

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

ФАКУЛЬТЕТ ПРОГРАММНОЙ ИНЖЕНЕРИИ И КОМПЬЮТЕРНОЙ ТЕХНИКИ

НАПРАВЛЕНИЕ ПРОГРАММНАЯ ИНЖЕНЕРИЯ

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА СИСТЕМНОЕ И ПРИКЛАДНОЕ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

СПЕЦИАЛИЗАЦИЯ СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 3 (Windows)

курса «Информационная безопасность»

по теме: «Разграничение доступа к реестру»

Вариант № 23

Выполнил студент:

Тюрин И.Н.

группа: Р33102

Преподаватель:

Маркина Т.А.,

Рыбаков С.Д.

Санкт-Петербург, 2025 г.

Содержание

Лабораторная работа № 3 (Windows). Разграничение доступа к реестру	2
1. Описание	2
2. Выполнение задания	3
1. Доступ к веткам и ключам	3
2. Способы восстановления системы	6
3. Задание по варианту	11
3. Вывод	15

Лабораторная работа № 3 (Windows)

Разграничение доступа к реестру

1. Описание

Цель работы: Изучить объекты реестра, ознакомиться с основными принципами управления доступом к объектам реестра. Изучить основные способы настройки доступа к реестру.

Основная часть

1. Какие конкретно ветки и ключи доступны (в отчёте: перечислите их названия):
 - (а) Пользователю хотя бы на чтение;
 - (б) только Администратору;
 - (с) только System.
2. Опишите в отчете способы восстановления реестра (для нечетных вариантов) (в отчете: подробное описание выполнения задания со скриншотами).
3. Данное задание выполняется исходя из варианта. Укажите ключ, который отвечает за указанный параметр системы

Задание варианта № 23:

- Создание псевдонимов к программам.
- Отсутствие разрыва связи при выходе из системы.
- Автоматическое удаление временных файлов после работы в Интернет.

2. Выполнение задания

Для выполнения работы использовалась виртуальная машина VirtualBox с установленной в нее операционной системой Windows 10 Pro N 22H2.

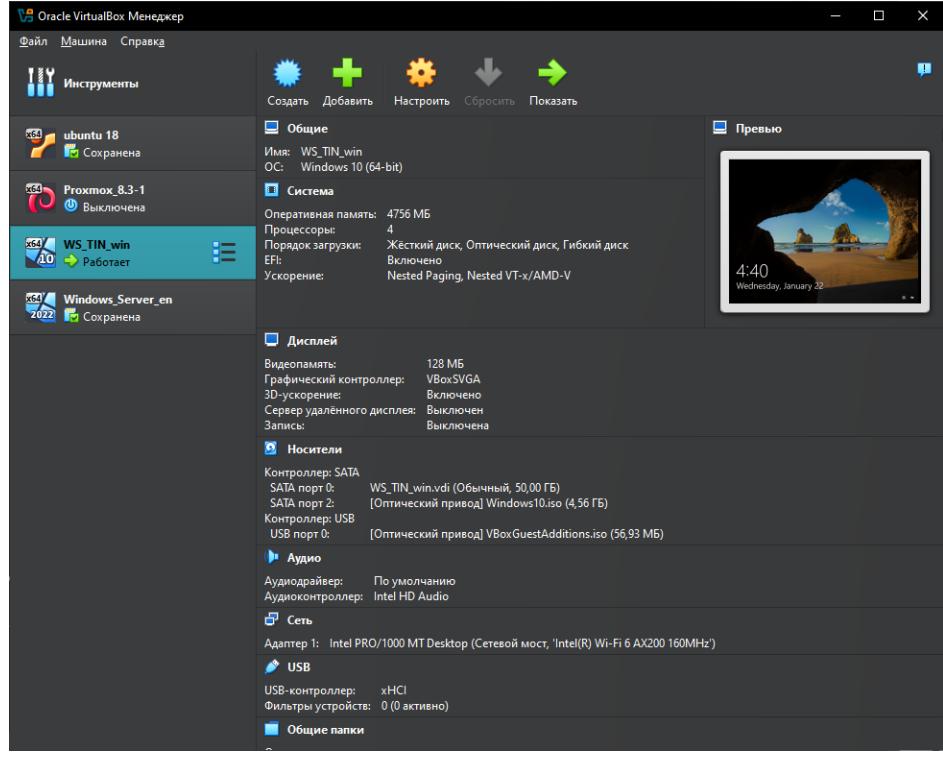


Рис. 1.1: Экспериментальное окружение

2. 1. Доступ к веткам и ключам

Доступ к реестру Windows можно получить с помощью графического приложения `regedit` или через командную оболочку командой `reg`.

Рассмотрим конкретные ветки и ключи и определим какие права есть у пользователя, администратора, системы. Можно сразу сказать, что SYSTEM имеет полный доступ ко всем каталогам и ключам реестра.

