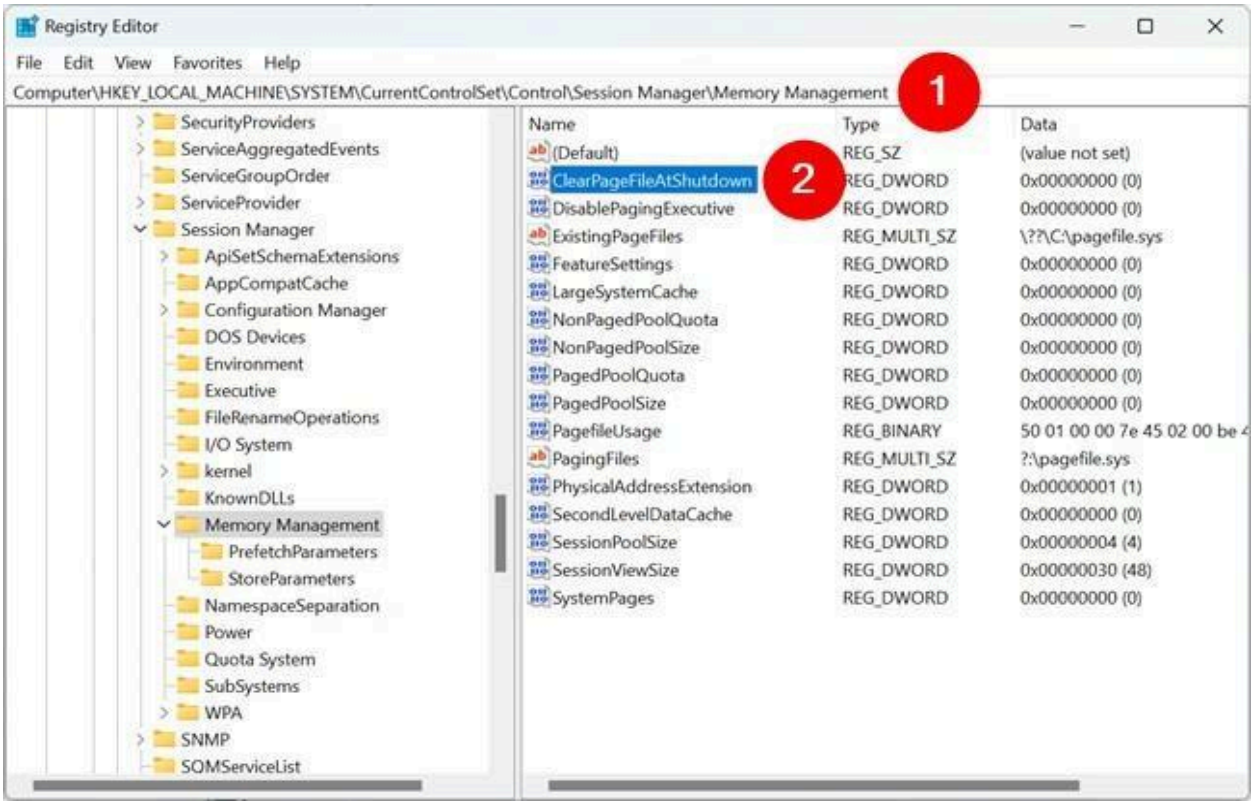
СОВЕТ: Если у вас нет большого опыта работы с *реестром Windows*, перед его изменением рекомендуется создать точку восстановления.
Учитывая все это, давайте посмотрим, как редактировать, создавать и удалять ключи и значения в *реестре Windows*:



2.8. Как редактировать реестр Windows

Чтобы отредактировать ключ или значение в *реестре Windows*, перейдите к его местоположению и дважды щелкните или дважды нажмите на его имя, чтобы перейти в режим редактирования. Для лучшего понимания рассмотрим следующий пример: вы хотите, чтобы ваш компьютер с Windows автоматически удалял файл виртуальной памяти (pagefile) каждый раз при выключении компьютера. Для этого необходимо изменить значение под названием *ClearPageFileAtShutDown* в *реестре Windows*. Название значения не так уж и загадочно, но путь к нему — да: чтобы добраться до него, необходимо открыть *редактор реестра* и перейти по пути:

