МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

РТУ МИРЭА

«МИРЭА – Российский технологический университет»

Институт кибербезопасности и цифровых технологий

Кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»

Практическая работа № 1

«Основы виртуализации. Работа с файлами»

по дисциплине «Безопасность операционных систем»

Москва

2023

1.1. Подготовка учебного стенда. Программное обеспечение для виртуализации

Порядок выполнения работы:

1. Установка Virtual Box

Скачайте дистрибутив для своей операционной системы и установите Oracle Virtual Box актуальной версии.

https://www.virtualbox.org/wiki/Downloads

2. Установка виртуального образа Windows 10

Для выполнения работы нам подойдет любая версия Windows 10, но лучше использовать облегченный образ системы. Скачайте его по ссылке.

https://disk.yandex.ru/d/2aMvl3enMBrFZA

Для создания виртуальной машины перейдите во вкладку “Инструменты” и нажмите кнопку “Создать”

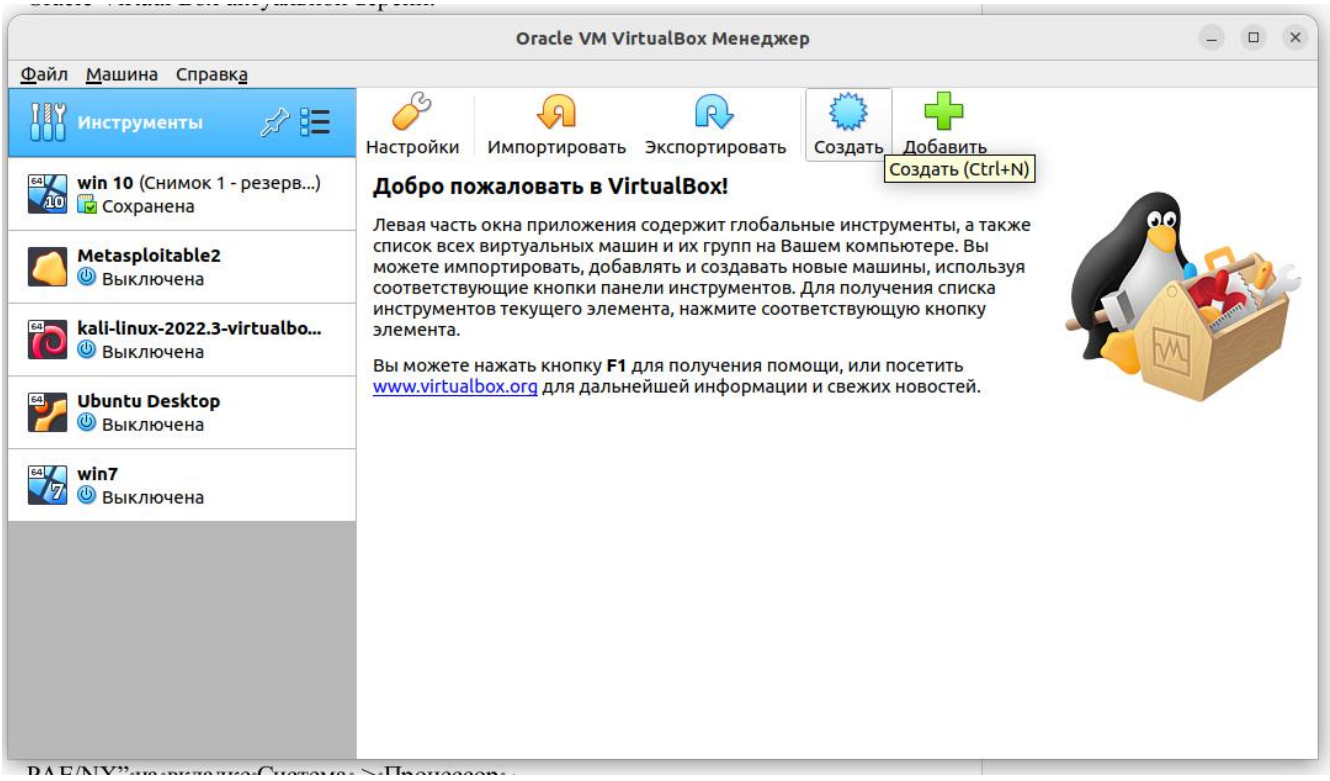

Рисунок 1. Окно приветствия Virutal Box

На вкладке создания виртуальной машины введите имя, установочный образ (при необходимости тип и разрядность ОС), на влкдаке “Оборудование” укажите объем ОЗУ (рекомендуется не менее 2 ГБ) и количество процессоров (рекомендуется не менее 2).