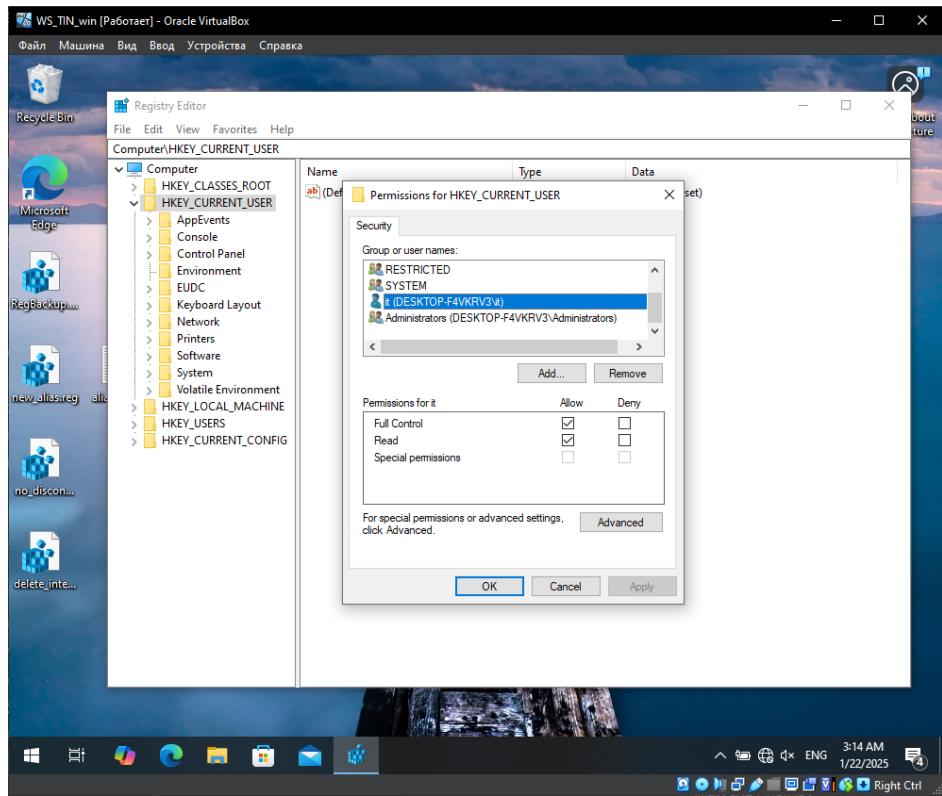


Рис. 1.2: Enter Caption

- **HKEY_CURRENT_USER (HKCU)**

Описание: хранит настройки и параметры текущего пользователя.

Пользователь, Администратор имеют полный доступ.

Примеры ключей:

- HKEY_CURRENT_USER\Software – пользовательские настройки приложений.
- HKEY_CURRENT_USER\Control Panel – параметры интерфейса (цвета, шрифты).

- **HKEY_LOCAL_MACHINE (HKLM)**

Описание: хранит общесистемные настройки, которые применяются ко всем пользователям.

Администратор – полный доступ,

Пользователь – чтение.

Примеры ключей:

- HKEY_LOCAL_MACHINE\Software – настройки установленных приложений.
- HKEY_LOCAL_MACHINE\SYSTEM – параметры системы (например, драйвера, службы).
- HKEY_LOCAL_MACHINE\SAM – база учётных записей (доступен только SYSTEM, Администратор не видит содержимого).

- HKEY_LOCAL_MACHINE\SECURITY – параметры безопасности (доступен только SYSTEM, Администратор не видит содержимого).
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services – управление службами Windows.
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security – лог безопасности (доступен только для SYSTEM).
- HKEY_CLASSES_ROOT (HKCR)
Описание: содержит ассоциации типов файлов и классов объектов COM.
Администратор – полный доступ,
пользователь – чтение.
Примеры ключей:
 - HKEY_CLASSES_ROOT\.txt – ассоциация текстового файла.
 - HKEY_CLASSES_ROOT\CLSID – идентификаторы классов COM-объектов.
 - HKEY_USERS (HKU)
Описание: хранит параметры для всех пользователей системы.
Пользователь – полный доступ к своим данным,
Администратор – полный доступ ко всем веткам.
Примеры ключей:
 - HKEY_USERS\S-1-5-21-<идентификатор>\Software – параметры профиля конкретного пользователя.

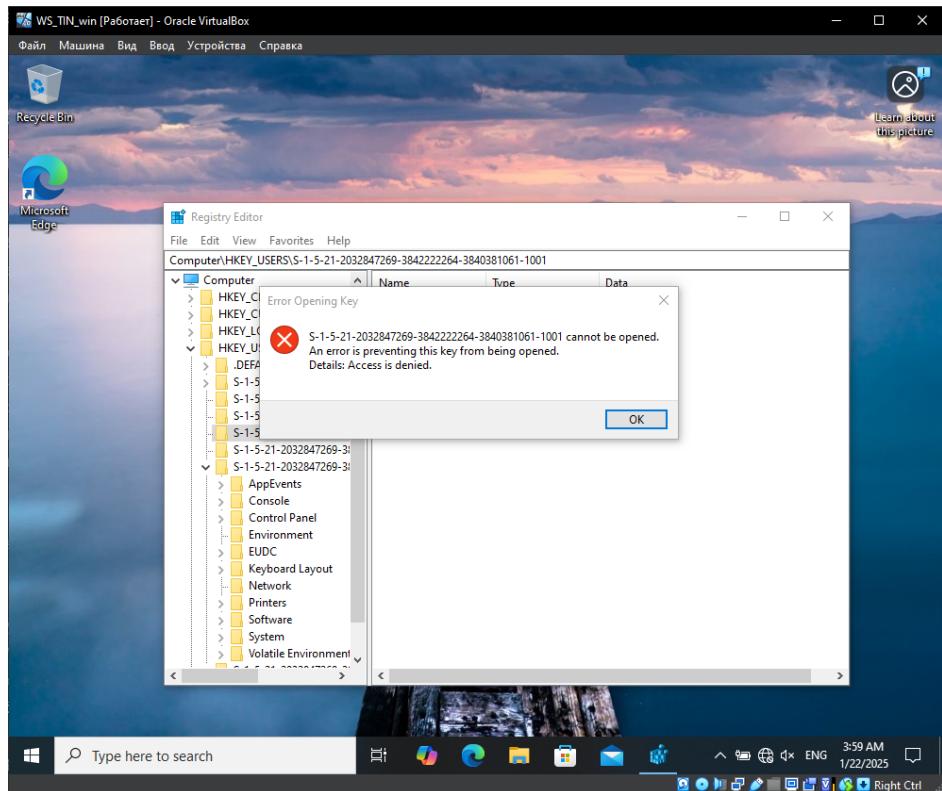


Рис. 1.3: Нет доступа к чужому каталогу для Пользователя.

