

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОЙ РАБОТЫ №1**

# **В РАМКАХ ДИСЦИПЛИНЫ «БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»**

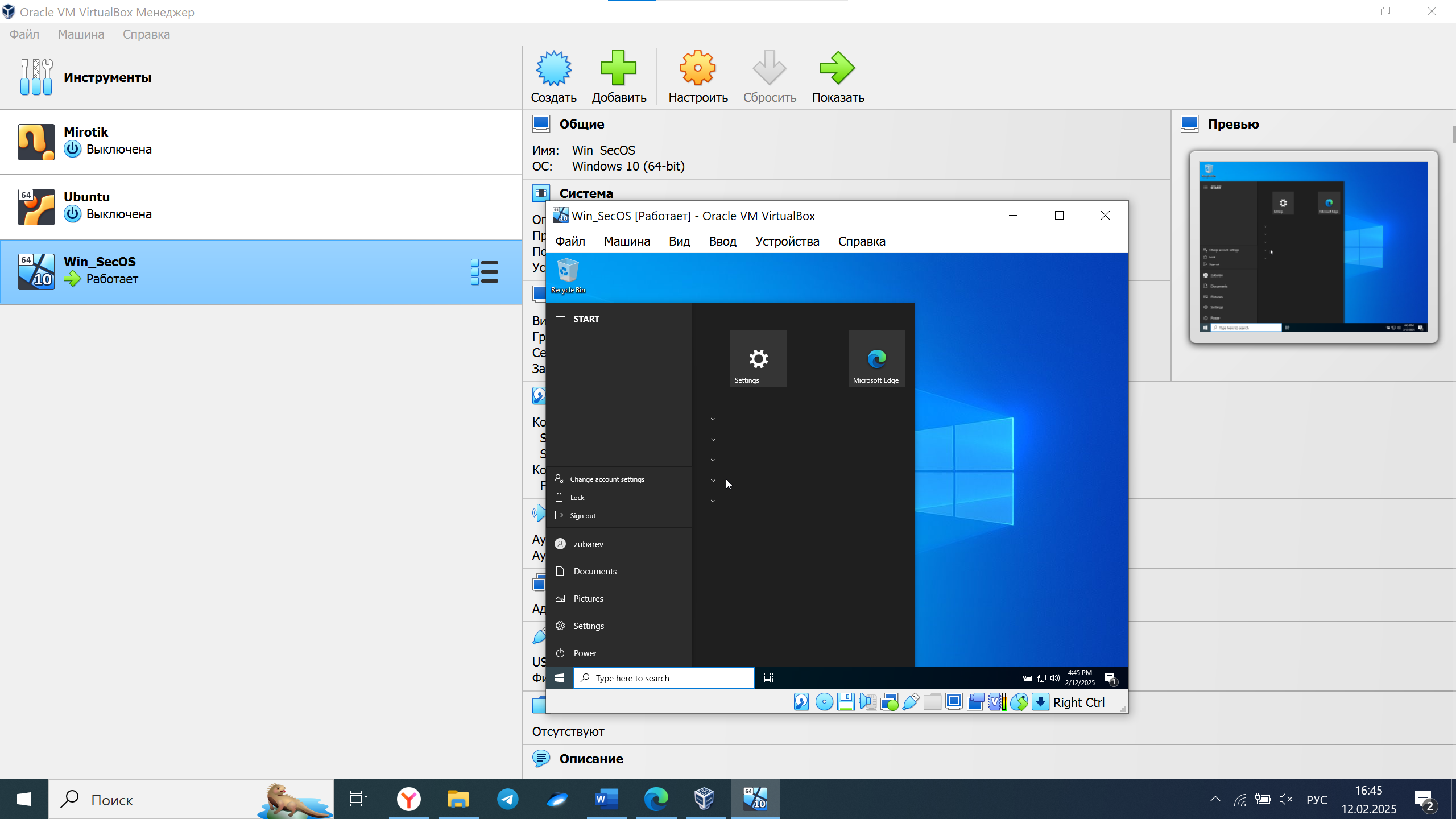
Выполнил:

Студент 3-ого курса

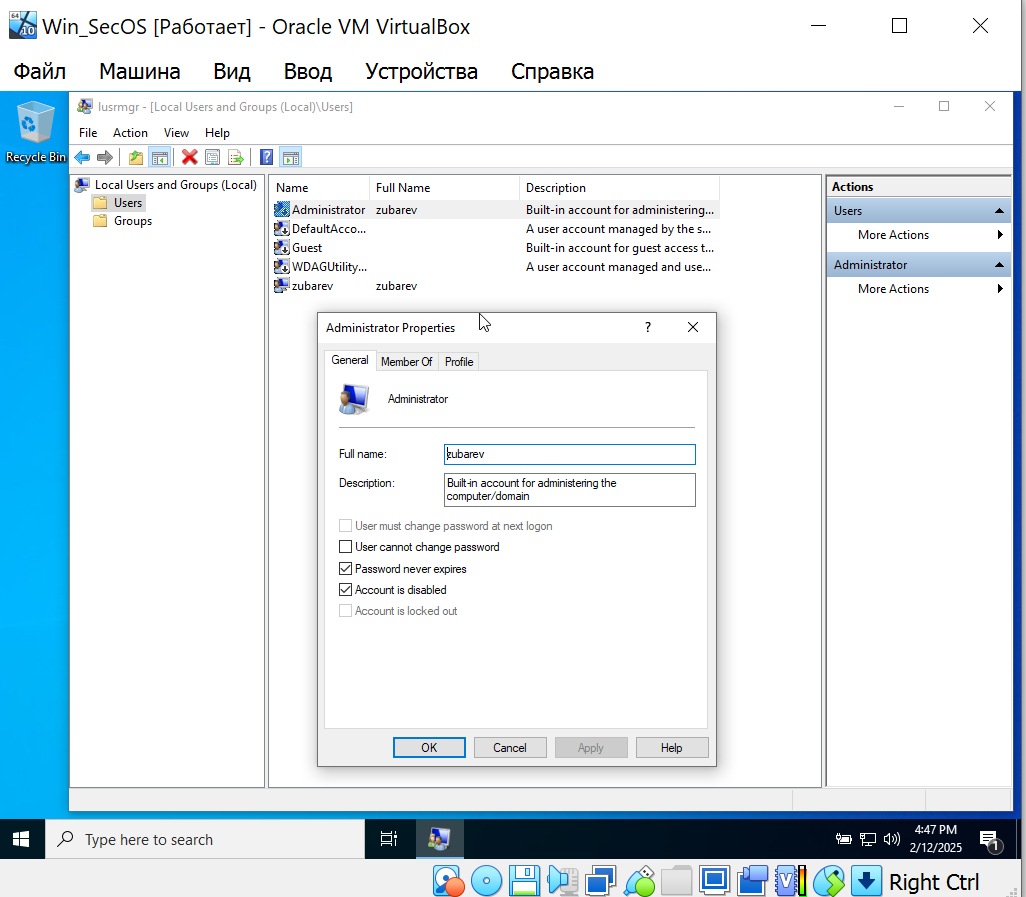
Учебной группы БИСО-02-22

Зубарев В.С.

