

Федеральное государственное автономное образовательное учреждение высшего
образования
«Национальный исследовательский университет ИТМО»
Факультет программной инженерии и компьютерной техники

Лабораторная работа 3
«Разграничение доступа к реестру»
по дисциплине
«Информационная безопасность»

Вариант № 49

Группа: Р34102

Выполнил: Лапин А.А.

Проверил:
Рыбаков С.Д.

Санкт-Петербург
2024г.

Оглавление

Оглавление	2
Цель работы	3
Программно-аппаратные средства, используемые при выполнении работы	4
Основная часть	5
1 Рассмотрим основные ветви реестра и типичный уровень доступа к ним:	6
2 Способы восстановления реестра	10
3 Настройка службы Superfetch: включение механизма Prefetcher только для загрузки системы.	16
4 Увеличение скорости выключения компьютера.	17
5 Деактивация клавиши Win.	19
Заключение	21

Цель работы

Целью данной лабораторной работы является изучение структуры системного реестра Windows, принципов разграничения доступа к его ключам и ветвям, а также приобретение практических навыков по настройке и восстановлению реестра. В ходе работы также рассматриваются методы настройки системы путём изменения параметров реестра, что позволяет более детально настроить параметры системы.

Программно-аппаратные средства, используемые при выполнении работы

Для выполнения работы было использовано ПО Parallels Desktop.

Характеристики созданной виртуальной машины:

8BC1
Parallels ARM Virtual Machine

Переименовать этот ПК

Характеристики устройства

Копировать

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

Ссылки по теме

Домен или рабочая группа

Защита системы

Дополнительные параметры системы

Характеристики Windows

Копировать

Выпуск

Windows 11 Pro

Версия

23H2

Дата установки

16.03.2024

Сборка ОС

22631.3374

Взаимодействие

Windows Feature Experience Pack 1000.22688.1000.0

Соглашение об использовании служб Майкрософт

Условия лицензионного соглашения на использование программного обеспечения корпорации Майкрософт

Активация Windows

Чтобы активировать Windows, перейдите в раздел "Параметры".

Рис. 1: Характеристики системы

Основная часть

Открыть реестр можно несколькими способами.

Способ 1: Использование поиска в Windows

- Нажмите на кнопку «Пуск» (или нажмите клавишу Win на клавиатуре).
- В строке поиска введите «реестр» или «редактор реестра».
- В результатах поиска появится приложение «Редактор реестра» (Regedit).
- Нажмите на него, чтобы открыть.

Способ 2: Использование команды «Выполнить»

- Нажмите сочетание клавиш Win + R, чтобы открыть окно «Выполнить».
- Введите команду: `regedit`
- Нажмите Enter или кнопку «ОК».

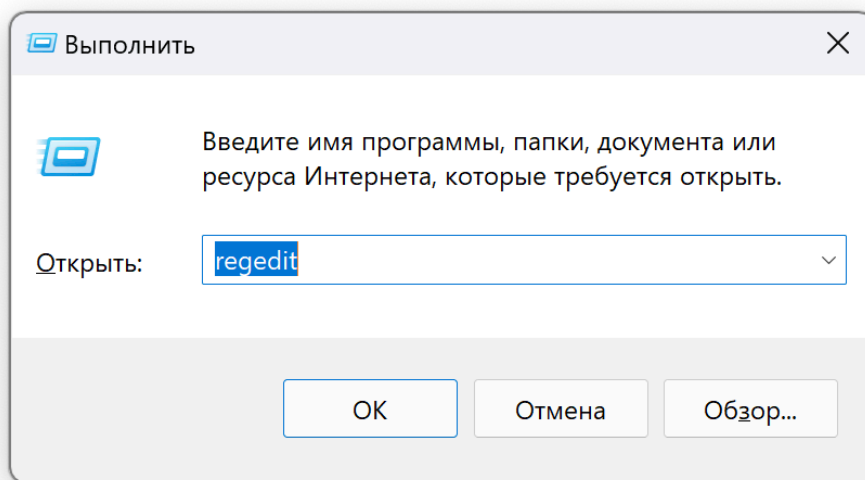


Рис. 2: Выполнение команды

Способ 3: Использование PowerShell или CMD

- Откройте PowerShell или командную строку (CMD)
- Введите команду: `regedit`
- Нажмите Enter.

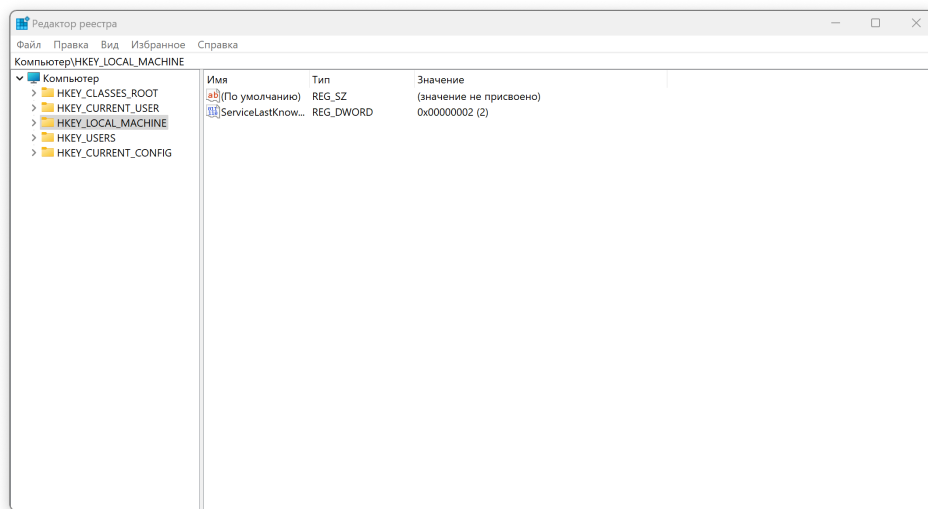


Рис. 3: Системный реестр

В операционной системе Windows 10 доступ к разделам и ключам системного реестра регулируется с помощью списков контроля доступа (ACL), определяющих права различных учетных записей и групп. Основные учетные записи, участвующие в управлении реестром, включают:

- **SYSTEM:** системная учетная запись, обладающая максимальными привилегиями.
- **Администраторы:** группа пользователей с правами администратора.
- **Пользователи:** стандартные учетные записи без административных привилегий.