- HKEY_USERS\.DEFAULT – используется системой до входа пользователя (доступен только SYSTEM).
- HKEY_CURRENT_CONFIG (HKCC)k
Описание: содержит информацию о текущей конфигурации оборудования.
Пользователь – чтение,
Администратор – полный доступ.
Примеры ключей:
 - HKEY_CURRENT_CONFIG\System\CurrentControlSet\Control\Print
– параметры принтеров.

2. 2. Способы восстановления системы

В операционной системе имеется множество способов для системы, которые заключаются в восстановлении состояния реестра сохраненного в последней точке восстановления.

Один из способов заключается в применении экспортированного ранее содержимого реестра. Таким образом можно вернуть прежние значения ключей, но не выйдет удалить созданные ключи.

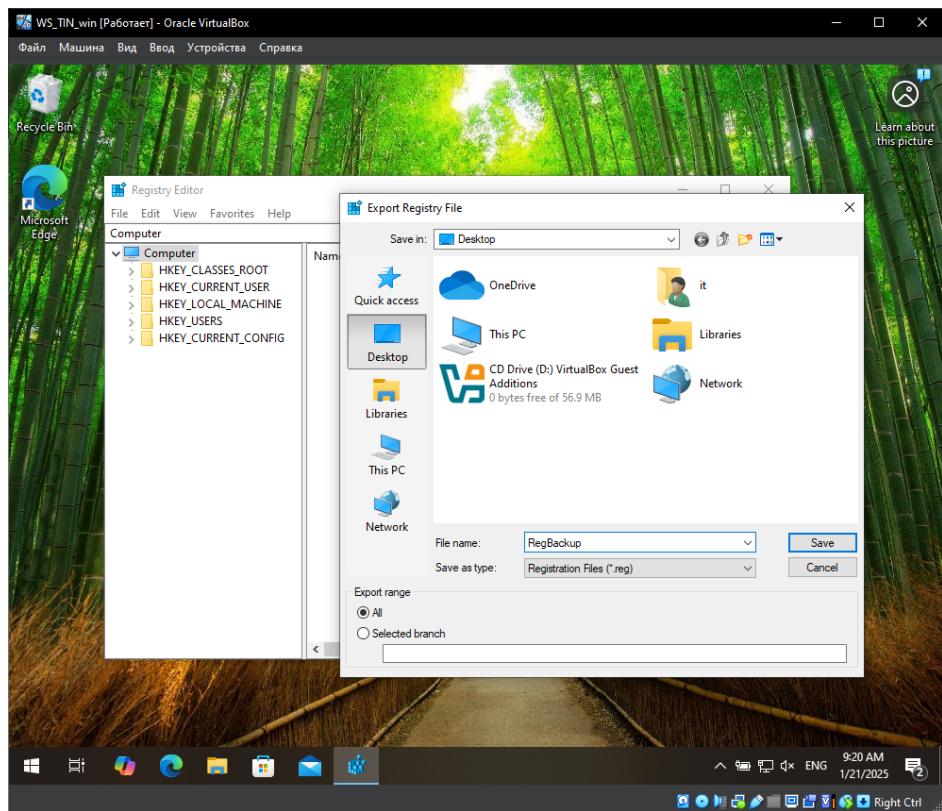


Рис. 1.4: Создание резервной копии реестра.

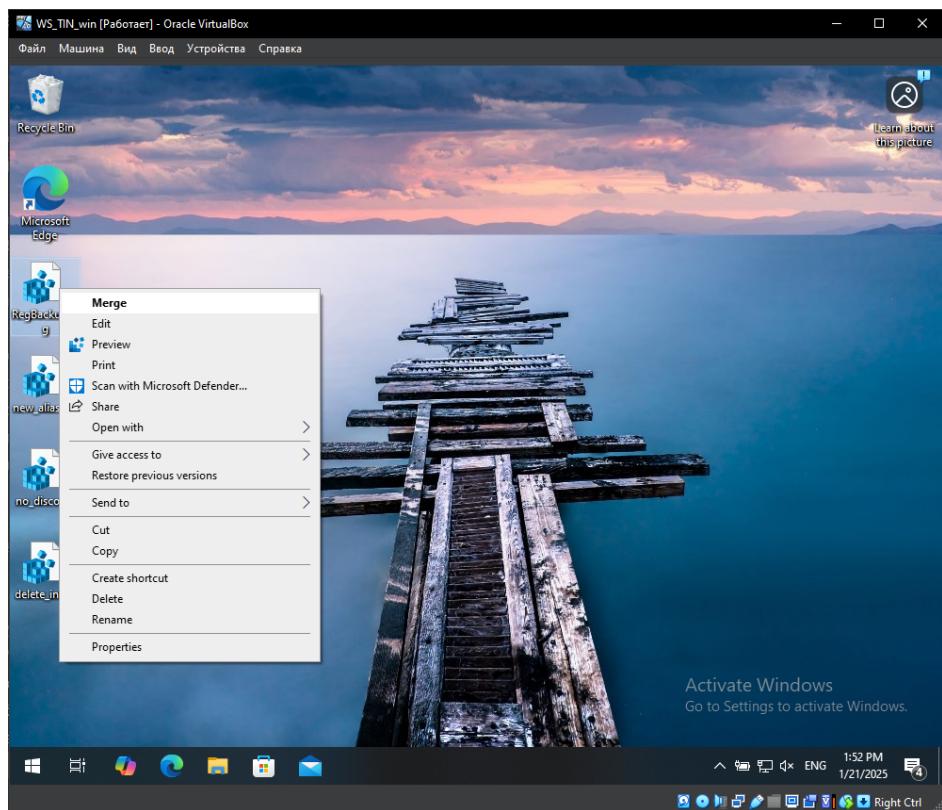


Рис. 1.5: Восстановление реестра путем слияния с экспортированной ранее резервной копией.