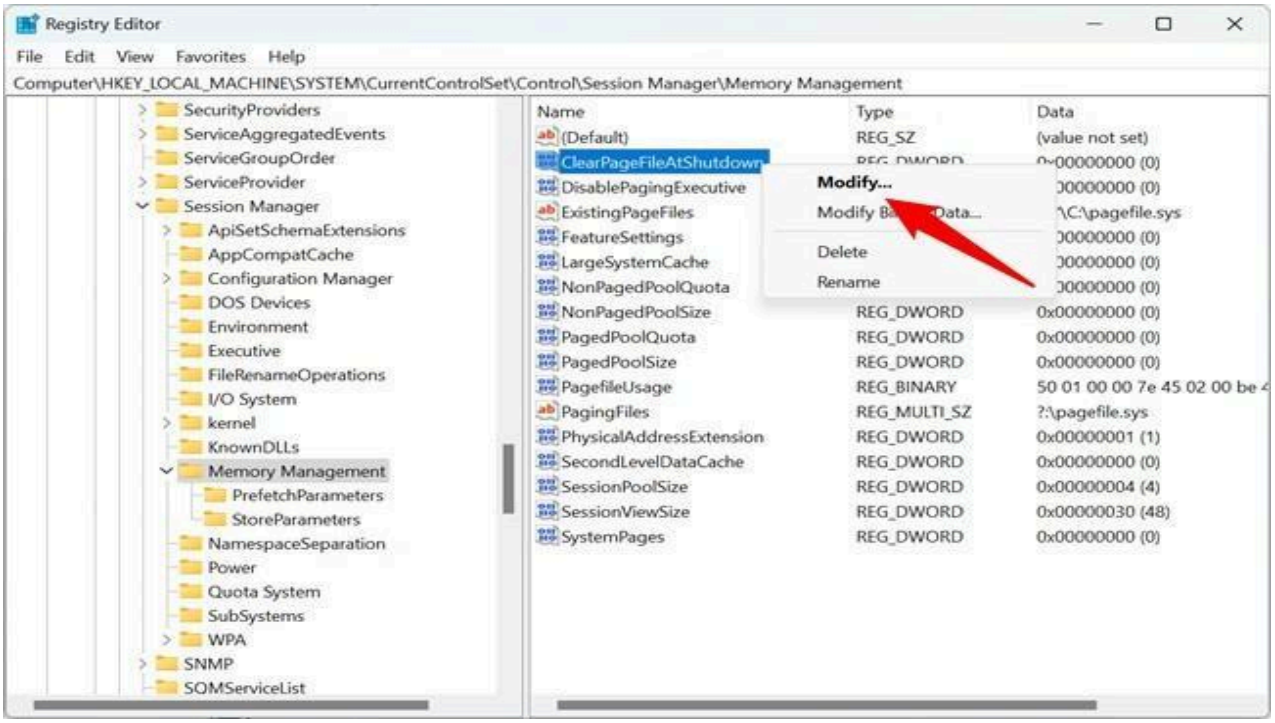
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management


Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
1
2
SecurityProviders
ServiceAggregatedEvents
ServiceGroupOrder
ServiceProvider
Session Manager
ApiSetSchemaExtensions
AppCompatCache
Configuration Manager
DOS Devices
Environment
Executive
FileRenameOperations
I/O System
kernel
KnownDLLs
Memory Management
PrefetchParameters
StoreParameters
NamespaceSeparation
Power
Quota System
SubSystems
WPA
SNMP
SOMServiceList
Name
Type
Data
(Default)
REG_SZ
(value not set)
ClearPageFileAtShutdown
REG_DWORD
0x00000000 (0)
DisablePagingExecutive
REG_DWORD
0x00000000 (0)
ExistingPageFiles
REG_MULTI_SZ
\??\C:\pagefile.sys
FeatureSettings
REG_DWORD
0x00000000 (0)
LargeSystemCache
REG_DWORD
0x00000000 (0)
NonPagedPoolQuota
REG_DWORD
0x00000000 (0)
NonPagedPoolSize
REG_DWORD
0x00000000 (0)
PagedPoolQuota
REG_DWORD
0x00000000 (0)
PagedPoolSize
REG_DWORD
0x00000000 (0)
PagefileUsage
REG_BINARY
50 01 00 00 7e 45 02 00 be
PagingFiles
REG_MULTI_SZ
?:\pagefile.sys
PhysicalAddressExtension
REG_DWORD
0x00000001 (1)
SecondLevelDataCache
REG_DWORD
0x00000000 (0)
SessionPoolSize
REG_DWORD
0x00000004 (4)
SessionViewSize
REG_DWORD
0x00000030 (48)
SystemPages
REG_DWORD
0x00000000 (0)

Поиск значения реестра в редакторе реестра

СОВЕТ: Если вы хотите узнать больше о навигации по *реестру Windows*, перейдите к этому руководству: Как перемещаться по реестру Windows.

Чтобы отредактировать значение, вы можете дважды щелкнуть по нему или щелкнуть правой кнопкой мыши и нажать *«Изменить» (Modify)*.



Изменение значения в редакторе реестра

Все, что вам нужно сделать, это ввести новое значение, которое вы хотите использовать. В данном случае 0 означает, что файл подкачки не удаляется при закрытии Windows 11, а 1 означает, что файл виртуальной памяти удаляется каждый раз, когда вы выключаете компьютер.