1 Рассмотрим основные ветви реестра и типичный уровень доступа к ним:

1. **HKEY_CURRENT_USER:** Это ссылка на определённый подраздел HKEY_USERS. Хранит настройки текущего пользователя.

Права доступа

SYSTEM: полный доступ.

Администраторы: полный доступ.

Пользователи: полный доступ.

- Содержит настройки, специфичные для текущего пользователя.
- Разберем некоторые из «кустов»:
 - **Software** — настройки программ, установленных для текущего пользователя.

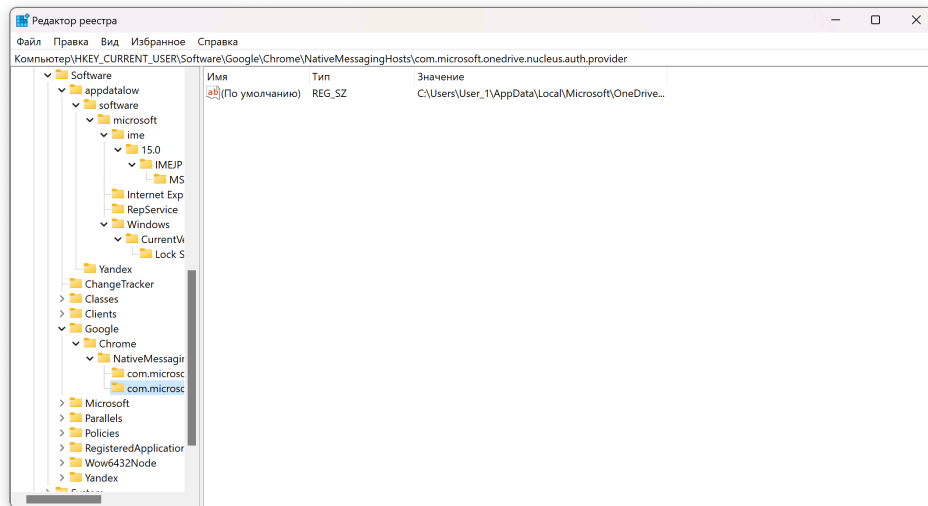


Рис. 4: Настройки программ

– **Control Panel** — параметры системы.

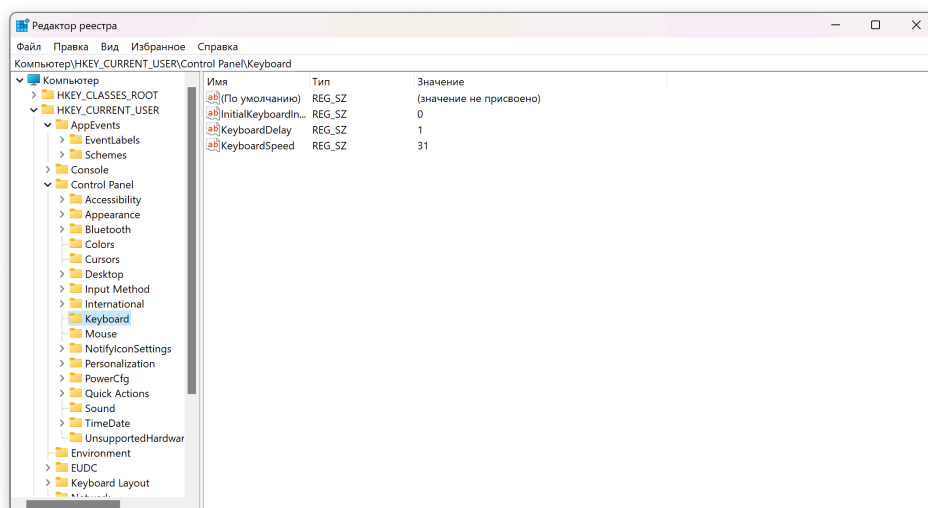


Рис. 5: Панель управления

– **Environment** — переменные среды, специфичные для пользователя.

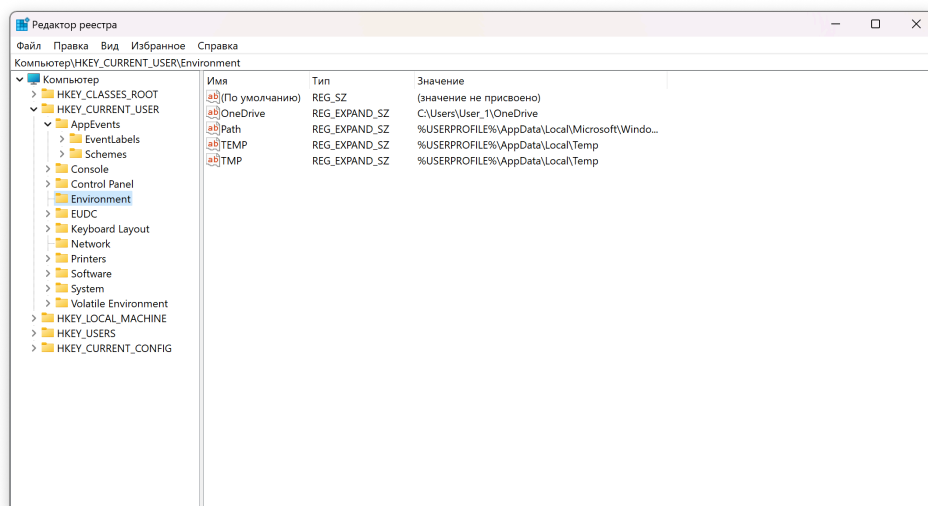


Рис. 6: Переменные среды

- Вот так можно изменять значения в реестре от имени обычного пользователя:

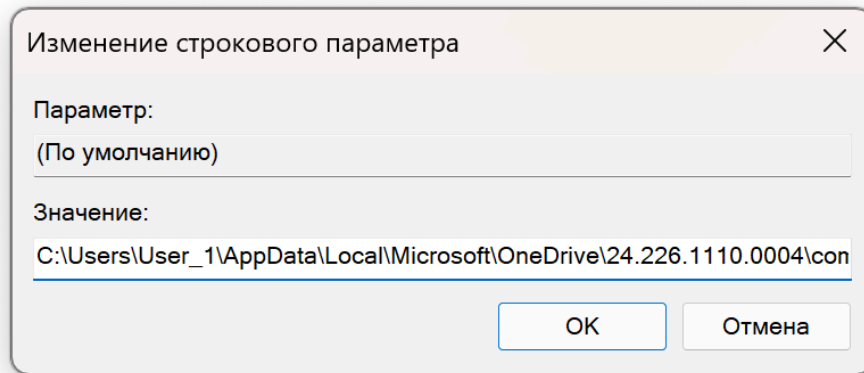


Рис. 7: Изменение значения

2. **HKEY_LOCAL_MACHINE**: Раздел содержит настройки, относящиеся к вашему компьютеру и действительны для всех пользователей. Раздел содержит информацию об аппаратной конфигурации и установленном программном обеспечении.