Работа виртуальной машины под ОС Windows 10

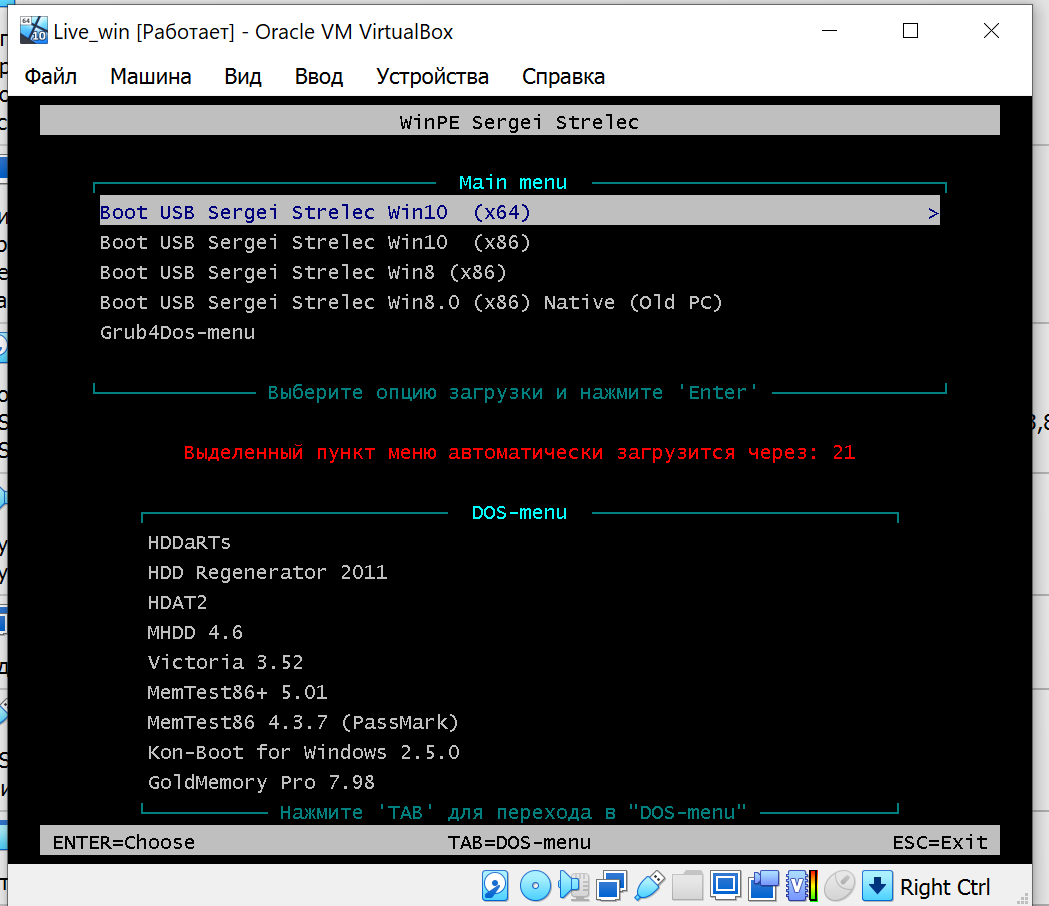


Активация учетной записи администратора

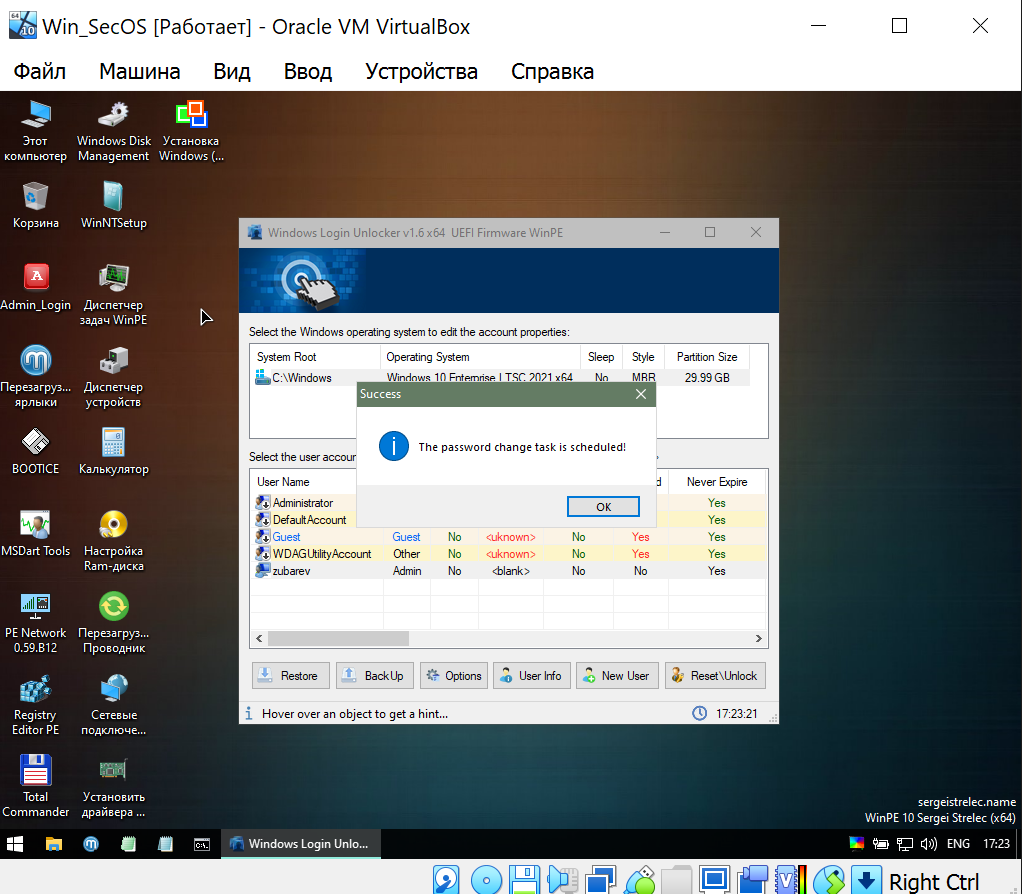


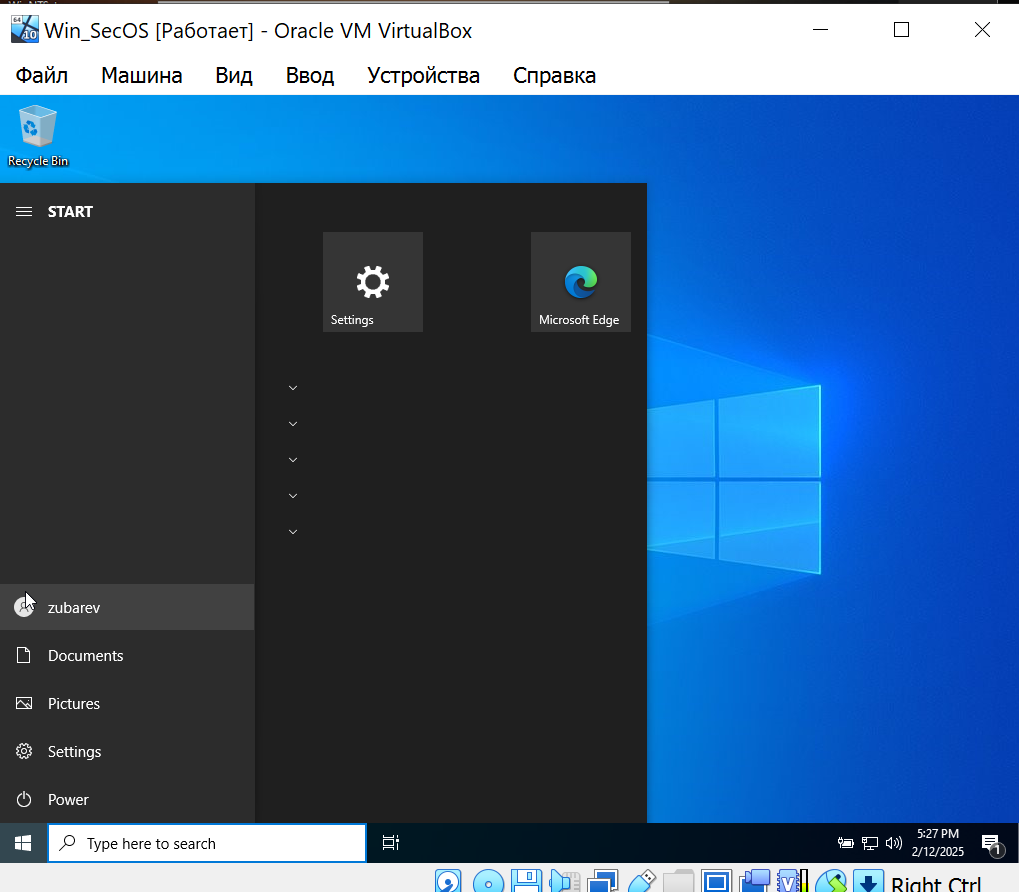
Выставление приоритетов загрузки виртуальной машины

Запуск системы с Live CD



Смена пароля



Вход с новым паролем  


Перечень известных систем виртуализации, их отличительные особенности?