Другой способ заключается в использовании средства восстановления,

которому необходим режим защищенной работы системы с периодическим созданием точек восстановления. В нем выбирается имеющаяся точка, а далее система выполняет автоматическое восстановление реестра из сохраненной копии.

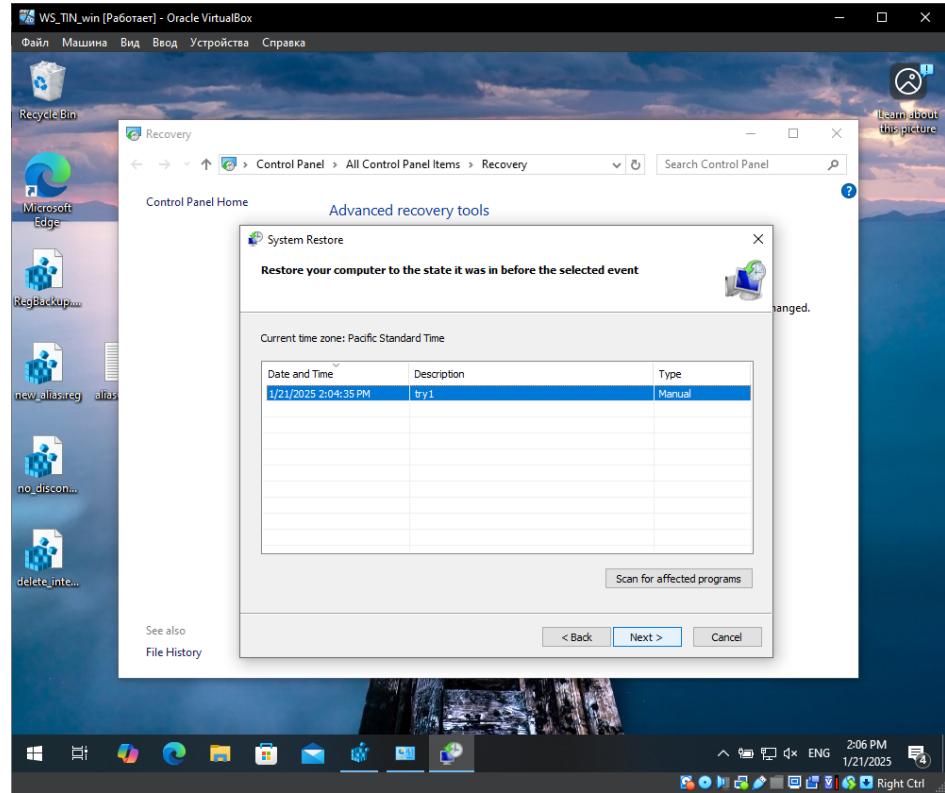


Рис. 1.6: Выбор точки восстановления (последняя сохраненная).

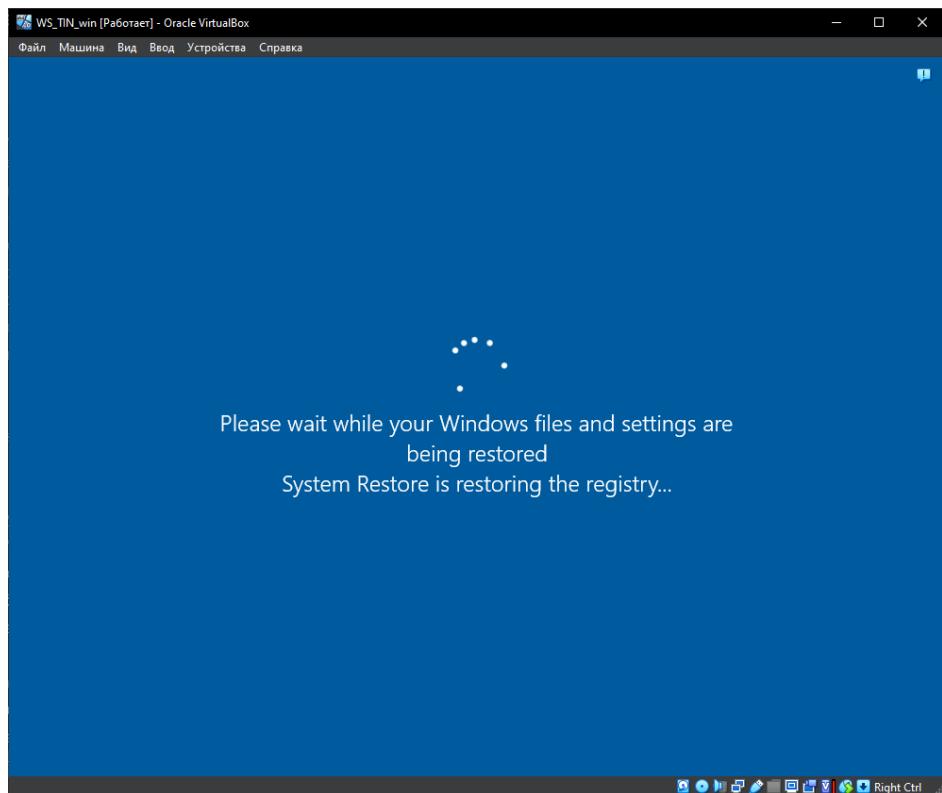


Рис. 1.7: Экран компьютера во время восстановления.