Права доступа

SYSTEM: полный доступ.

Администраторы: частичный доступ.

Пользователи: большинство доступно для чтения, есть недоступные разделы, есть разделы с полным доступом.

- Разберем некоторые из «кустов»:
 - **Software** — глобальные настройки программ.
 - **System** — настройки текущей конфигурации системы.
 - **Hardware** — описание аппаратного обеспечения (динамическая ветка, создается при запросе).
 - **SAM** — данные о пользователях и группах (Security Accounts Manager). Недоступна для обычных пользователей.
 - **Security** — политики безопасности. Недоступна для обычных пользователей.
- Отказ в доступе пользователю:

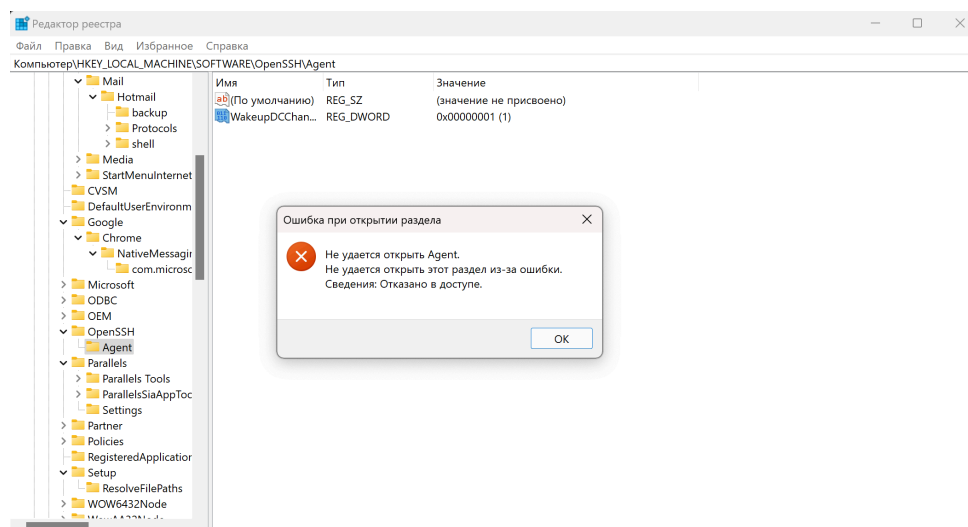


Рис. 8: Отказ в доступе в OpenSSH/Agent

- Отказ на редактирование администратору:

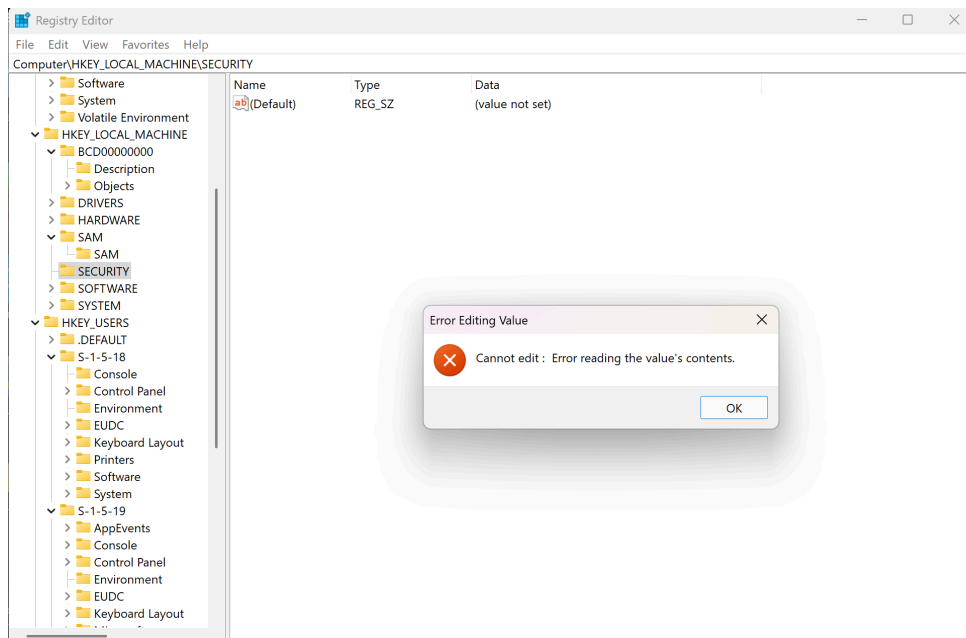


Рис. 9: Отказ на редактирование Security

3. **HKEY_USERS:** Этот раздел содержит настройки для всех пользователей компьютера

Права доступа

SYSTEM: полный доступ.

Администраторы: полный доступ.

Пользователи: Пользователь может просматривать только данные соответствующие его SID.

4. **HKEY_CURRENT_CONFIG:** Это ссылка на HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Hardware Profiles\Current. Раздел содержит сведения о настройках оборудования, используемом локальным компьютером при запуске системы, т.е. содержит информацию о текущей конфигурации.

Права доступа

SYSTEM: полный доступ.

Администраторы: полный доступ.

Пользователи: чтение.