Ответ:   
**Oracle Virtual Box, VMWare workstation(Pro)**Отличительные особенности VB – бесплатный, VMware - платный

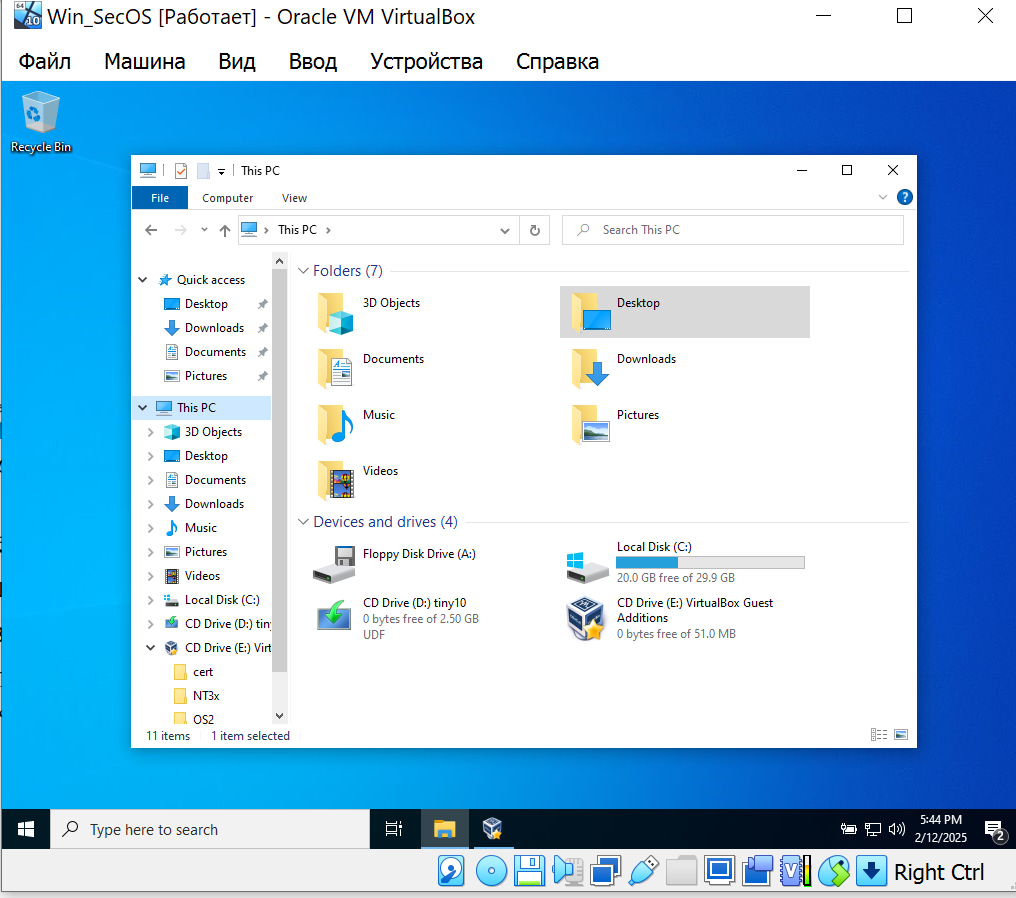
Перечень известных образов Live CD, особенности их работы?  
Ответ:

**Kaspersky Rescue Disk**. Средство лечения заражения, при условии, что система была поражена настолько, что не может нормально функционировать.