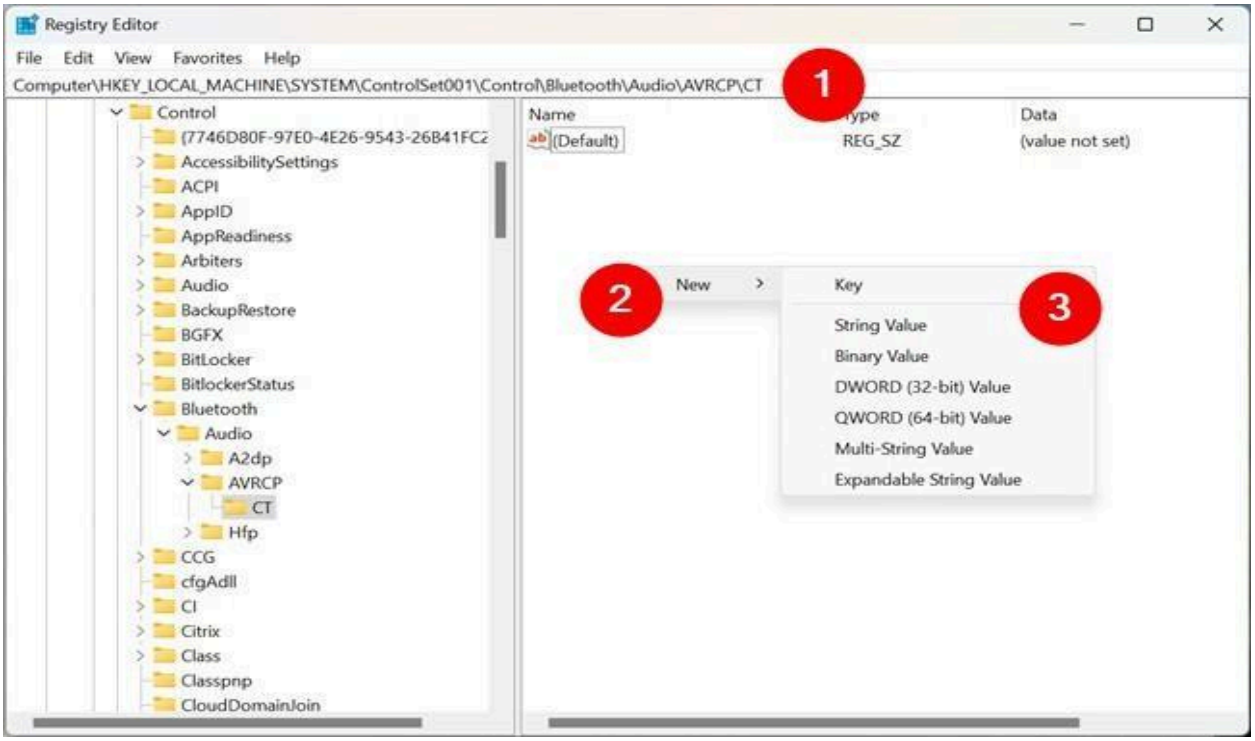
Ввод нового значения реестра

Нажмите клавишу *Enter* или кнопку *OK*, и новое значение будет установлено в *реестре Windows*. Чтобы оно вступило в силу, необходимо перезагрузить компьютер с Windows.

2.9. Как добавить ключи или значения в реестр Windows

Редактор реестра позволяет создавать новые ключи и значения, а также удалять существующие. Однако эти операции еще более сложны, чем редактирование того, что уже находится в *реестре Windows.* Поэтому я считаю необходимым еще раз предупредить вас: не приступайте к этим операциям, если не знаете, что делаете! В противном случае ваша система может перестать работать должным образом.