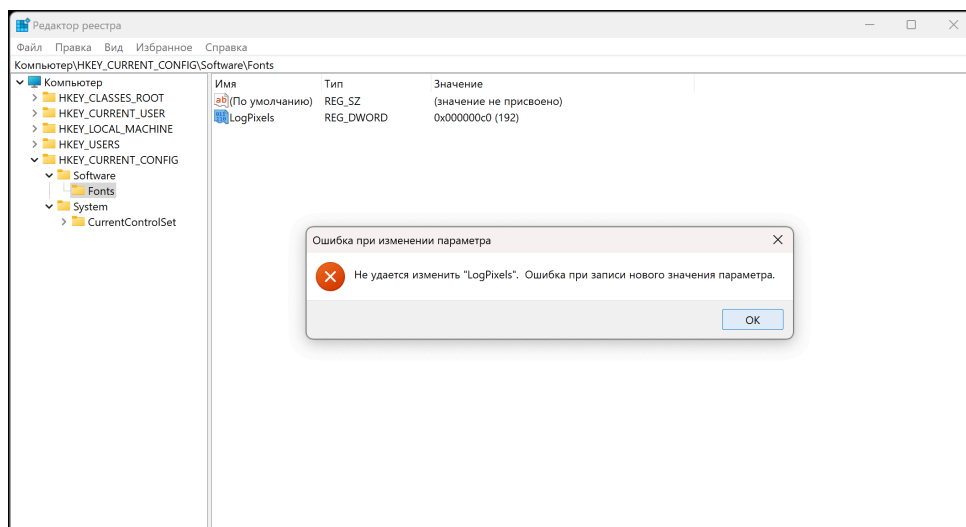


Рис. 10: Обычному пользователю доступно только чтение

5. **HKEY_CLASSES_ROOT:** Отображает данные из HKEY_LOCAL_MACHINE\Software\Classes и HKEY_CURRENT_USER\Software\Classes. Хранящиеся здесь сведения обеспечивают запуск необ-

ходимой программы при открытии файла с помощью проводника. Этот раздел содержит связи между приложениями и типами файлов, а также информацию об OLE.

Права доступа

SYSTEM: полный доступ.

Администраторы: полный доступ.

Пользователи: чтение.

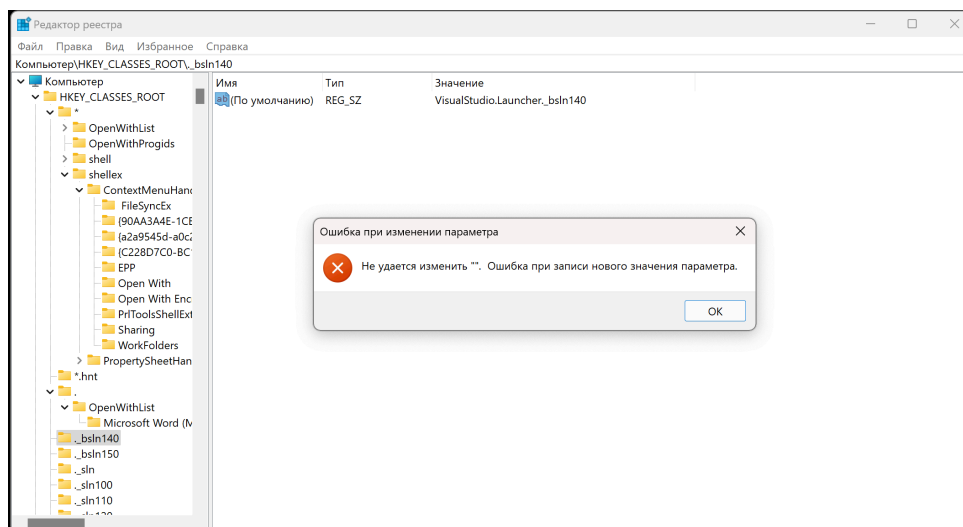


Рис. 11: Обычному пользователю доступно только чтение

2 Способы восстановления реестра

1. Восстановление реестра из резервной копии

- (a) Автоматически созданная резервная копия. Windows автоматически создает резервные копии реестра в папке `C:\Windows\System32\config\RegBack`. Эти файлы обновляются после каждого значительного обновления системы. Для восстановления реестра из резервной копии необходимо скопировать файлы из папки `RegBack` в папку `config`.

Шаги:

- i. Откройте командную строку.
- ii. Введите команду:

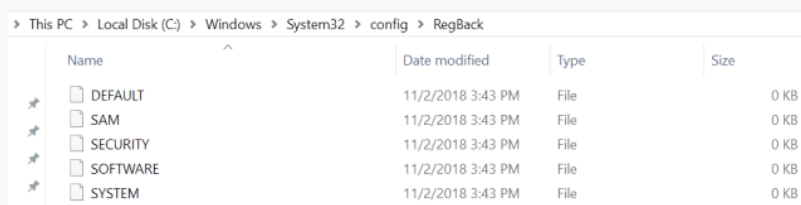
```
xcopy c:\windows\system32\config\regback c:\windows\system32\config
```

- iii. Подтвердите замену файлов, введя `A`.
- iv. Перезагрузите компьютер.

Важно: Начиная с Windows 10 версии 1803, автоматическое создание резервных копий реестра отключено по умолчанию. В таком случае папка `RegBack` может быть пуста или содержать нулевые файлы.

Резервное копирование системного реестра в папку RegBack перестало выполняться в Windows 10 версии 1803

Начиная с Windows 10, версия 1803, Windows больше не выполняет автоматическое резервное копирование системного реестра в папку RegBack. Если вы перейдете в папку \Windows\System32\config\RegBack в проводнике Windows, вы по-прежнему увидите все ветки реестра, но каждый файл будет иметь размер 0 кб.



Name	Date modified	Type	Size
DEFAULT	11/2/2018 3:43 PM	File	0 KB
SAM	11/2/2018 3:43 PM	File	0 KB
SECURITY	11/2/2018 3:43 PM	File	0 KB
SOFTWARE	11/2/2018 3:43 PM	File	0 KB
SYSTEM	11/2/2018 3:43 PM	File	0 KB

Рис. 12: Резервная копия реестра

Это изменение сделано специально и призвано помочь уменьшить общий размер дискового пространства Windows. Для восстановления системы с поврежденной веткой реестра Microsoft рекомендует использовать точку восстановления системы.