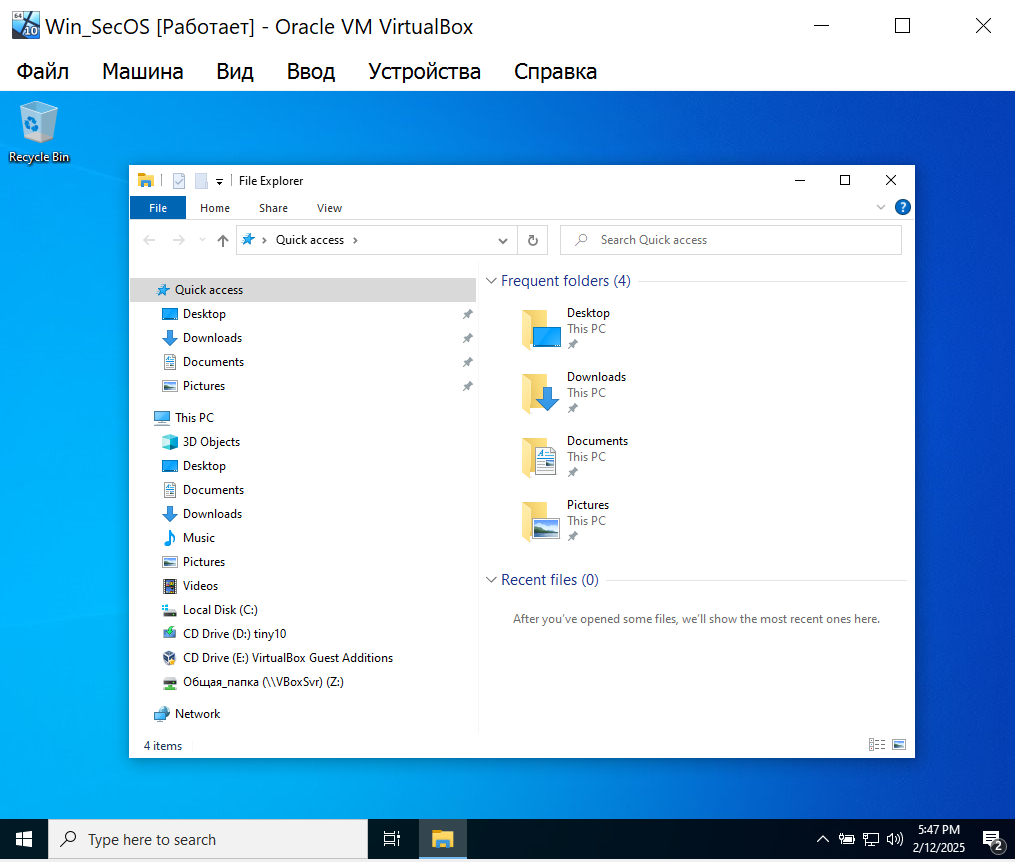
Какие встроенные средства защиты и средства защиты информации помогут защититься от уязвимости, которую мы использовали?

Ответ: Включение пароля администратора в BIOS и заперт загрузки со сторонних носителей.