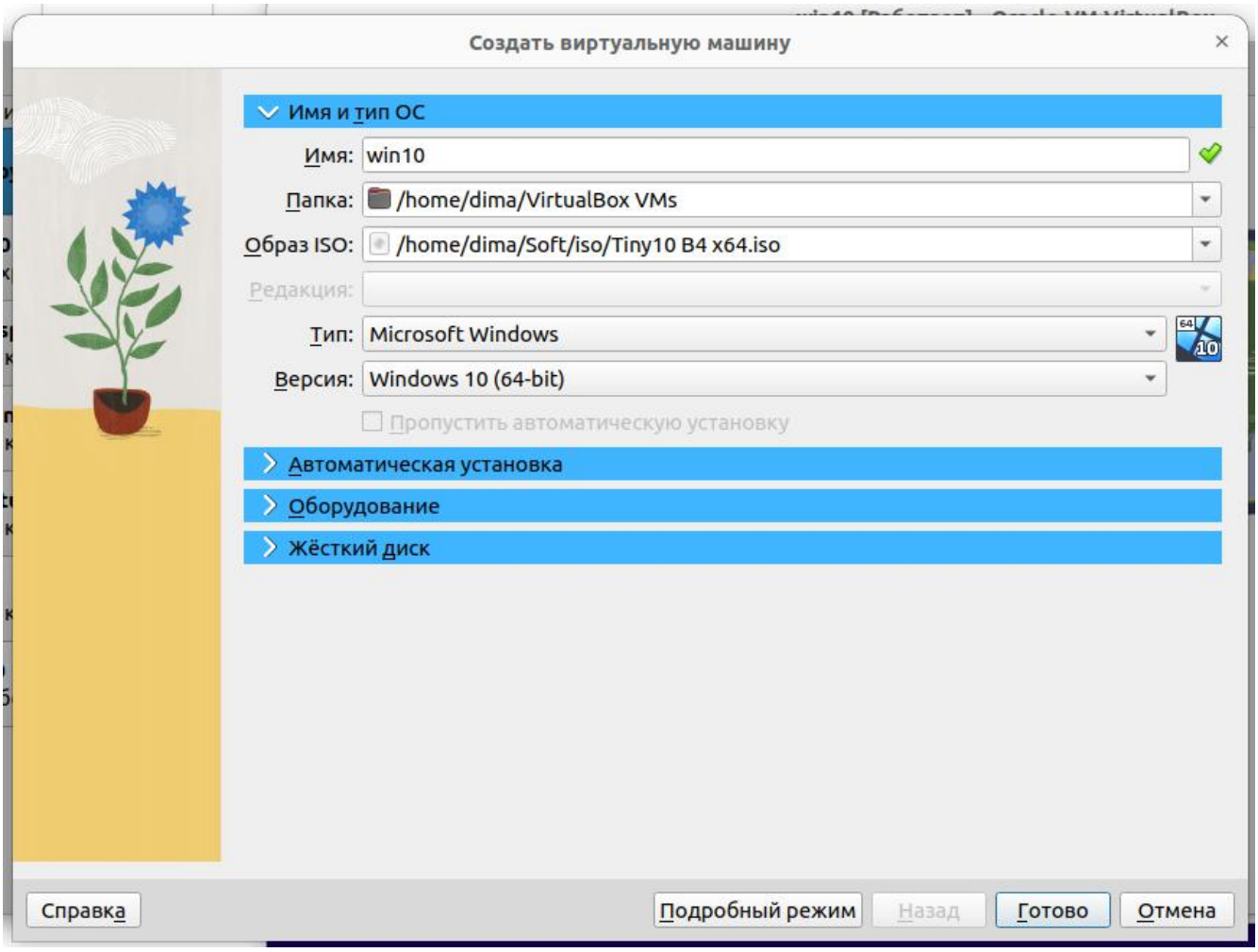

Рисунок 2. Создание виртуальной машины

Следующим этапом необходимо на вкладке “Жесткий диск” создать новый виртуальный жесткий диск. Фиксированный виртуальный жесткий диск работает быстрее, но под него сразу требуется выделить полный объем, динамический виртуальный жесткий диск будет увеличиваться по мере необходимости и для наших целей это предпочтительнее. Укажите размер жесткого диска (не менее 30 ГБ).