Если вам приходится использовать устаревшее поведение резервного копирования, вы можете включить его, настроив следующую запись реестра и перезагрузив компьютер:

- Path: HKLM\System\CurrentControlSet\Control\Session Manager\Configuration Manager\EnablePeriodicBackup
- Type: REG_DWORD
- Value: 1

Windows создает резервную копию реестра в папку RegBack при перезагрузке компьютера и задачу RegIdleBackup для управления последующими резервными копиями. Windows хранит информацию о задаче в библиотеке запланированных задач в папке Microsoft\Windows\Registry. Задача имеет следующие свойства:

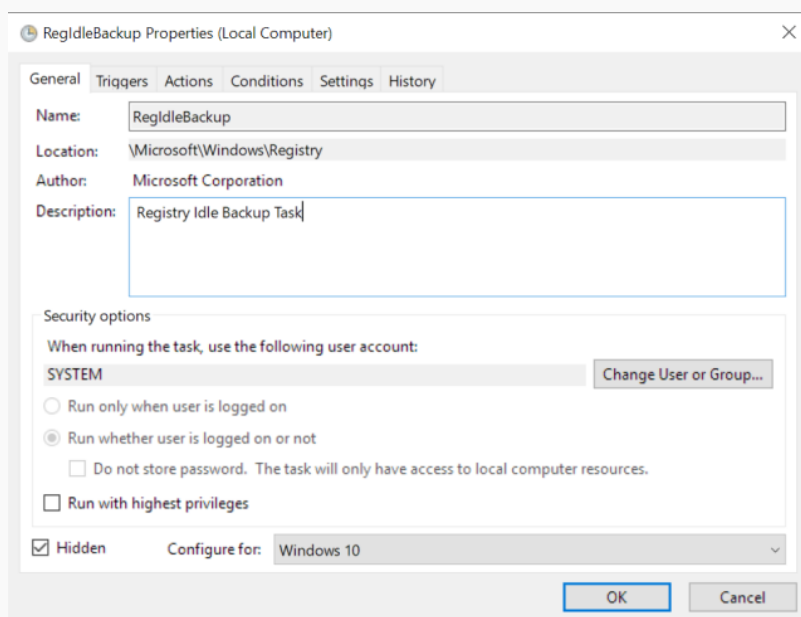


Рис. 13: Задача RegIdleBackup

(b) Создание собственной резервной копии.

Пользователь может создать резервную копию реестра вручную, чтобы использовать её в будущем.

Шаги:

- i. Откройте редактор реестра (regedit).
- ii. Выберите корневой раздел Компьютер.
- iii. Выберите в меню Файл пункт Экспорт.

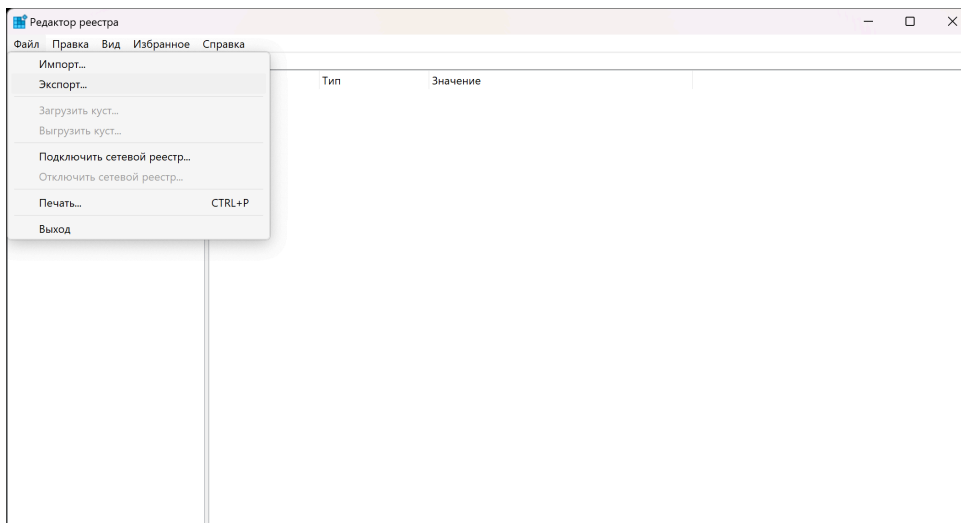


Рис. 14: Экспорт реестра

- iv. Для восстановления достаточно дважды кликнуть по файлу .reg и подтвердить внесение изменений.

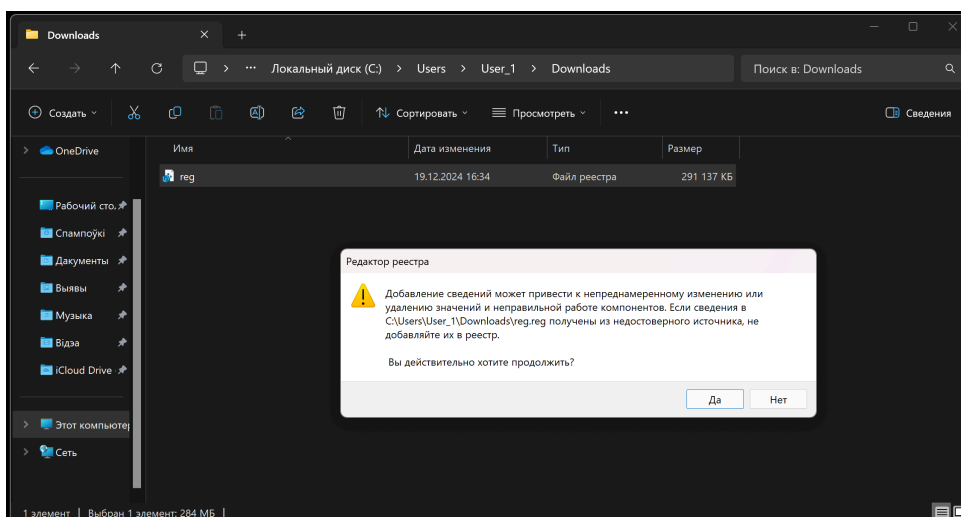


Рис. 15: Восстановление реестра

2. Использование утилиты SFC

Утилита SFC (System File Checker) позволяет восстановить поврежденные системные файлы, включая файлы реестра.