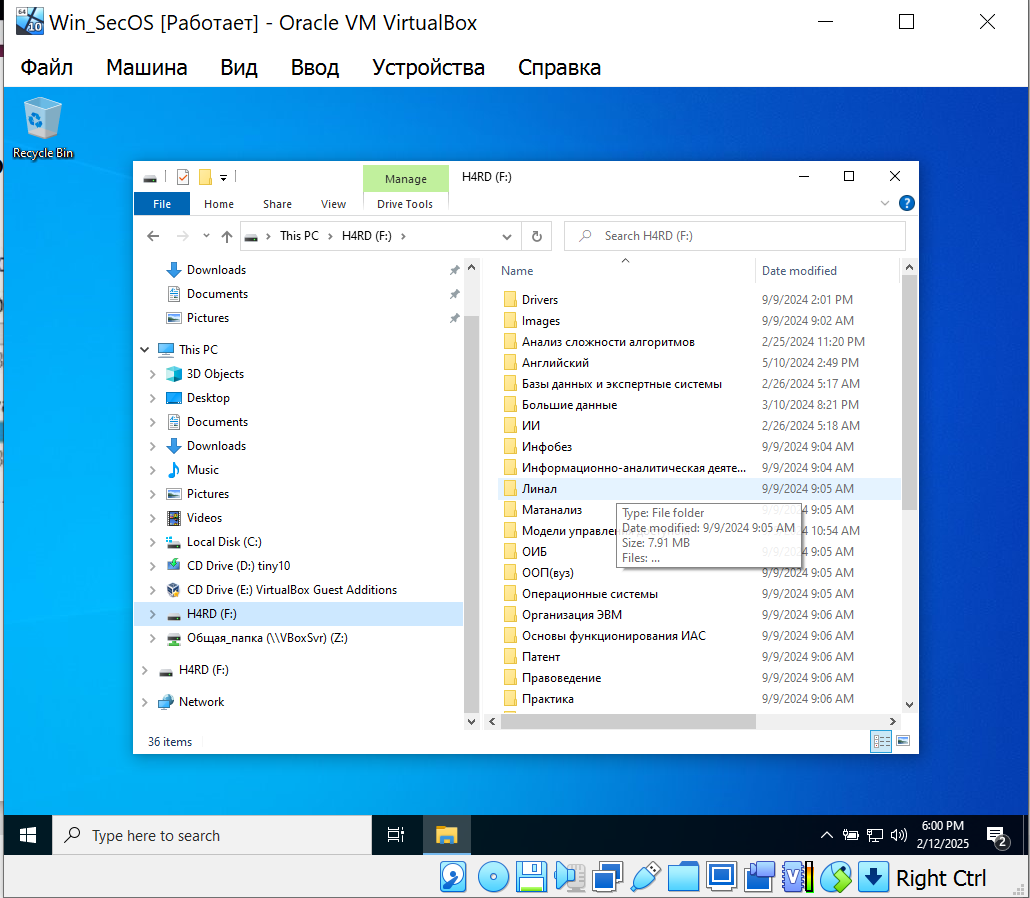
Установка Дополнений VB



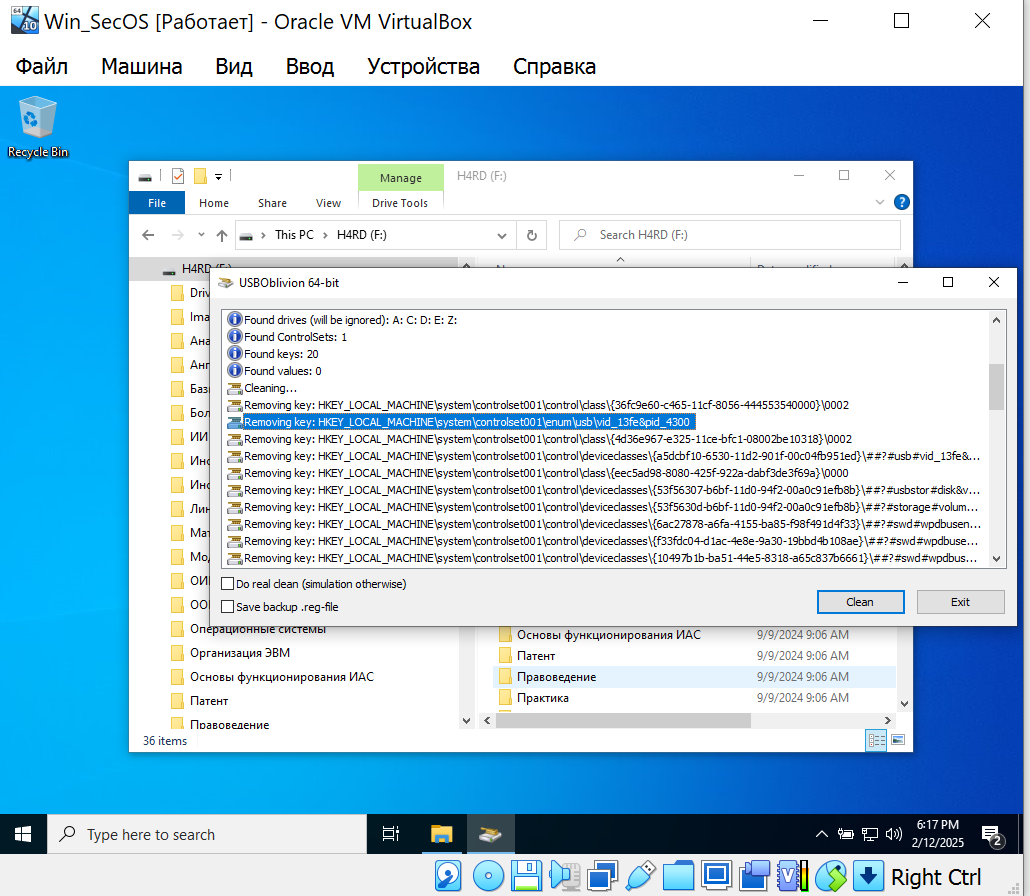
Добавление общей папки

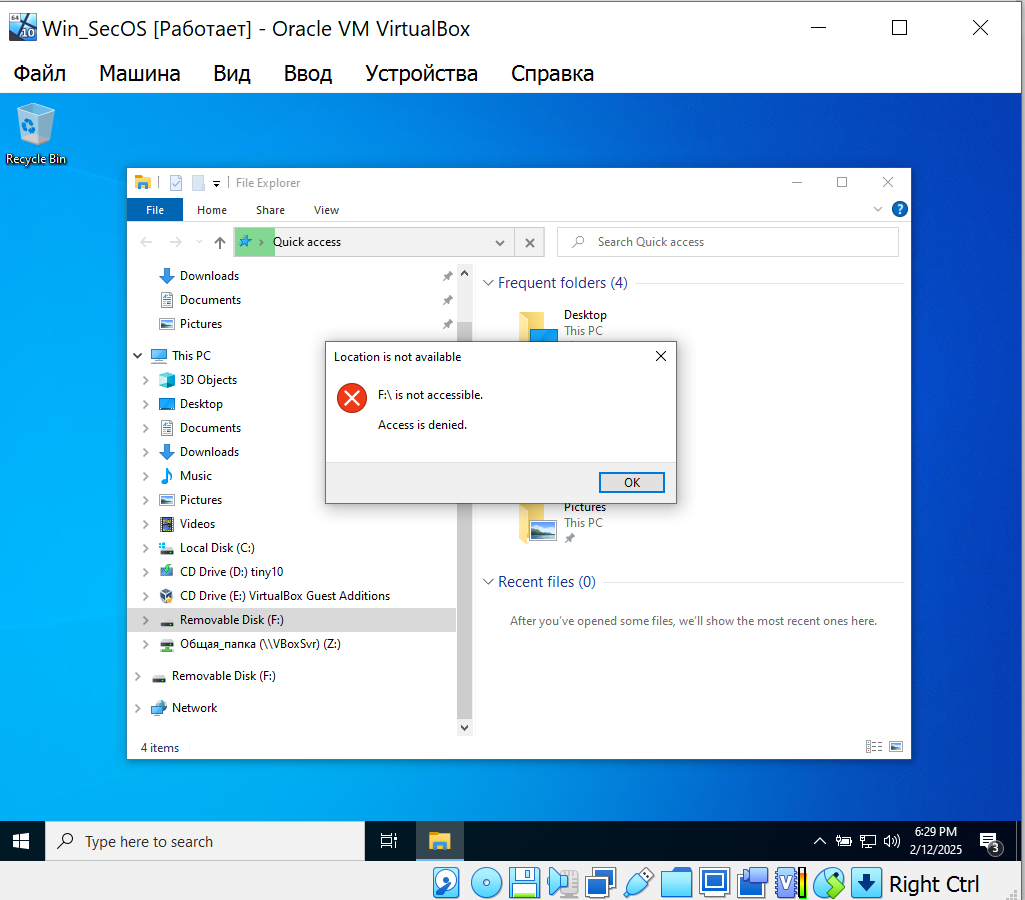


Подключение USB Носителя