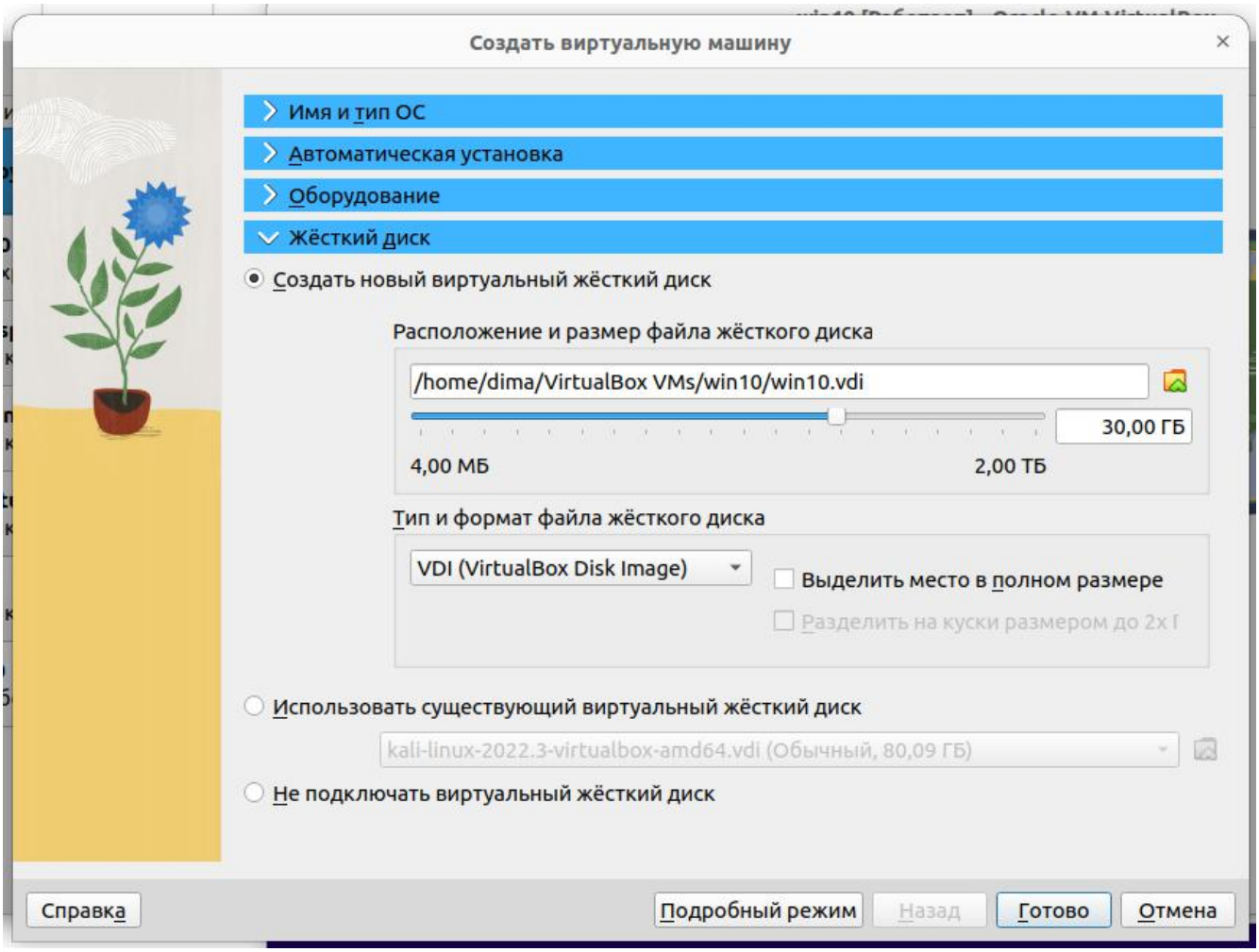

Рисунок 3. Создание виртуального жесткого диска

Запустите виртуальную машщиу и произведите установку Windows 10.

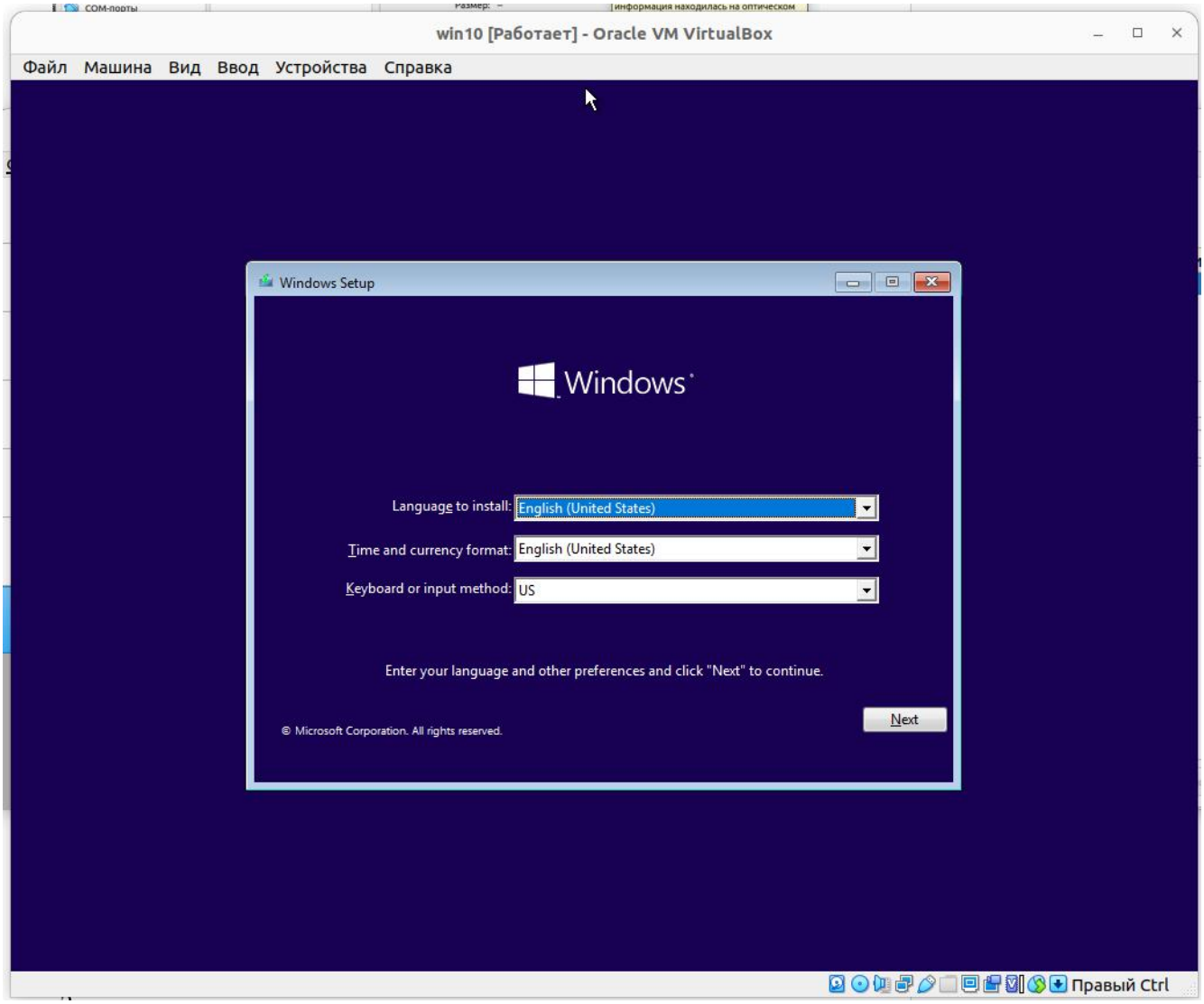

Рисунок 4. Установка Windows 10

3. Подключение учетной записи Администратора
   Перейдите в оснастку “Локальные пользователи и группы”. Win+R -> lusrmgr.msc