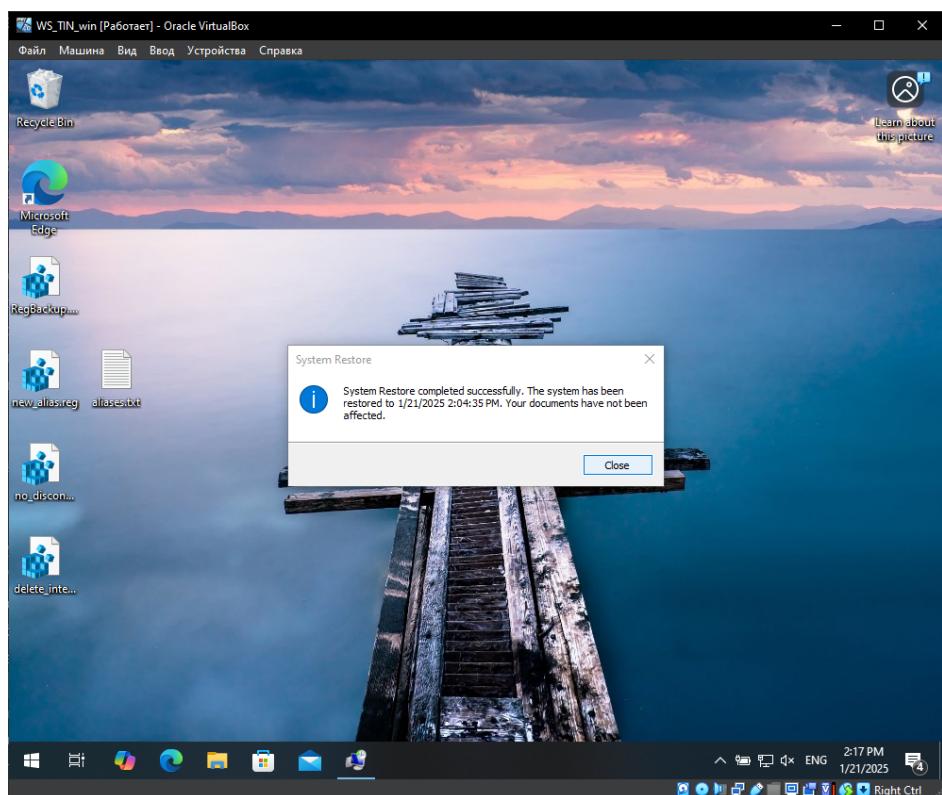


Рис. 1.8: Восстановление выполнено успешно.

Кроме того, восстановление системы можно выполнить из меню расширенного запуска системы.

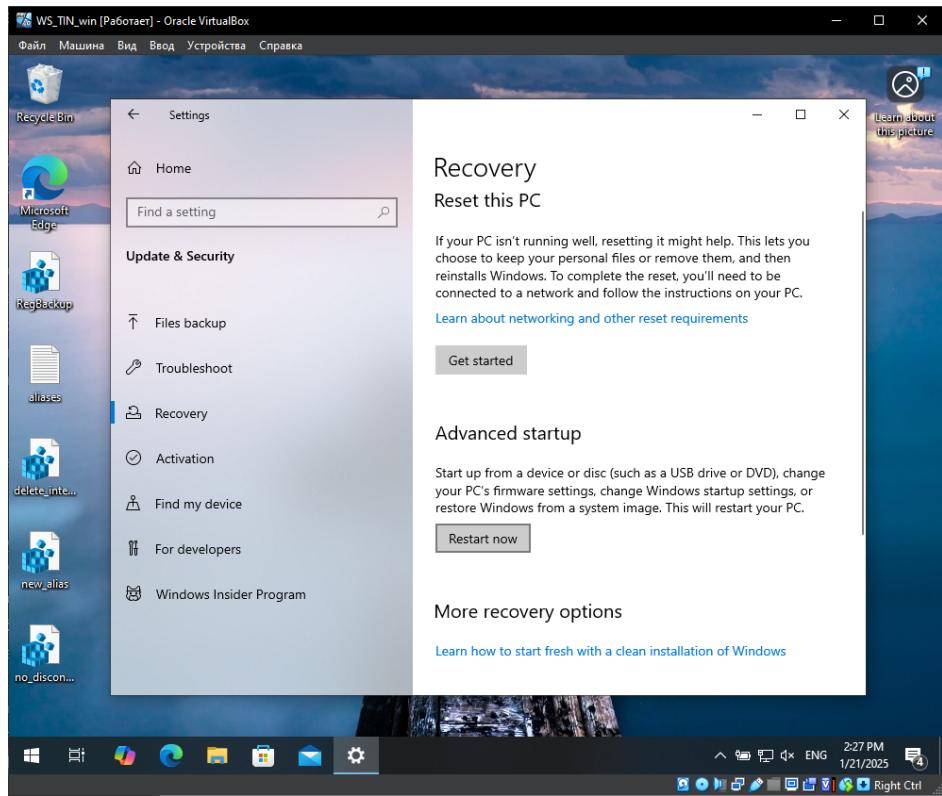


Рис. 1.9: Кнопка перезагрузки с включением расширенных возможностей запуска.