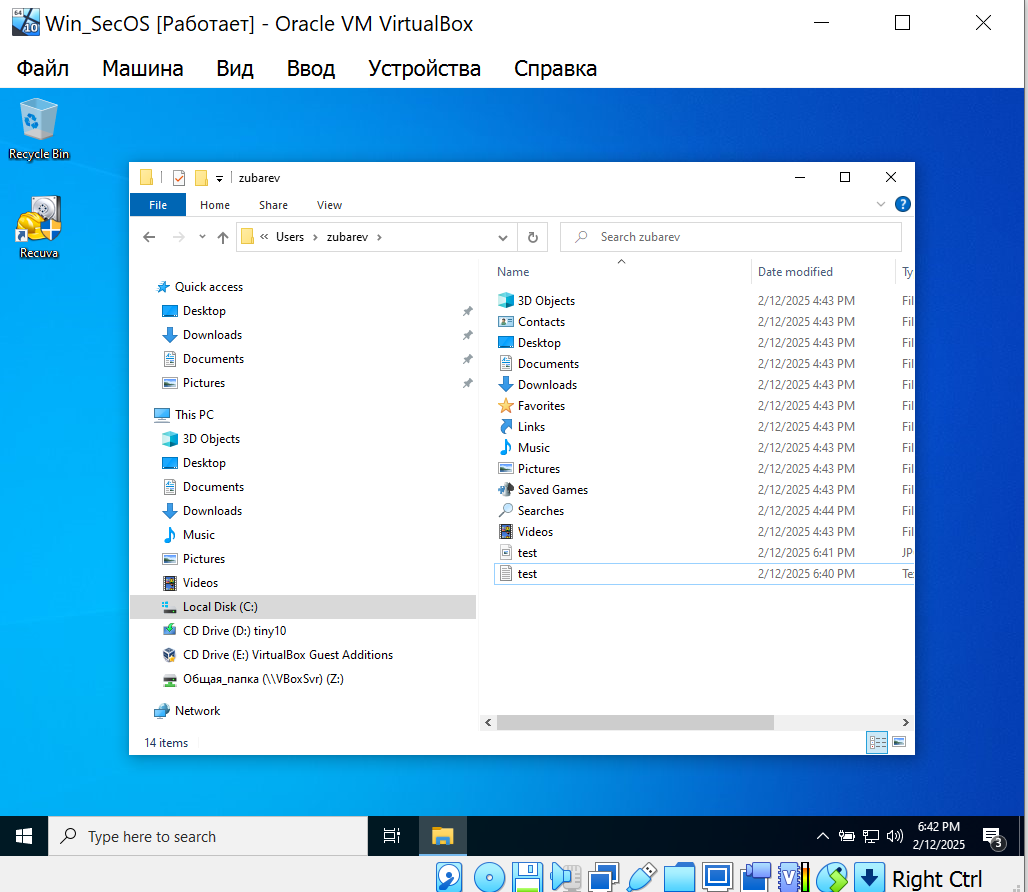


Серийный номер = 8669111080577343469&0 VID = 13fe PID = 4300

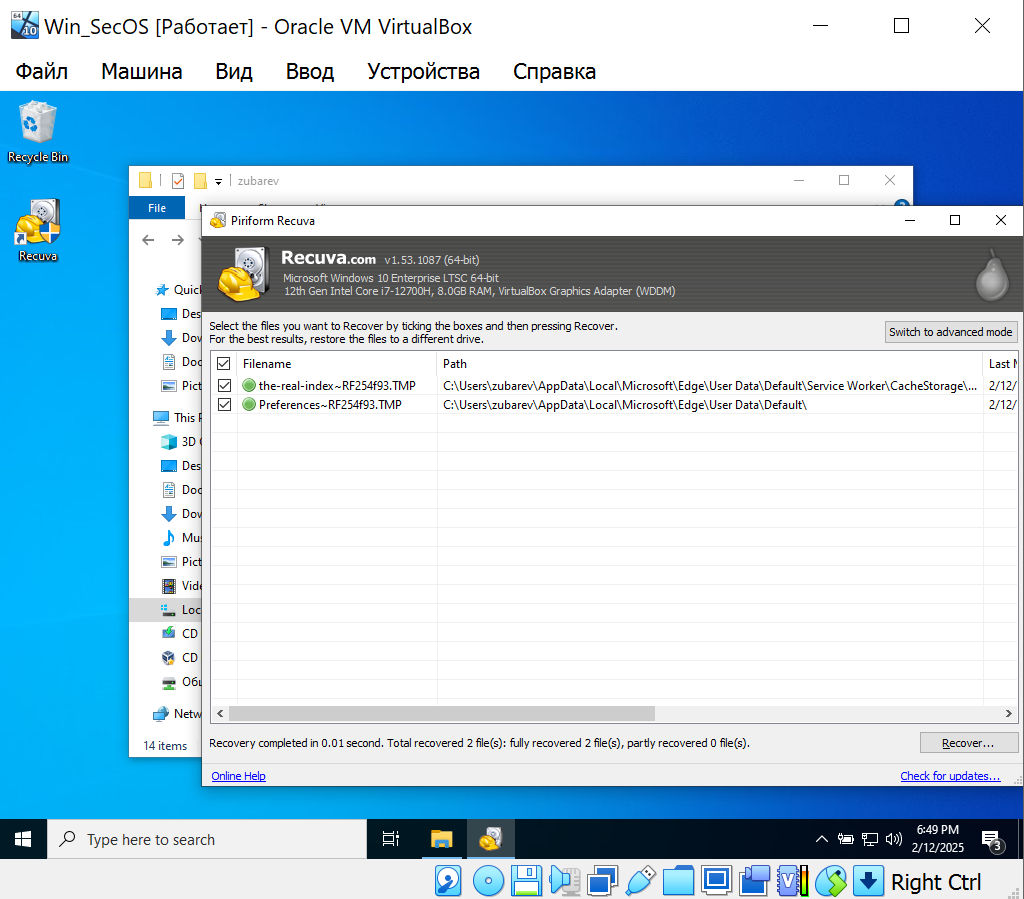


Блокировка флешки через Device Locker  