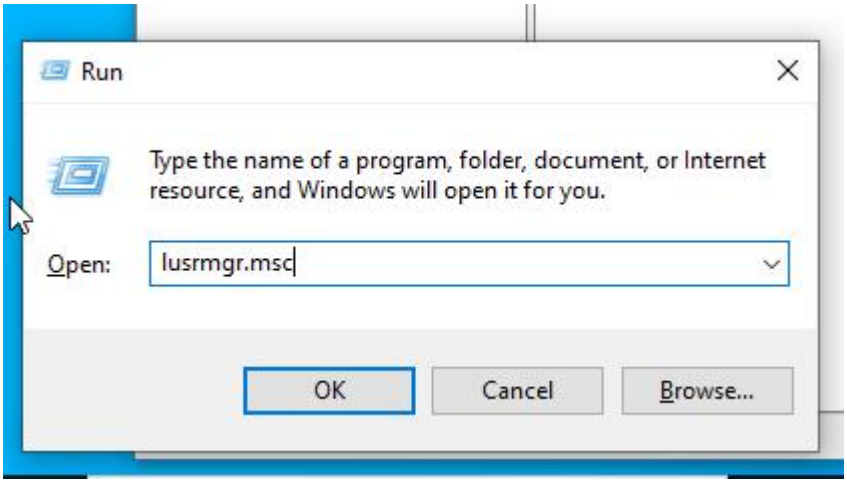

Рисунок 5. Установка Windows 10

Активируйте учетную запись Администратора и задайте пароль.

Завершите работу виртуальной ОС.

1.2. Знакомство с Live CD

Live CD - операционная система, загружающаяся со сменного носителя (CD, DVD, USB-накопитель и т.д.), не требующая для своего функционирования установки на жесткий диск, т.е. портативная.

Скачайте образ Live CD в популярной сборке от Sergey Strelec.

https://disk.yandex.ru/d/dqzMO2-B_DJyWw

В настройках виртуальной ОС перейдите в раздел “Система” и установите порядок загрузки носителей (в приоритете загрузка с оптического диска).