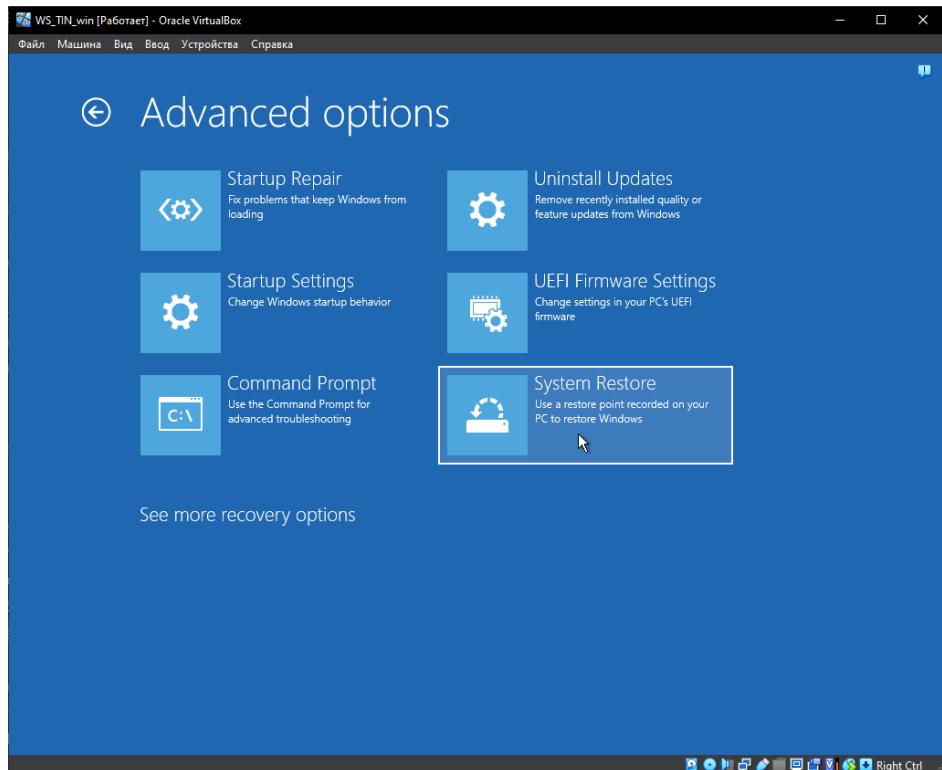


Рис. 1.10: Восстановление из через расширенные возможности запуска.

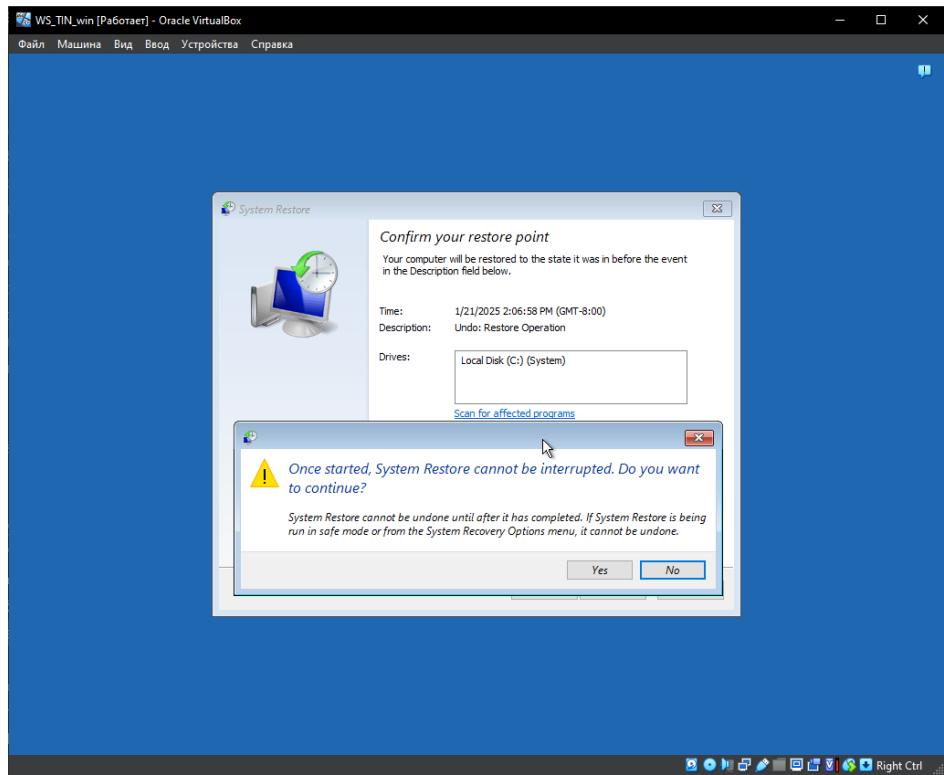


Рис. 1.11: Восстановление системы при запуске.

2. 3. Задание по варианту

Создание псевдонима к программе `notepad.exe`. Этот метод работает за счет добавления команды которая выполняется при запуске командной оболочки: `doskey` создает псевдоним приложения, который доступен во время сеанса работы с командной оболочкой.

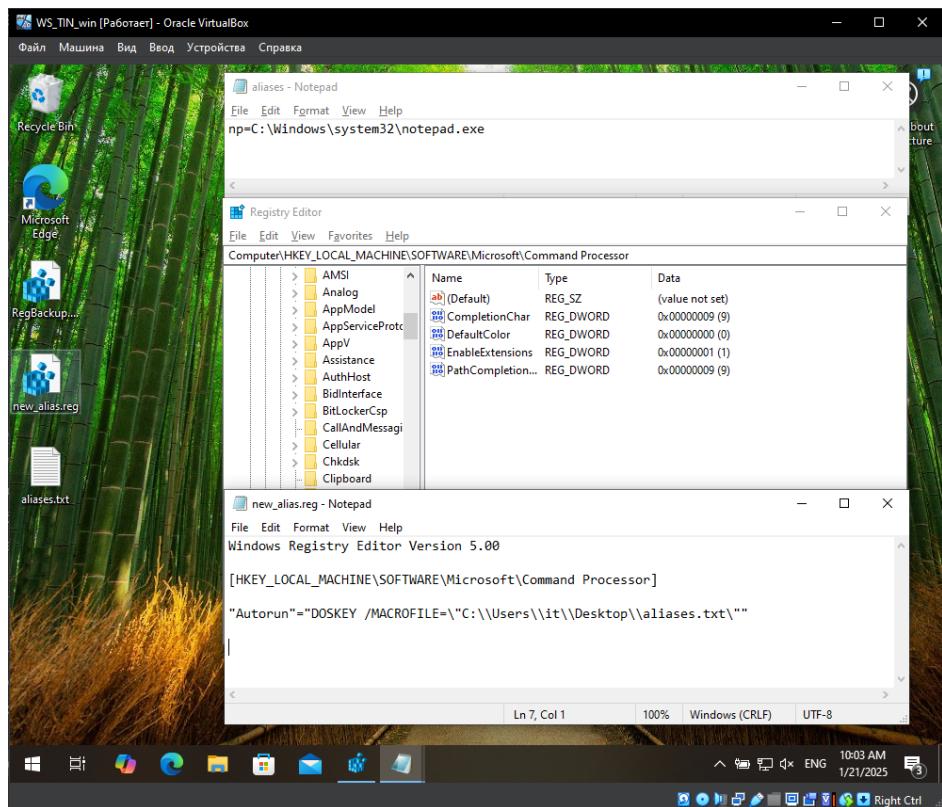


Рис. 1.12: Содержимое reg-файла и аргументов для утилиты doskey для добавления псевдонима приложения notepad.exe.