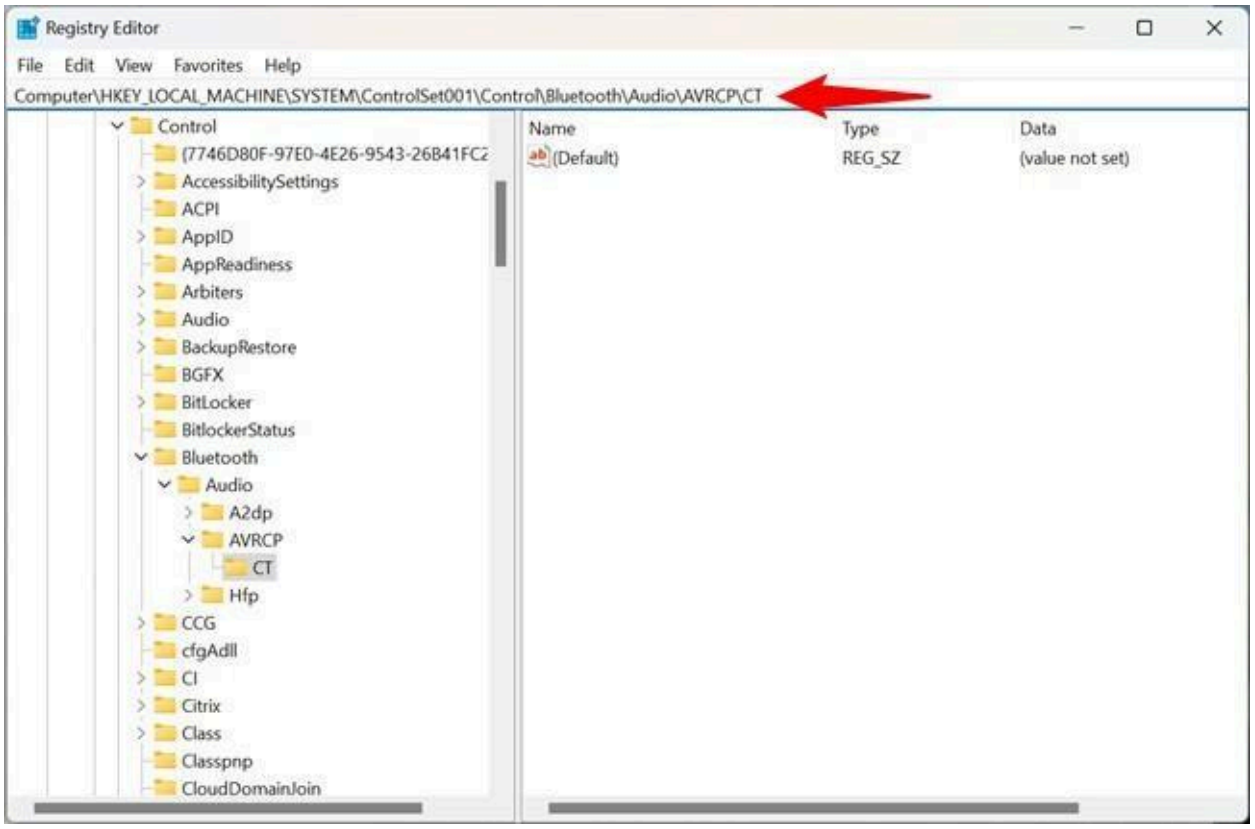
Если вы хотите создать новый ключ или значение, перейдите к тому месту в *реестре Windows*, где оно вам нужно. Затем щелкните правой кнопкой мыши или нажмите и удерживайте пустое место в правой панели окна. В контекстном меню выберите *«New» (Новый)* и выберите *«Key» (Ключ)* или тип значения (*Value)*, которое хотите создать.



Добавление ключа или значения в Registry Editotr

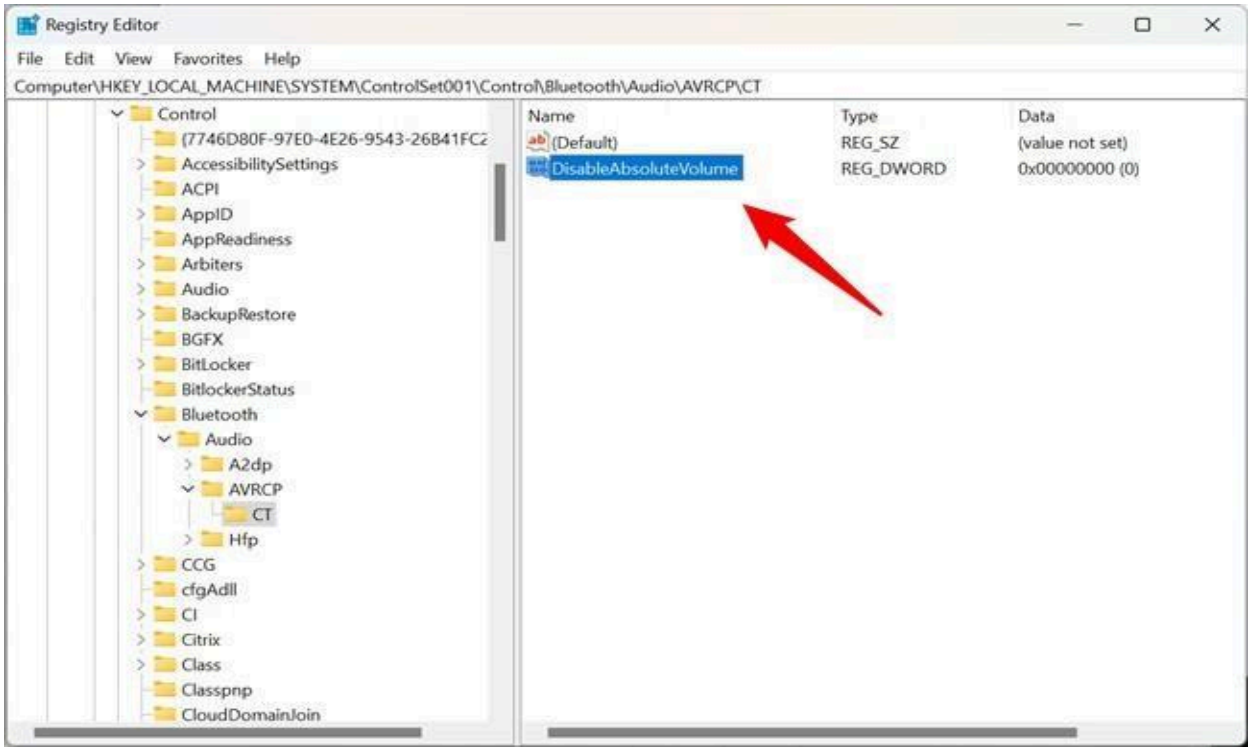
Например, я хотел отключить абсолютный объем Bluetooth на своем ПК с Windows 11, потому что мои динамики не работают с ним. Для этого мне пришлось использовать *реестр Windows*, чтобы сначала перейти в следующее место:

```
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Bluetooth\
Audio\AVRCP\CT
```