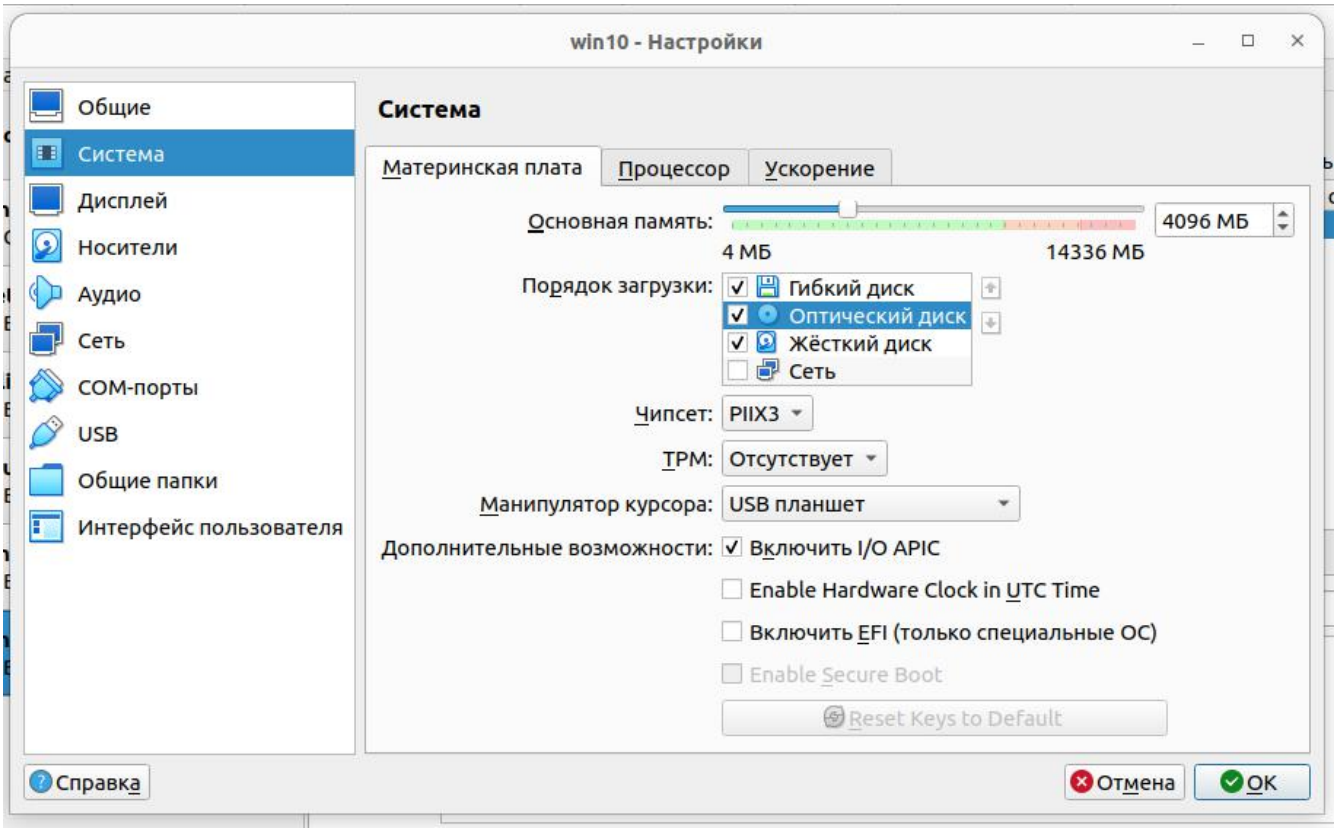

Рисунок 6. Настройка виртуальной ОС

Перейдите в раздел “Носители” и извлеките установочный образ Windows и загрузите образ Live CD. Не забудьте поставить галочку “Живой CD/DVD”.

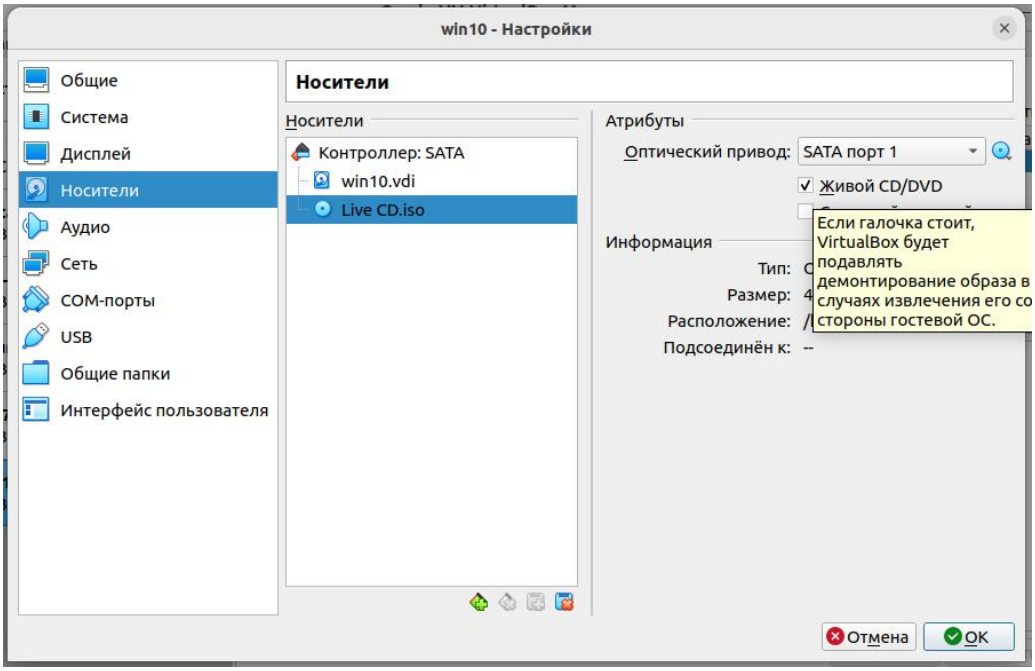

Рисунок 7. Подключение Live CD

После запуска виртуальной машины в приоритетном порядке будет запущен Live CD, выберите разрядность системы в соответствии с разрядностью образа Windows 10.