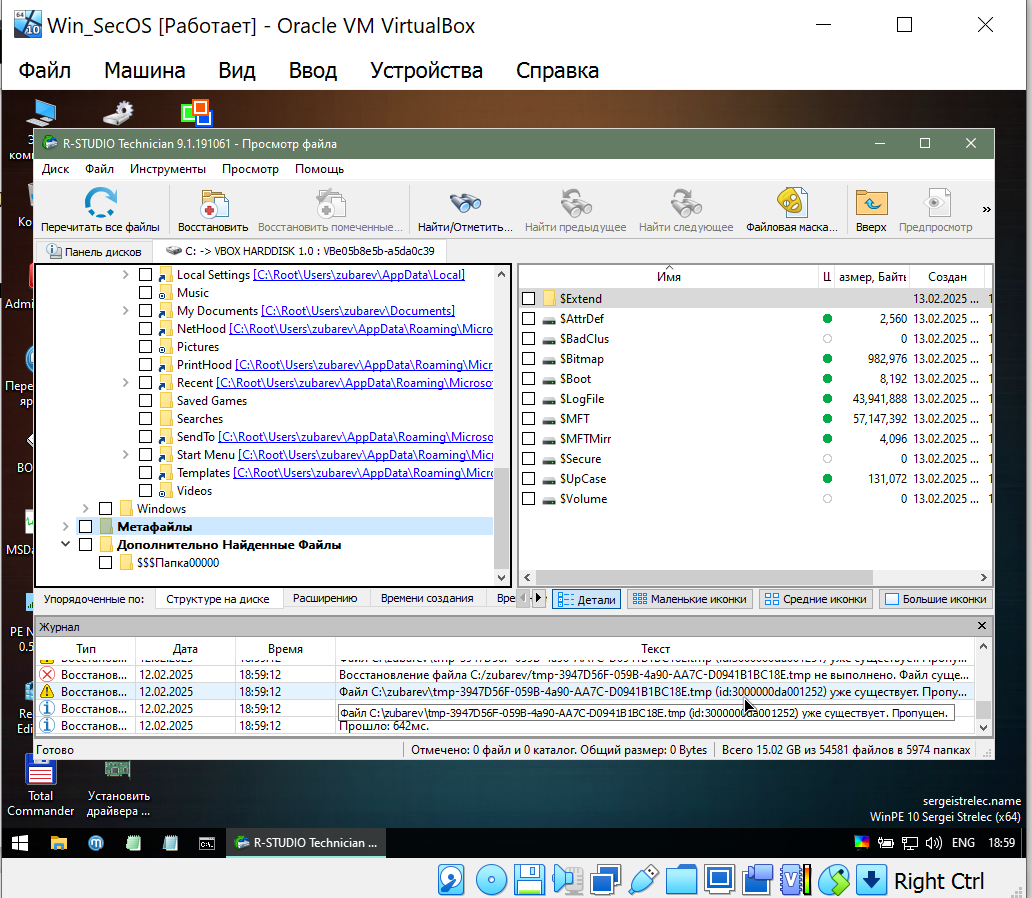
Device locker фиксирует состояния подключенных устройств (серийный номер, vid, pid) и в случае подключения других устройств блокирует к ним доступ