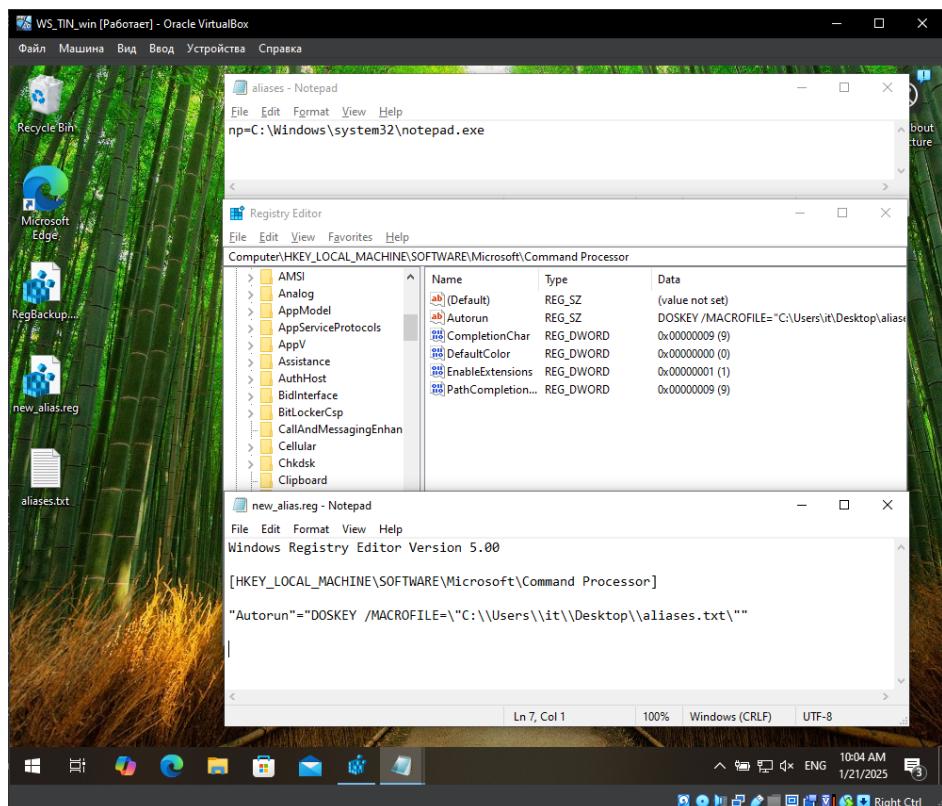


Рис. 1.13: Результат применения reg-файла.

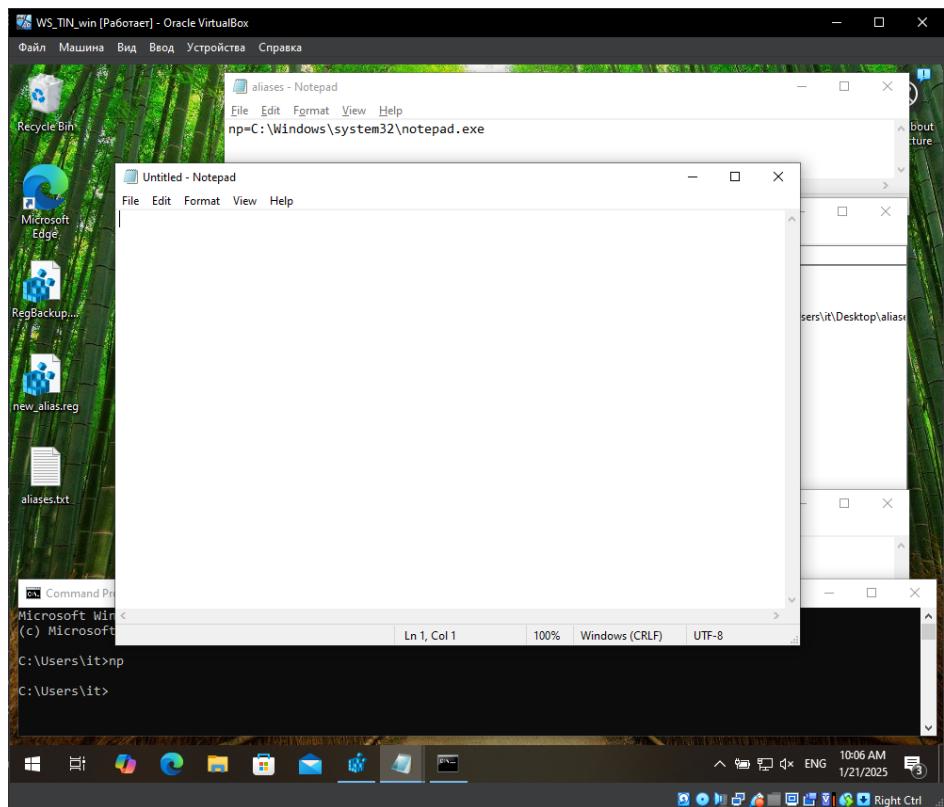


Рис. 1.14: Демонстрация работы добавленного псевдонима для приложения.

Отключение автоматического разрыва соединения при выходе из системы. Метод представлен для системной службы LanmanServer, т.е. пользовательские процессы завершаются при выходе из системы (signout). Изначально в атрибуте записано значение `dword:f`.