Переход к этому местоположению в редакторе реестра

Затем мне пришлось создать новое значение *DWORD (32-разрядное)*, названное *DisableAbsoluteVolume*.



Создание нового ключа в редакторе реестра

Чтобы этот ключ работал так, как я хотел, мне нужно было установить его значение на 1. Как упоминалось ранее, чтобы изменить значение, нужно дважды щелкнуть по нему (или выбрать *«Изменить»* в контекстном меню). Затем достаточно ввести новое значение и нажать *«ОК»*.

Ввод значения реестра

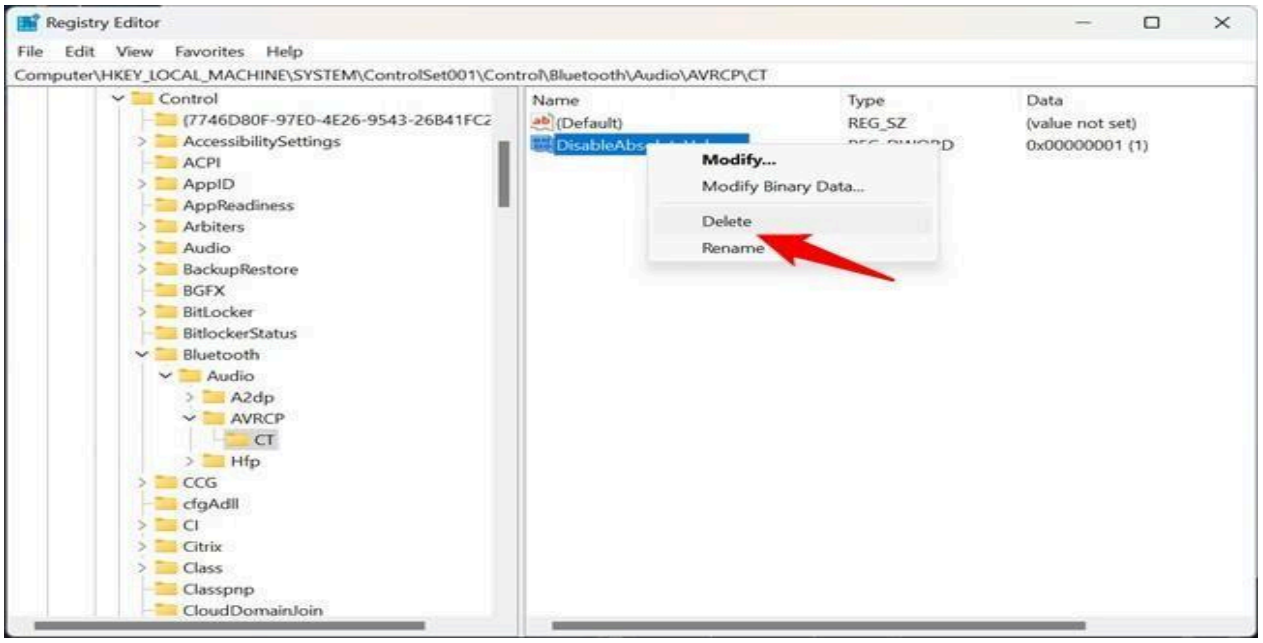
Перезагрузите компьютер, и Windows начнет использовать новый ключ/значение, который вы создали в *реестре*.

2.10. Как удалить ключ или значение из реестра Windows

Удаление ключа или значения из *реестра Windows* еще проще, чем его редактирование или создание. Все, что нужно сделать, это перейти к месту расположения ключа или значения, которое вы хотите удалить, щелкнуть правой кнопкой мыши или нажать и удерживать его имя, а затем выбрать *«Удалить»* в контекстном меню.