Шаги:

- (a) Откройте командную строку с правами администратора.
- (b) Введите команду:

```
sfc /scannow
```

- (c) Подождите, пока система проверит и восстановит поврежденные файлы.

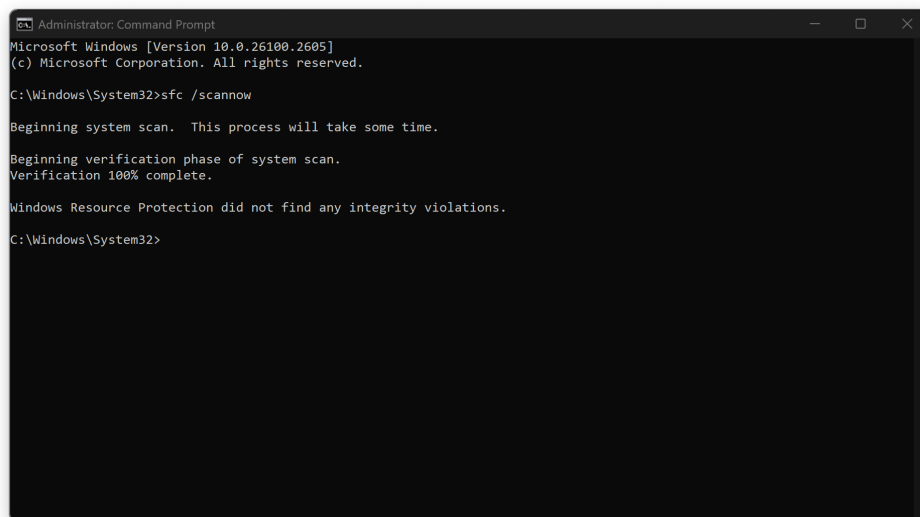


Рис. 16: Использование утилиты SFC

3. Восстановление через точки восстановления

Точки восстановления создаются системой автоматически или вручную и содержат резервные копии системных файлов, включая реестр.

Примечание: Функция точек восстановления может быть отключена по умолчанию.

Шаги:

- (a) Откройте Свойства системы, выберите Настройка параметров восстановления.

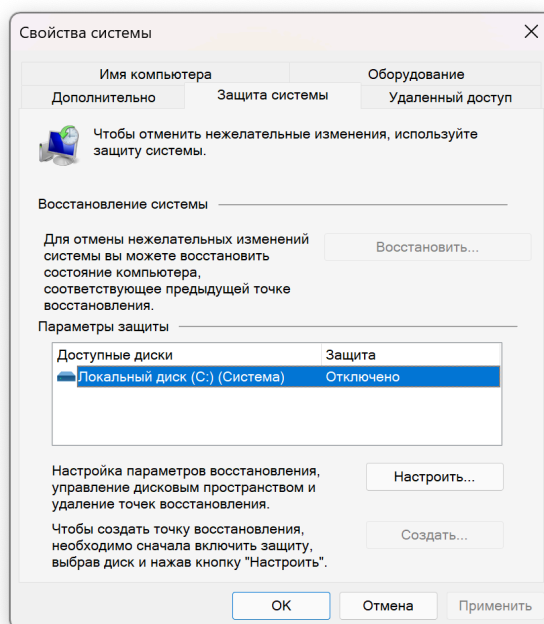


Рис. 17: Свойства системы

- (b) Включите защиту системы.

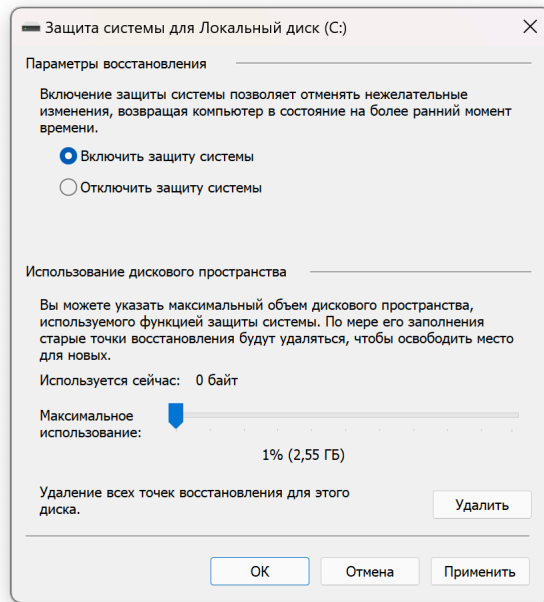


Рис. 18: Включение защиты системы

- (с) Нажмите на «Создать точку восстановления для дисков с включенной функцией защиты системы.»
- (d) Создайте точку восстановления.

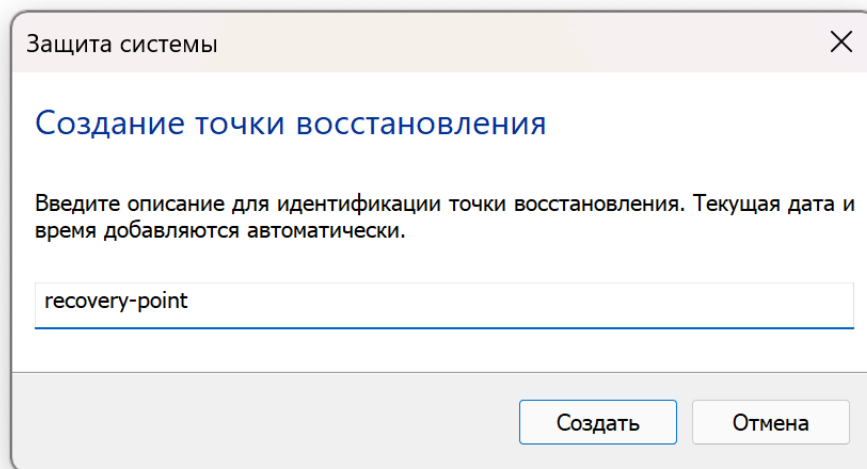


Рис. 19: Создание точки восстановления

- (е) После успешного создания точки восстановления, появится кнопка Восстановить. Нажмите на нее и выберите точку восстановления.