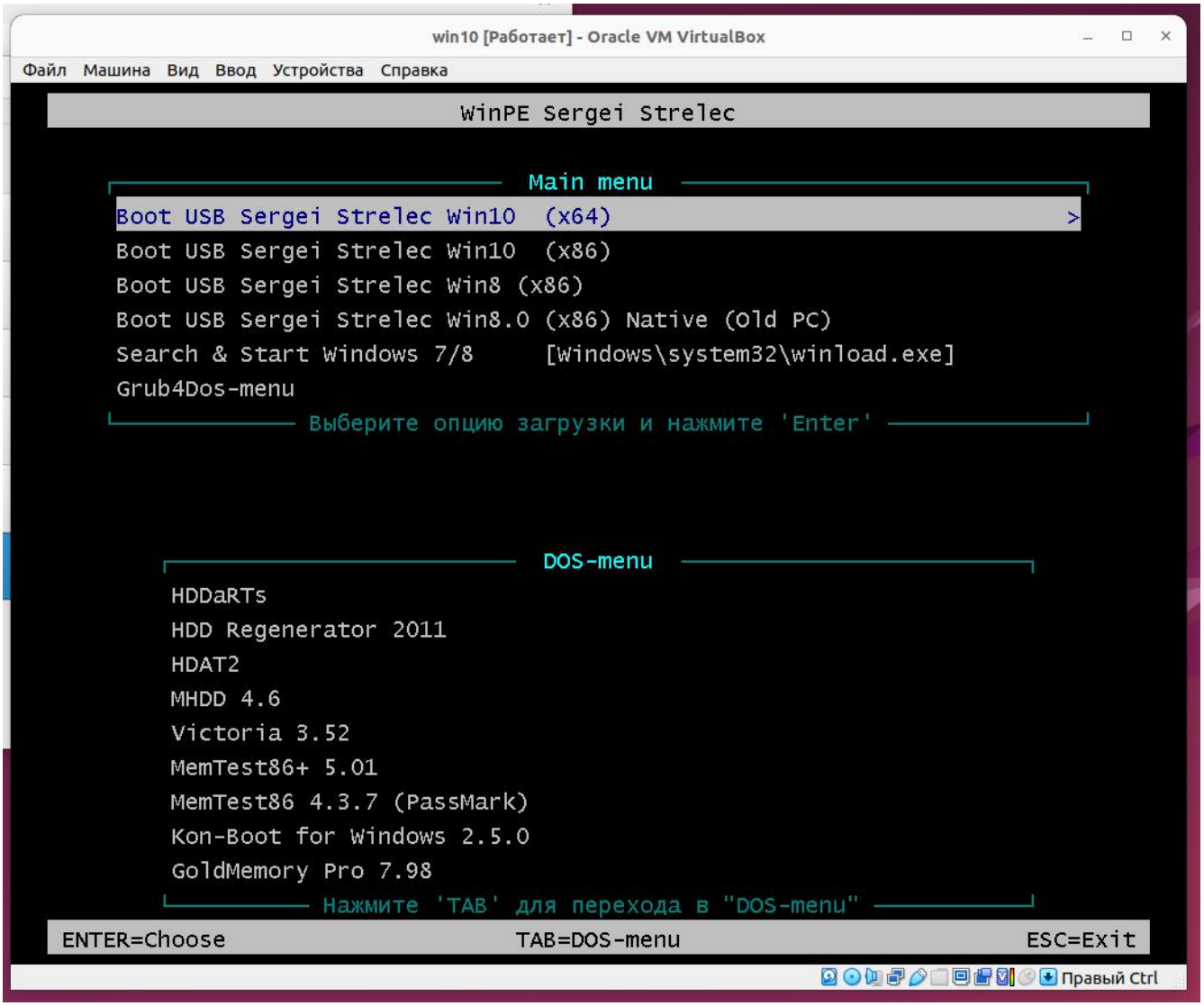

Рисунок 8. Выбор вариантов загрузки Live CD

С помощью любой программы из раздела “Сброс пароля” произведите замену пароля администратора.

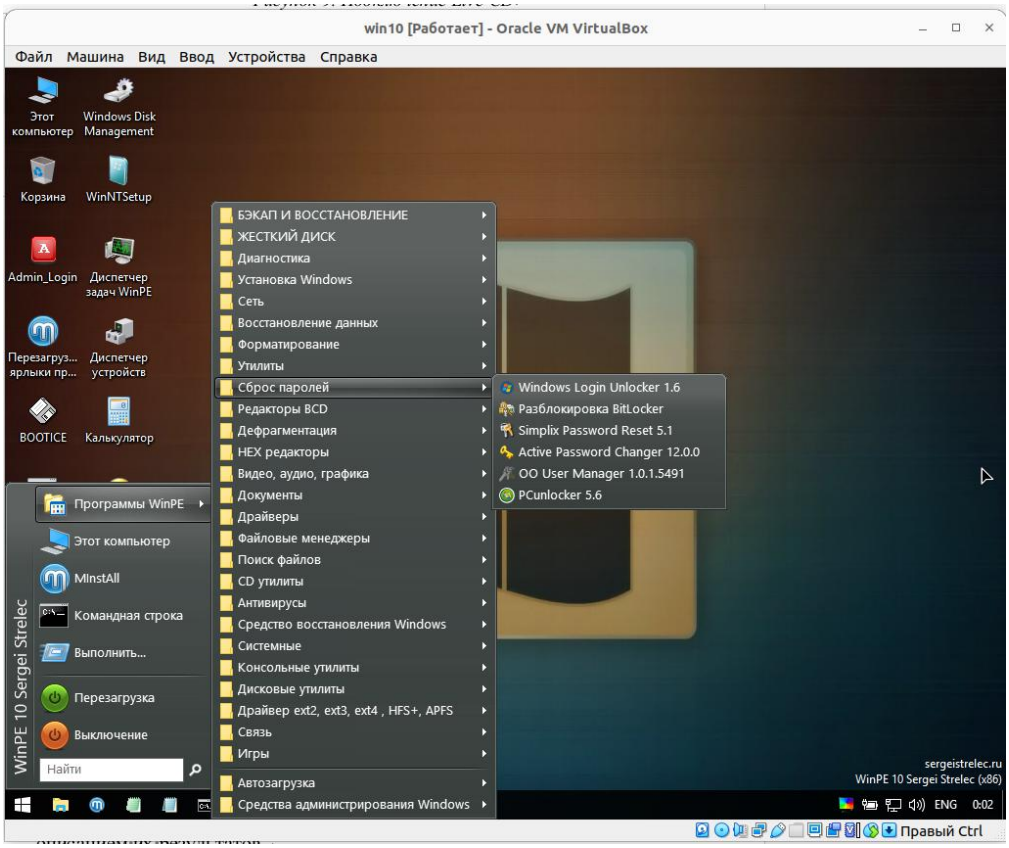

Рисунок 9. Сброс пароля Администратора

После этого вы можете завершить работу системы, но перед запуском виртуальной ОС нужно извлечь образ Live CD из виртуального оптического привода.