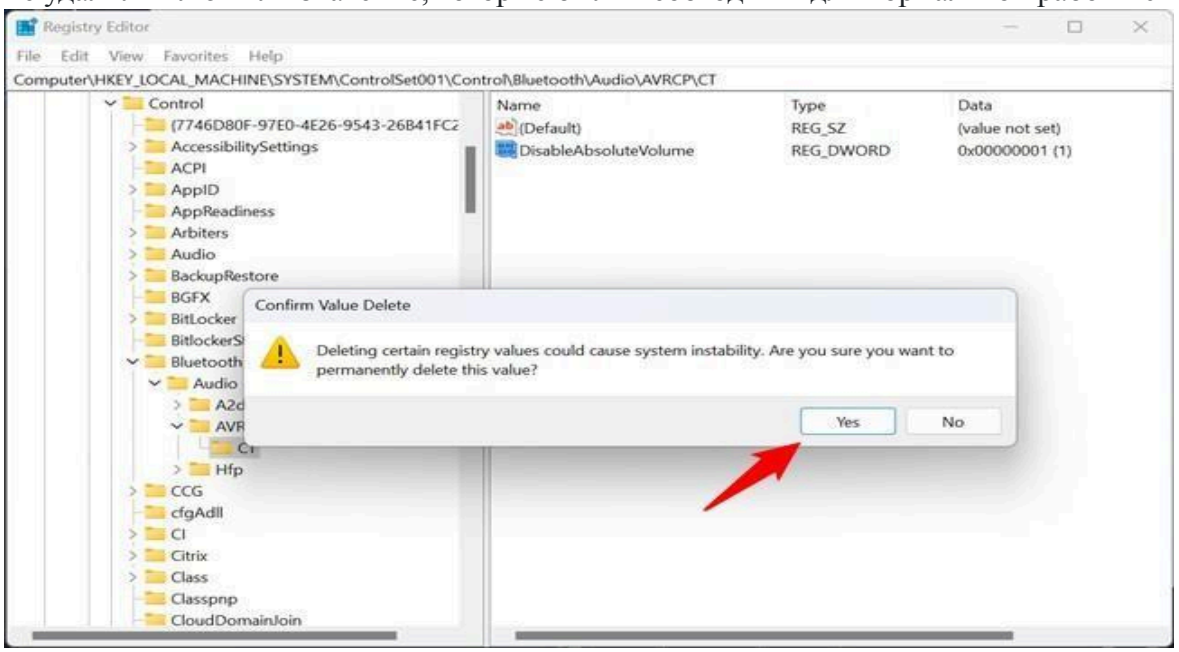
Удаление ключа или значения из реестра

Редактор реестра попросит вас подтвердить, что вы хотите удалить выбранный ключ или значение. Это подтверждение необходимо, поскольку, как указывает Windows, удаление определенных значений из реестра может привести к нестабильности системы — *«deleting certain registry values could cause system instability»*. Если вы уверены в своих действиях, нажмите *Yes (Да)*, чтобы окончательно удалить выбранный ключ или значение реестра.



Ключ или значение окончательно удаляется из реестра

Чтобы внести изменения в *peecmp Windows*, перезагрузите компьютер. Надеемся, вы не удалили ключ или значение, которые были необходимы для нормальной работы системы.



3. Файл подкачки в Windows 10: как настроить, увеличить, изменить и отключить

Файл подкачки — это дисковое пространство, используемое Windows для хранения временных данных, когда оперативной памяти недостаточно для обработки всех процессов, запущенных в системе. Правильная настройка и управление файлом подкачки может помочь улучшить производительность системы. Вот как можно настроить, увеличить, изменить и отключить файл подкачки в Windows 10:

1 Откройте «Панель управления» и перейдите в «Система и безопасность» > «Система» > «Настройка системы».

2 В открывшемся окне выберите вкладку «Дополнительно» и нажмите кнопку «Настройка» в разделе «Производительность».

3 В открывшемся окне «Параметры производительности» выберите вкладку «Дополнительно» и нажмите кнопку «Изменить» в разделе «Виртуальная память».

4 Снимите флажок «Автоматически управлять размером файла подкачки для всех дисков» и выберите диск, который хотите изменить.

5 Теперь у вас есть возможность изменить размеры файла подкачки. Вы можете выбрать опцию «Пользовательский размер», чтобы указать начальный и максимальный размер файла подкачки.

6 Чтобы отключить файл страницы, вы можете выбрать опцию «Без файла страницы» для соответствующего диска.

7 После внесения необходимых изменений нажмите «Настройка», а затем «ОК», чтобы сохранить настройки.

8 Таким образом, следуя этим шагам, вы можете настроить, увеличить, изменить и отключить файл подкачки в Windows 10 в соответствии с вашими потребностями. Это может помочь вам оптимизировать производительность компьютера и более эффективно управлять доступной памятью.

Таким образом, следуя этим шагам, вы можете настроить, увеличить, изменить и отключить файл подкачки в Windows 10 в соответствии с вашими потребностями. Это может помочь вам оптимизировать производительность компьютера и более эффективно управлять доступной памятью.