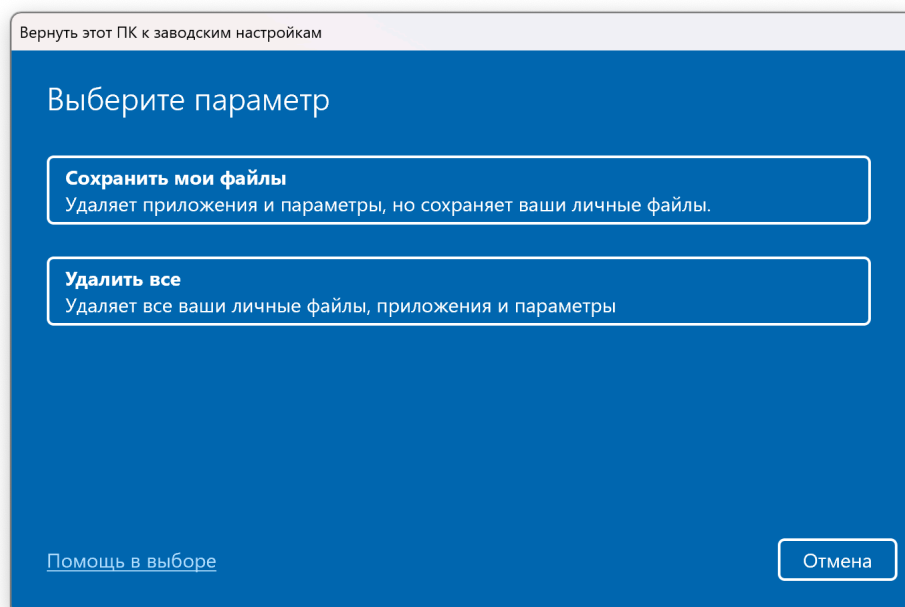


Рис. 22: Восстановление через сброс системы

Примечание: Этот метод удаляет все пользовательские программы и настройки, но сохраняет личные файлы.

3 Настройка службы Superfetch: включение механизма Prefetcher только для загрузки системы.

Superfetch анализирует ваш рабочий процесс и предзагружает часто используемые приложения и данные в оперативную память, чтобы ускорить доступ к ним.

Однако, на современных компьютерах данная функция не особо нужна, более того, для твердотельных дисков SSD SuperFetch и PreFetch рекомендуется отключить.

Шаги для настройки Prefetcher только для загрузки системы:

1. Откройте редактор реестра:
2. Нажмите Win + R, чтобы открыть окно «Выполнить».
3. Введите regedit и нажмите Enter.
4. Перейдите к ключу реестра:
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
5. Найдите параметр EnablePrefetcher:
 - В правой части окна найдите параметр EnablePrefetcher.
 - Если его нет, создайте его:
 - (a) Щелкните правой кнопкой мыши на пустом пространстве в правой части окна.
 - (b) Выберите Создать > DWORD (32-разрядный) значение.
 - (c) Назовите его EnablePrefetcher.
6. Измените значение EnablePrefetcher:
 - Дважды щелкните на EnablePrefetcher.
 - Установите значение в зависимости от ваших потребностей:
 - 0 - Prefetcher отключен.

- 1 - Prefetcher включен только для загрузки системы.
- 2 - Prefetcher включен только для загрузки приложений.
- 3 - Prefetcher включен для загрузки системы и приложений (режим по умолчанию).
- **Примечание:** Для редактирования реестра необходимо иметь права администратора.
- Для нашего случая необходимо установить значение 1.

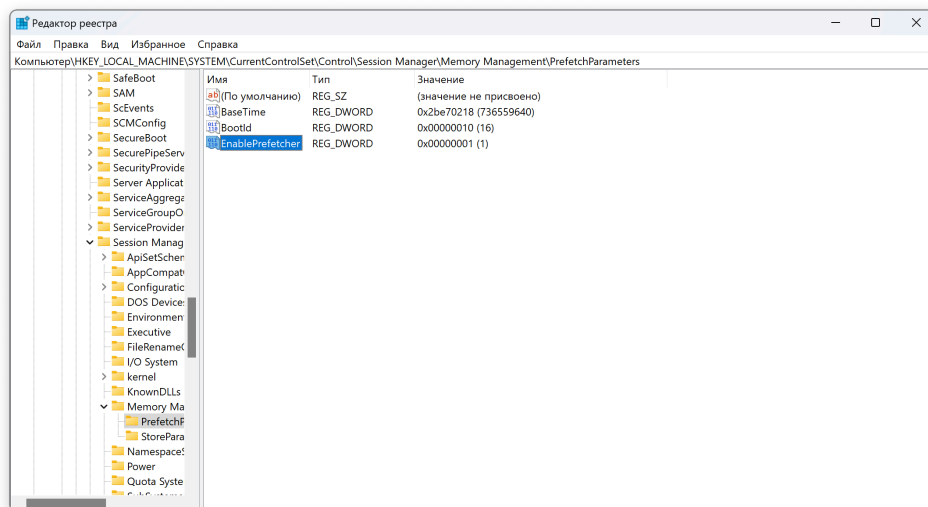


Рис. 23: Настройка Prefetcher

7. Примените изменения:

- Нажмите ОК, чтобы сохранить изменения.
- Закройте редактор реестра.

8. Перезагрузите систему:

- Перезагрузите компьютер, чтобы изменения вступили в силу.

4 Увеличение скорости выключения компьютера.

Шаги для увеличения скорости выключения:

1. Откройте Редактор реестра:

- Win + R, чтобы открыть окно «Выполнить».
- Введите regedit и нажмите Enter.

2. Перейдите к нужному разделу реестра:

- В редакторе реестра перейдите по следующему пути:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

3. Найдите параметр «WaitToKillServiceTimeout»:

- В правой части окна найдите параметр с именем WaitToKillServiceTimeout.
- Если этого параметра нет, вы можете создать его:
 - (a) Щелкните правой кнопкой мыши на пустом пространстве в правой части окна.
 - (b) Выберите Создать > Строковое значение.
 - (c) Назовите его WaitToKillServiceTimeout.

4. Измените значение параметра:

- Дважды щелкните на WaitToKillServiceTimeout.

- По умолчанию значение может быть установлено на 5000 (5 секунд). Вы можете уменьшить это значение, например, до 1000 (1 секунды).
- Введите новое значение и нажмите ОК.