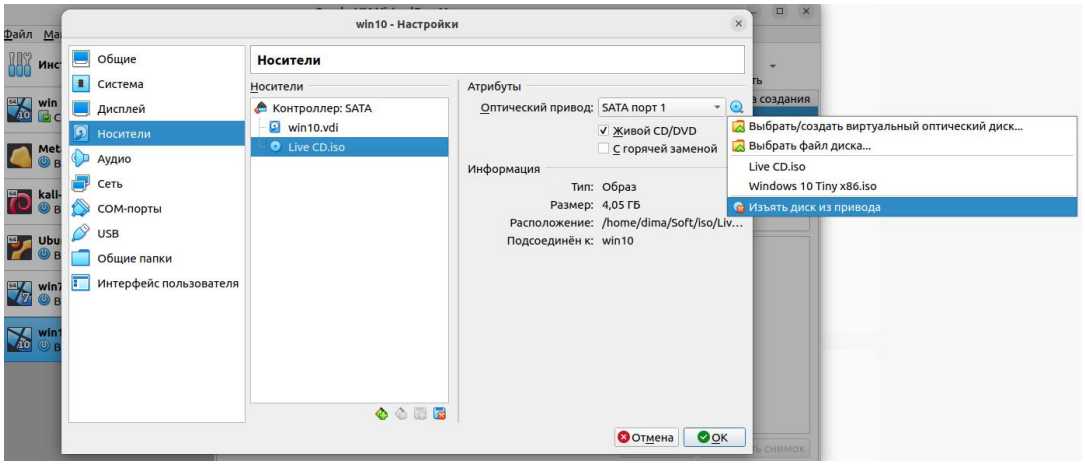

Рисунок 10. Извлечение образа Live CD

Запустите виртуальную ОС и войдите под пользователем Администратор с

новым паролем.

В отчёте о выполненной работе необходимо указать:

- перечень известных систем виртуализации, их отличительные особенности;
- перечень известных образов Live CD, особенности их работы;
- какие встроенные средства защиты и средства защиты информации помогут защититься от уязвимости, которую мы использовали?

1.3. Взаимодействие с гостевой ОС

Для дальнейшей работы с гостевой ОС необходимо установить дополнения гостевой ОС, для этого в окне с Windows 10 выберите вкладку “Устройства” и подключить образ диска дополнений гостевой ОС.

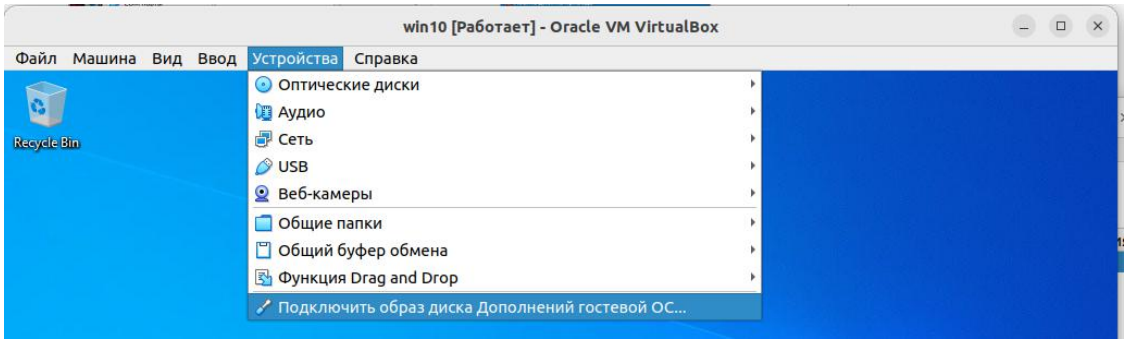

Рисунок 11. Подключение образа диска дополнений гостевой ОС

Выполните установку.