Важно помнить, что отключение файла подкачки может привести к нестабильной работе системы, если оперативной памяти недостаточно для обработки всех процессов. Если после отключения файла подкачки возникнут проблемы, вы можете вернуться к настройкам по умолчанию или настроить размер файла подкачки в соответствии с потребностями системы.

Лабораторная работа 3

Тема: Администрирование Windows

Цель лабораторной работы: Освоить методы и инструменты администрирования учетных записей пользователей и групп для эффективного управления безопасностью и ресурсами в операционной системе Windows. Изучить структуру и функции реестра Windows, а также методы его администрирования и изменения с целью настройки и оптимизации системы. Изучить роль и способ настройки файла подкачки (pagefile.sys) как механизма виртуальной памяти в Windows.

Цели лабораторной работы:

Для администрирования учетных записей пользователей и групп пользователей:

- Ознакомление с типами учетных записей пользователей и их ролью в Windows.
- Создание, изменение и удаление учетных записей пользователей.
- Управление паролями и связанными с ними политиками безопасности.
- Создание и администрирование групп пользователей.
- Распределение прав и разрешений через группы.
- Мониторинг активности и входа пользователей.

Для реестра Windows

- Ознакомление с понятием реестра и его ролью в Windows.
- Изучение структуры реестра (ульи, ключи, подключи, значения).
- Использование редактора реестра (*regedit*) для навигации и поиска.
- Изменение некоторых настроек системы через реестр.

Для файла страницы в Windows

- Понимание концепции виртуальной памяти и взаимосвязи между ОЗУ и файлом страницы.
- Определение и анализ настроек файла подкачки по умолчанию.
- Расчет рекомендуемого размера файла подкачки в зависимости от доступной оперативной памяти.
- Изменение размера и местоположения файла подкачки.
- Тестирование влияния на производительность системы в зависимости от настроек файла подкачки.

Практические задачи по: Управление учетными записями пользователей и группами пользователей.

1. **Создание новой учетной записи пользователя**
   - Создайте нового локального пользователя со стандартными правами (например, *Student1)*.
   - Установите пароль и настройте опцию, чтобы пользователь был обязан изменить его при первом входе в систему.
   - Создайте нового локального пользователя со стандартными правами (например, *Student2*).
2. **Изменение типа учетной записи**
   - Превратите ранее созданную учетную запись стандартного пользователя в учетную запись с правами администратора.
   - Удалите пользователя *Student2*.
3. **Управление паролями пользователей**
   - Установите сложный пароль для существующего пользователя.
   - Включите опцию периодического истечения срока действия пароля (например, через 30 дней).
4. **Создание и управление группами**
   - Создайте новую группу (например, *«Лаборатория»*).
   - Добавьте в эту группу двух существующих пользователей.
   - Проверьте их принадлежность к группе.
5. **Применение ограничений по группам**
   - Настройте ограничение (например, запрет на установку программ или изменение настроек).

- Проверьте разницу между пользователем, являющимся членом группы с ограничениями, и пользователем с правами администратора.

6. **Мониторинг и аудит деятельности пользователей**

- Откройте «Просмотр событий» и найдите события, связанные с входом/выходом пользователей.
- Сохраните отчет с этими событиями и сделайте выводы о важности мониторинга.

Практические задачи для: Реестр Windows.

7. Уровень 1:

- Чтение ключа реестра

Цель: Прочитать значение ключа реестра и отобразите ее в консоли.

Цель: научиться открывать и считывать ключи реестра.

- Создание нового ключа в реестре

Цель: Создать новый ключ и значений в разделе реестра.

Цель: научиться создавать ключи и добавлять данные

o изменение значения ключа реестра

Цель: найти существующий ключ и изменить его значение.

Цель: Научиться изменять настройки в реестре.

8. Уровень 2:

- Удаление ключа реестра

Цель: удалить определенный ключ реестра.

Цель: научиться безопасно удалять ключи и значения из реестра.

- Создание и управление параметром с несколькими значениями

Задача: Создайте параметр типа Multi-String и добавьте несколько значений.

Цель: Понять различные типы данных в реестре.

- Создание резервной копии раздела реестра

Задача: Создать экспорт (резервную копию) определенного раздела реестра.

Цель: Понять, как безопасно работать с реестром и создавать его резервные копии.

9. Уровень 3:

- Автоматизация изменений в реестре с помощью скрипта

Цель: Написать скрипт (например, в PowerShell или Python) для автоматического изменения определенных ключей реестра.

Цель: научиться автоматизировать работу с реестром с помощью скриптов.

- Работа с реестром с помощью службы Windows

Задача: Создание или изменение службы Windows путем изменения реестра.

Цель: научиться управлять службами Windows с помощью реестра.

- Изменение ключей регистра для программ автозагрузки

Задача: Добавление программы в автозагрузчик путем изменения реестра.

Цель: Понять, как управлять автозагрузкой приложений через реестр.