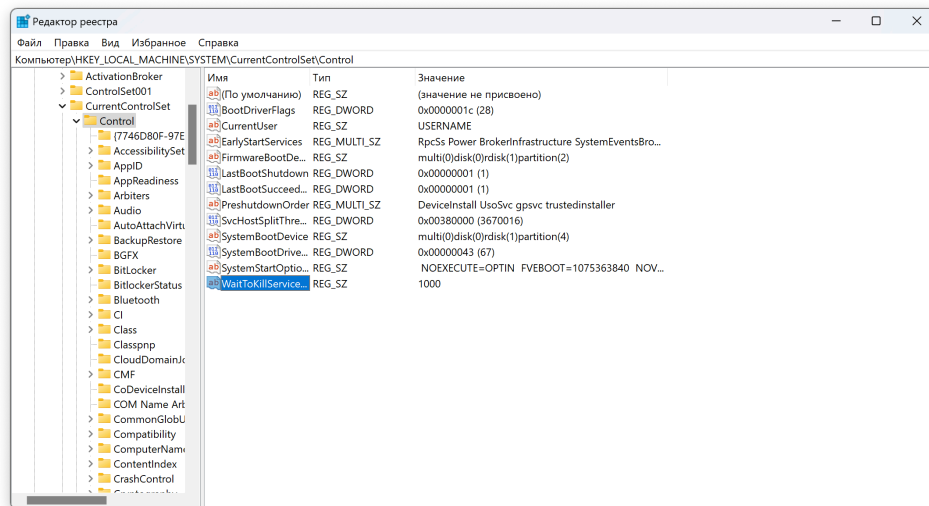


Рис. 24: Настройка скорости выключения

- **Примечание:** Для редактирования реестра необходимо иметь права администратора.
5. Также ускорить выключение можно, выключив отчиску файла подкачки.
- Перейдите к ключу реестра:
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
 - Найдите параметр ClearPageFileAtShutdown.
 - В правой части окна находится параметр ClearPageFileAtShutdown.
 - Если его нет, создайте его:
 - Щелкните правой кнопкой мыши на пустом пространстве в правой части окна.
 - Выберите Создать > DWORD (32-разрядный) значение.
 - Назовите его ClearPageFileAtShutdown.
 - Измените значение ClearPageFileAtShutdown:
 - Дважды щелкните на ClearPageFileAtShutdown.
 - Установите значение в 0.

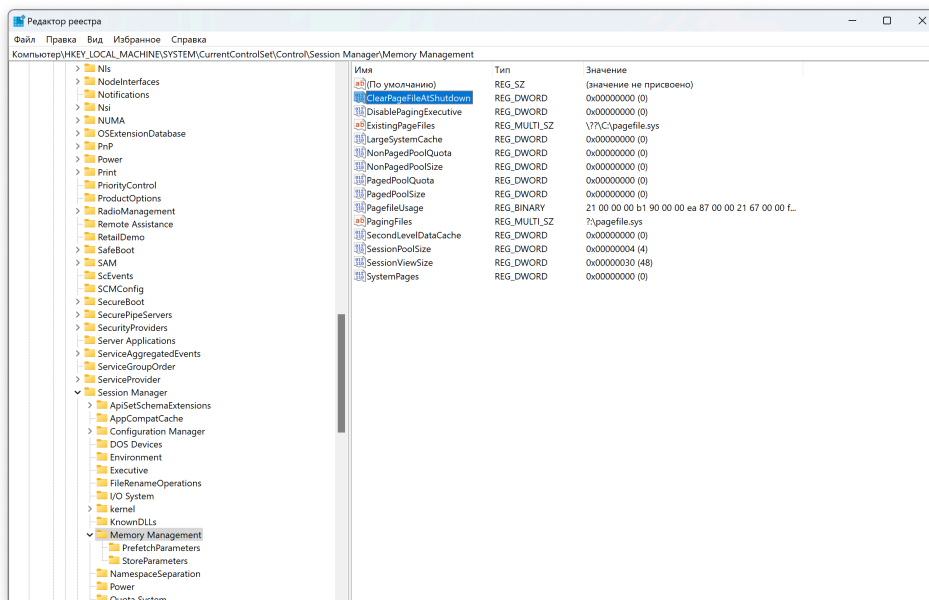


Рис. 25: Настройка скорости выключения

– **Примечание:** Для редактирования реестра необходимо иметь права администратора.

6. Перезагрузите компьютер:

- После внесения изменений перезагрузите компьютер, чтобы изменения вступили в силу.

5 Деактивация клавиши Win.

Шаги для деактивации клавиши Win через реестр:

1. Откройте Редактор реестра:

- Win + R, чтобы открыть окно «Выполнить».
- Введите regedit и нажмите Enter.

2. Перейдите к нужному разделу реестра:

- В редакторе реестра перейдите по следующему пути:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout

3. Создать новый бинарный ключ:

- В правой части окна найдите пустое пространство и щелкните правой кнопкой мыши.
- Выберите Создать > Двоичное значение.
- Назовите его Scancode Map.

4. Изменить значение ключа:

- Дважды щелкните на созданном ключе Scancode Map.
- Введите следующее значение:

1	00 00 00 00 00 00 00 00
2	03 00 00 00 00 00 5B E0
3	00 00 5C E0 00 00 00 00

- Это значение отключает клавишу Win.

Заключение

В ходе выполнения лабораторной работы были изучены основные ветви системного реестра Windows, их структура, права доступа и способы управления ими. Были рассмотрены различные методы открытия редактора реестра, а также изучены основные учетные записи и группы, участвующие в управлении доступом к реестру.

Кроме того, были рассмотрены способы восстановления реестра, включая использование резервных копий, утилиты SFC, точек восстановления системы и сброса системы. Эти методы позволяют эффективно восстановить работоспособность системы в случае повреждения реестра.

Также были выполнены практические задания по настройке системы через реестр, такие как включение механизма Prefetcher только для загрузки системы, увеличение скорости выключения компьютера и деактивация клавиши Win. Эти настройки демонстрируют возможности реестра в настройке работы операционной системы Windows.

Таким образом, работа позволила не только изучить структуру реестра, но и приобрести практические навыки по настройке системы с его помощью.