Перенос файлов  


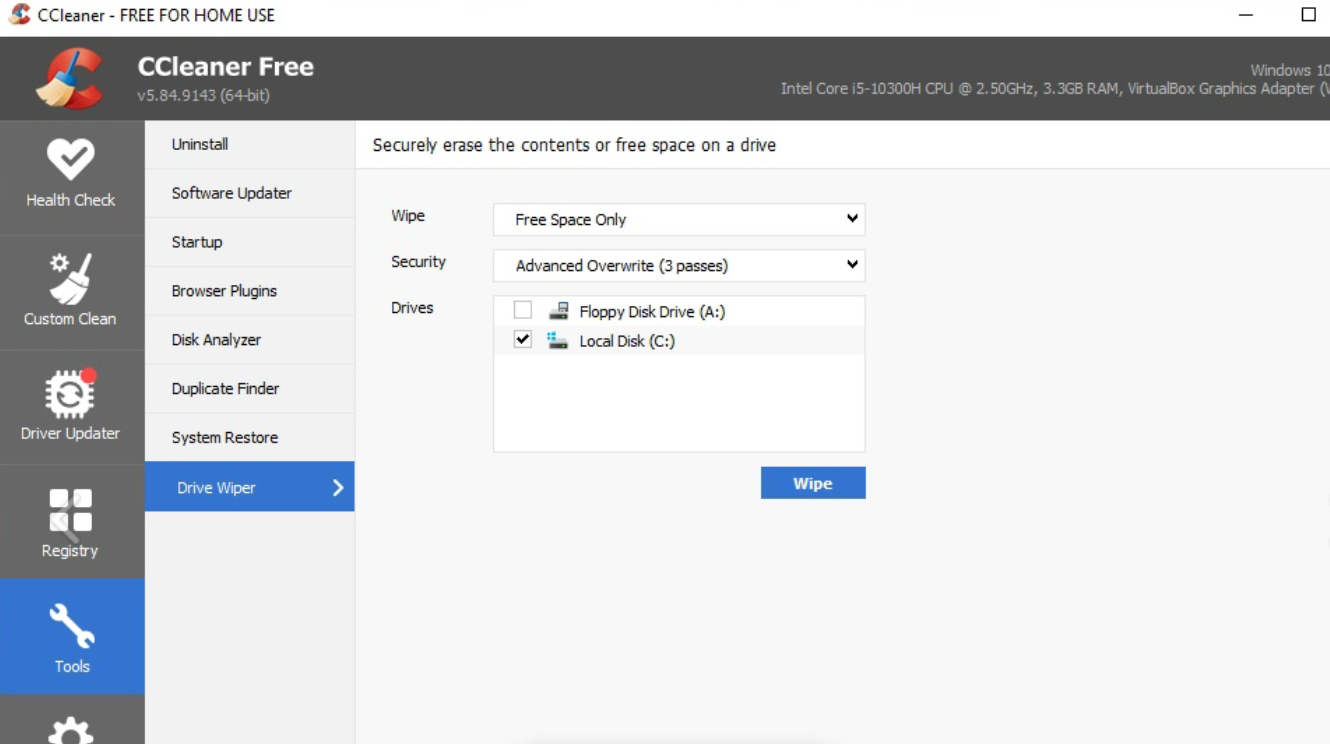
Восстановление файлов



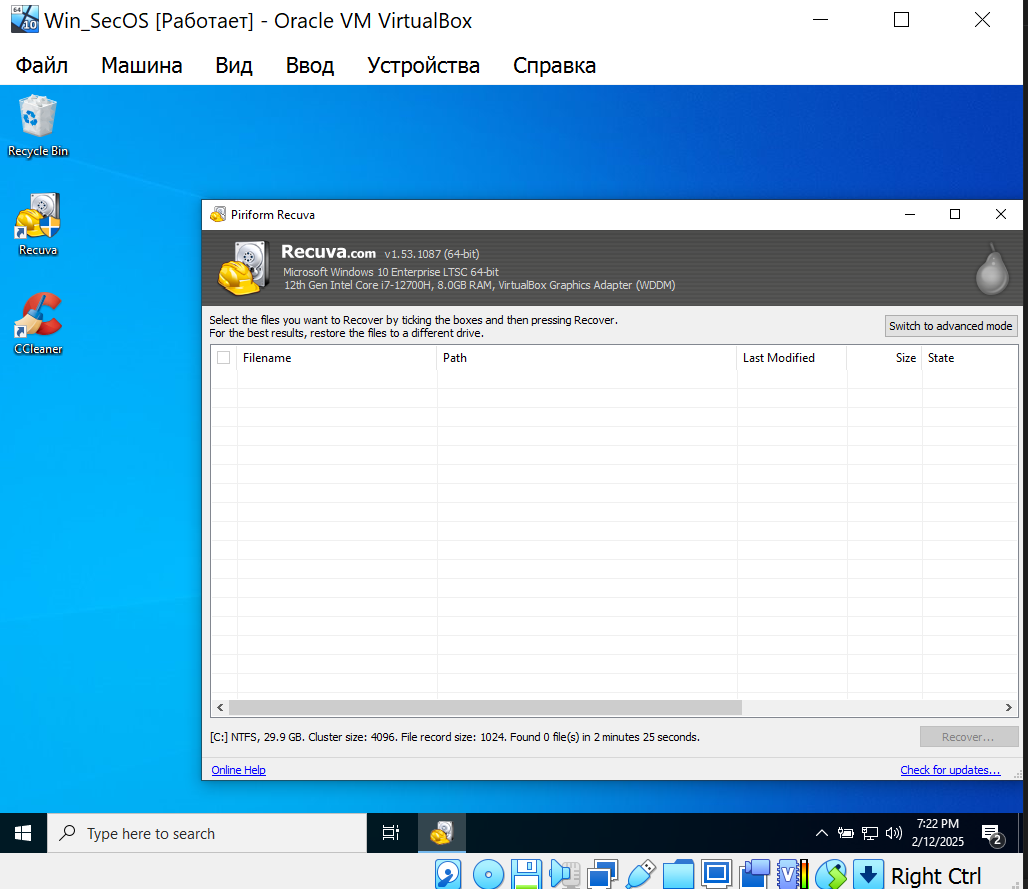
Восстановление через Live CD



Затиранииe диска через CCleaner



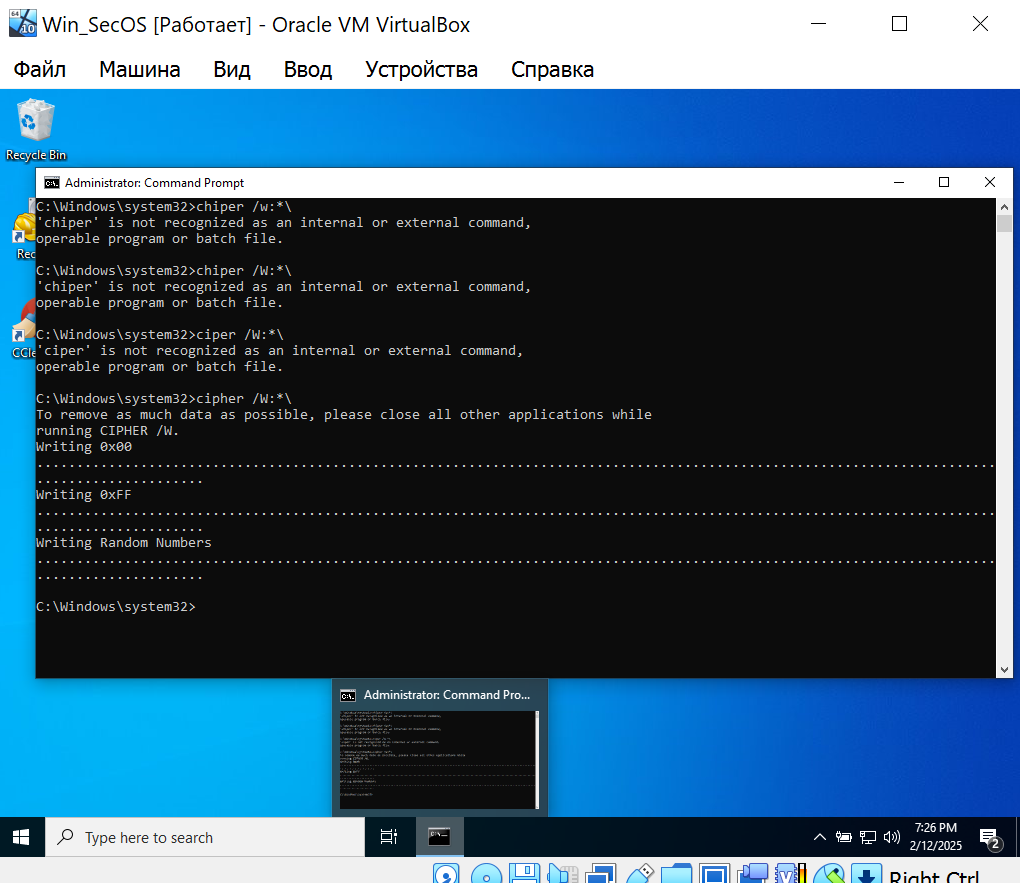
Восстановление после затирания



Результаты восстановления файлов;

До затирания файлы восстановить возможно (так как при удалении затираются только заголовки файловой системы), а после затирания данные восстановить будет практически не возможно.

Затирание через cipher



Cipher — это утилита командной строки для управления шифрованием файлов в Windows. Она отображает состояние шифрования текущего или указанного каталога и всех файлов в нём, может задавать режимы и параметры шифрования, создавать сертификаты и ключи, выполнять шифрование или расшифровку файлов и каталогов, управлять доступом пользователей к зашифрованным данным.

Параметр /W в команде cipher **удаляет данные из доступного неиспользуемого дискового пространства на всём томе**. Если выбран этот параметр, все остальные будут игнорироваться. Заданный каталог может располагаться в любом месте локального диска. Если это точка или точки подключения к каталогу в другом томе, данные в этом томе будут удалены.