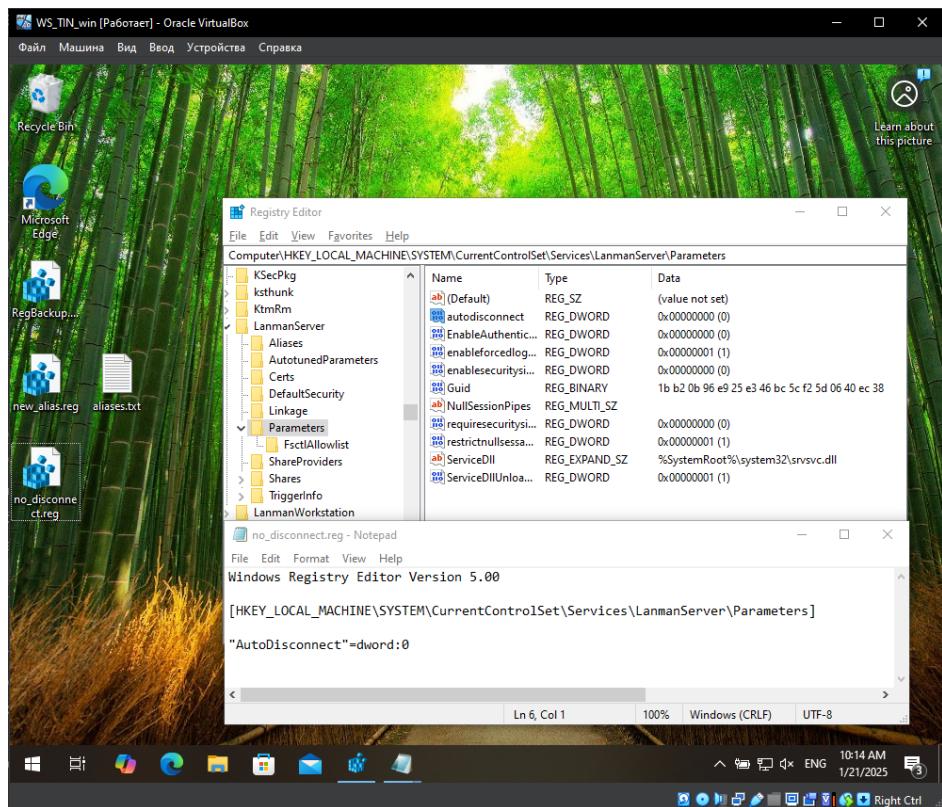


Рис. 1.15: Содержимое reg-файла для выключения автоматического отключения связи при выходе из системы.

Автоматическое удаление временных файлов после работы в Интернет. Метод должен работать для Internet Explorer, однако на современных версиях Windows он не доступен и по умолчанию используется Edge, а он, как нормальный chromium-браузер сохраняет кеш в каких-то указанных в настройках каталогах и позволяет настраивать автоудаление в настройках приложения.

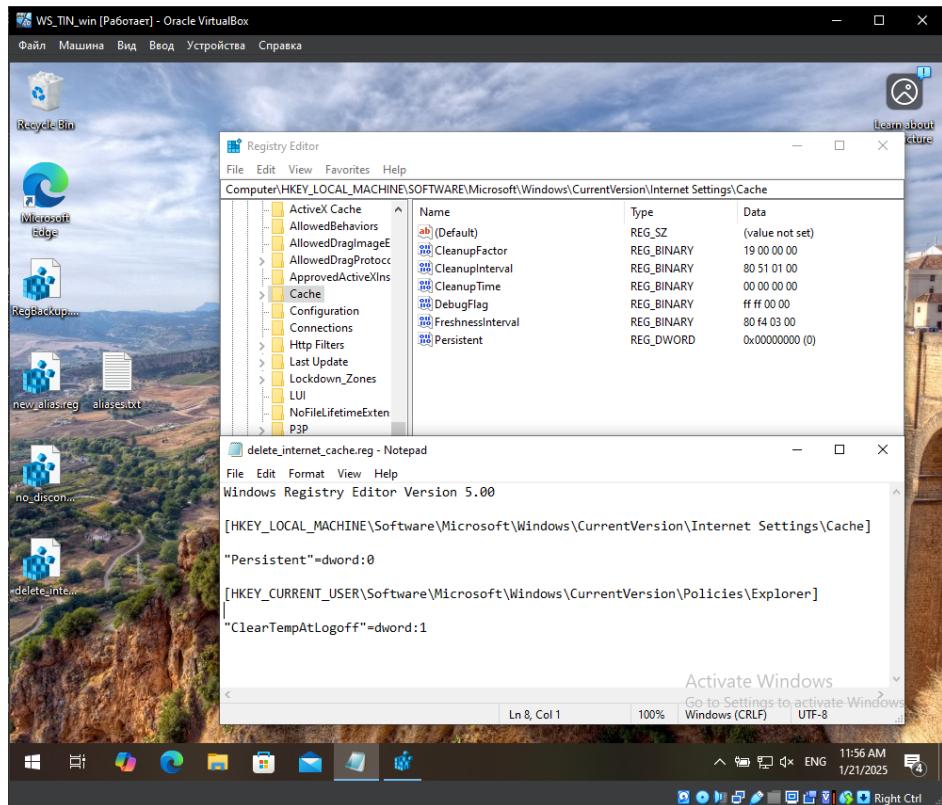


Рис. 1.16: Содержимое reg-файла для отключения кеширования данных в «Интернет».

3. Вывод

Изучили основы устройства реестра Windows, научились использовать его для настраивания различных параметров операционной системы и прикладных приложений. Изучили и испытали способы восстановления системы.

Реестр Windows показывает централизованный подход к конфигурированию операционной системы в противовес подходу в *nix-системах с помощью отдельных конфигурационных файлов. Этот подход в некоторых случаях, например, когда значение ключа очевидно, оказывается удобно, но в целом реестр выглядит очень громоздким и не удобным для эксплуатации рядовым пользователем.