Практические задачи для: Файл страницы в Windows.

10. **Идентификация файла страницы**

- Включите отображение скрытых системных файлов и найдите `файл pagefile.sys` на системном диске.
- Запишите текущий размер файла.

11. **Проверка настроек виртуальной памяти по умолчанию**

- Перейдите в: *Свойства системы → Дополнительные параметры системы → Производительность → Настройки → Дополнительно → Виртуальная память*.
- Проанализируйте опцию «Автоматически управлять размером файла подкачки для всех дисков».

12. **Определение рекомендуемого размера файла подкачки**

- Используйте значение установленной оперативной памяти и сравните его с размером, рекомендованным Windows.
- Вручную рассчитайте минимальный и максимальный рекомендуемый размер (1,5x и 3x RAM).

13. **Изменение размера файла страницы**

- Отключите опцию автоматического управления и установите индивидуальный размер.
- Перезагрузка системы для применения изменения.

14. **Анализ влияния на производительность**

- Запустите приложение, которое потребляет много памяти (например, браузер с несколькими вкладками, приложение для редактирования фото/видео).
- Отслеживайте использование памяти и файла подкачки в *диспетчере задач* → *Производительность* → *Память*.

15. **Сравнительный анализ и выводы**

- Сравните поведение системы с исходным и измененным размером файла подкачки.
- Напишите вывод о роли и важности файла страницы для стабильности и производительности Windows.

Критерии оценки:

Для получения оценки 5-6 обязательны критерии 1, 2, 7, 10, 11.
Для получения оценки 7-8 обязательны критерии 3, 4, 8, 12, 13.
Для получения оценки 9-10 обязательны критерии 5, 6, 9, 14, 15.
Если использовался ИИ (искусственный интеллект), оценка снижается на 2 балла, только если студент дал объяснения в функциональности. В противном случае лабораторная работа не принимается.

Контрольные вопросы:

1. Управление учетными записями пользователей и группами пользователей в Windows

1. Какие типы учетных записей пользователей существуют в Windows и в чем их различия?
2. Какова роль групп пользователей и какие преимущества дает их использование?
3. Как можно изменить пароль пользователя в графическом интерфейсе и в командной строке?
4. В чем разница между правами стандартного пользователя и администратора?
5. Какие политики безопасности могут быть применены к учетным записям пользователей?
6. Как можно проверить активность пользователя (входы, выходы, неудачные попытки)?

Файл страницы в Windows

1. Что такое файл подкачки (pagefile.sys) и где он находится в системе?
2. В чем разница между оперативной памятью и виртуальной памятью?
3. Как установить рекомендуемый размер файла подкачки?
4. Что произойдет, если полностью отключить файл страницы?
5. Каковы преимущества и недостатки перемещения файла подкачки на другой раздел или диск?
6. Как можно отслеживать использование файла подкачки в Windows?

Реестр Windows

1. Что такое реестр Windows и какова его роль в работе системы?
2. Каковы основные компоненты (ульи) реестра и что они содержат?
3. Какие типы значений могут храниться в ключе реестра (например, REG_SZ, REG_DWORD и т. д.)?
4. Как запустить и использовать редактор реестра (*regedit*)?
5. Как экспортировать и импортировать ключ реестра?
6. Каковы риски неправильного изменения реестра и какие меры предосторожности следует принять?

Список рекомендуемой литературы:

1. С. Ţăpuş, А. Ţăpuş – *Операционные системы. Основные принципы и механизмы*, издательство Politehnica Press, Бухарест.
2. М. Патрашку – *Практическое руководство по использованию Windows 10*, издательство Pro Universitaria, 2019.
3. Г. Текучи, Д. Кэлушер – *Операционные системы и их администрирование*, издательство Matrix Rom, Бухарест.

4. Руководства и справочники Microsoft на румынском языке: https://support.microsoft.com/ro-ro.
5. А. А. Богданов – *Операционные системы. Практикум по администрированию Windows*, Москва: Издательство БХВ, 2020.
6. В. Г. Олифер, Н. А. Олифер – *Компьютерные сети. Принципы, технологии, протоколы* (главы об управлении учетными записями).
7. А. В. Горшков – *Windows 10. Полное руководство пользователя и администратора*, Санкт-Петербург: Питер, 2018.
8. Справка и документация Microsoft на русском: https://learn.microsoft.com/ru-ru/windows.
9. Брайан Книттель, Пол Макфедрис – *Windows 10 Inside Out*, Microsoft Press, 2021.
10. William R. Stanek – *Windows 10 Administration: The Complete Guide*, Stanek & Associates, 2020.
11. Mark Russinovich, David Solomon, Alex Ionescu – *Windows Internals, Part 1 and 2*, Microsoft Press, 7th Edition, 2021.
12. Microsoft Learn – Официальная документация: https://learn.microsoft.com/en-us/windows.