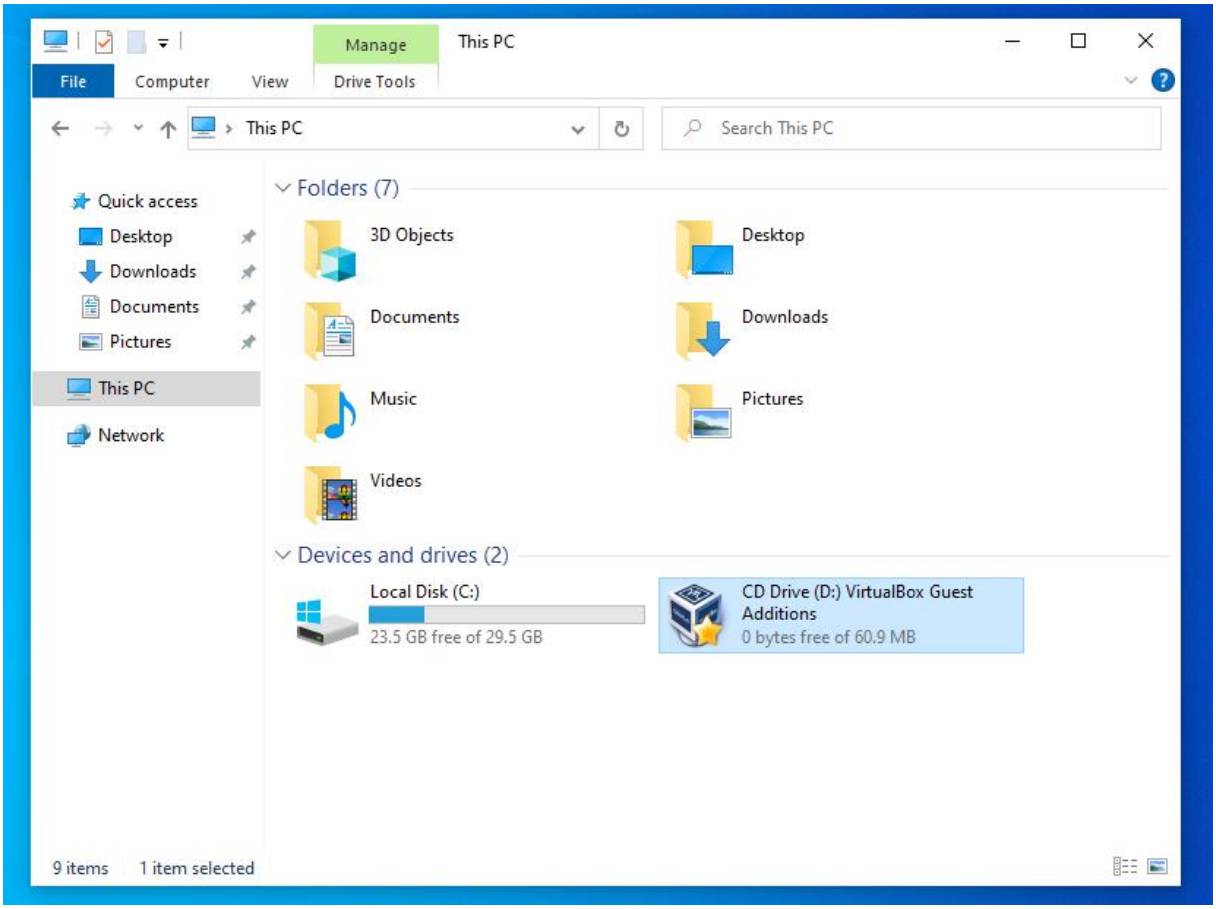

Рисунок 12. Подключение образа диска дополнений гостевой ОС

Для дальнейшей работы с виртуальными ОС нужно научиться обмениваться файлами, сделать это можно несколькими способами. Самый простой способ - это подключение сетевой папки. Перейдите в настройки, раздел “Общие папки”, добавьте общую папку, указав путь к папке на хостовой ОС. Не забудьте поставить галочку “авто-подключение”.

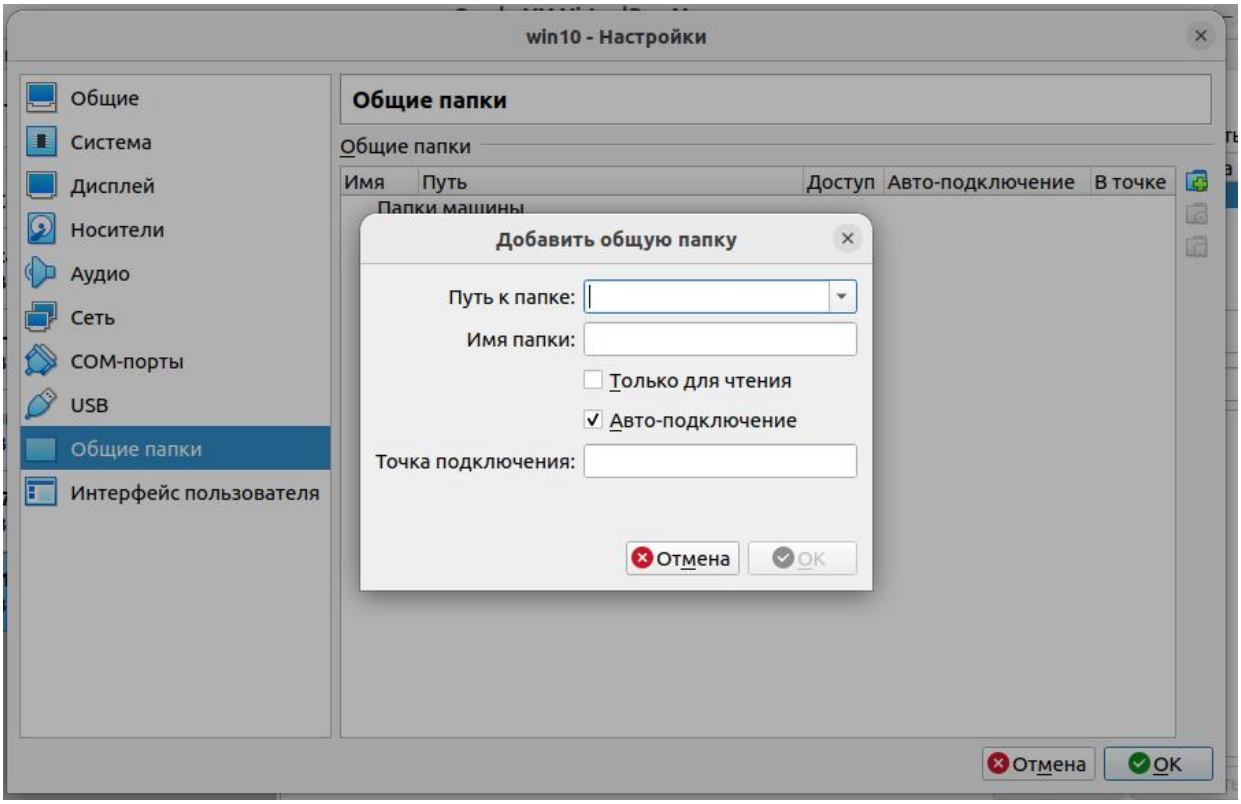

Рисунок 13. Добавление общей папки

Второй способ - подключение USB-носителя. Подключите USB-носитель к хостовой ОС. В окне с Windows 10 выберите вкладку “Устройства” - “USB” - “***Ваш USB-носитель***”.

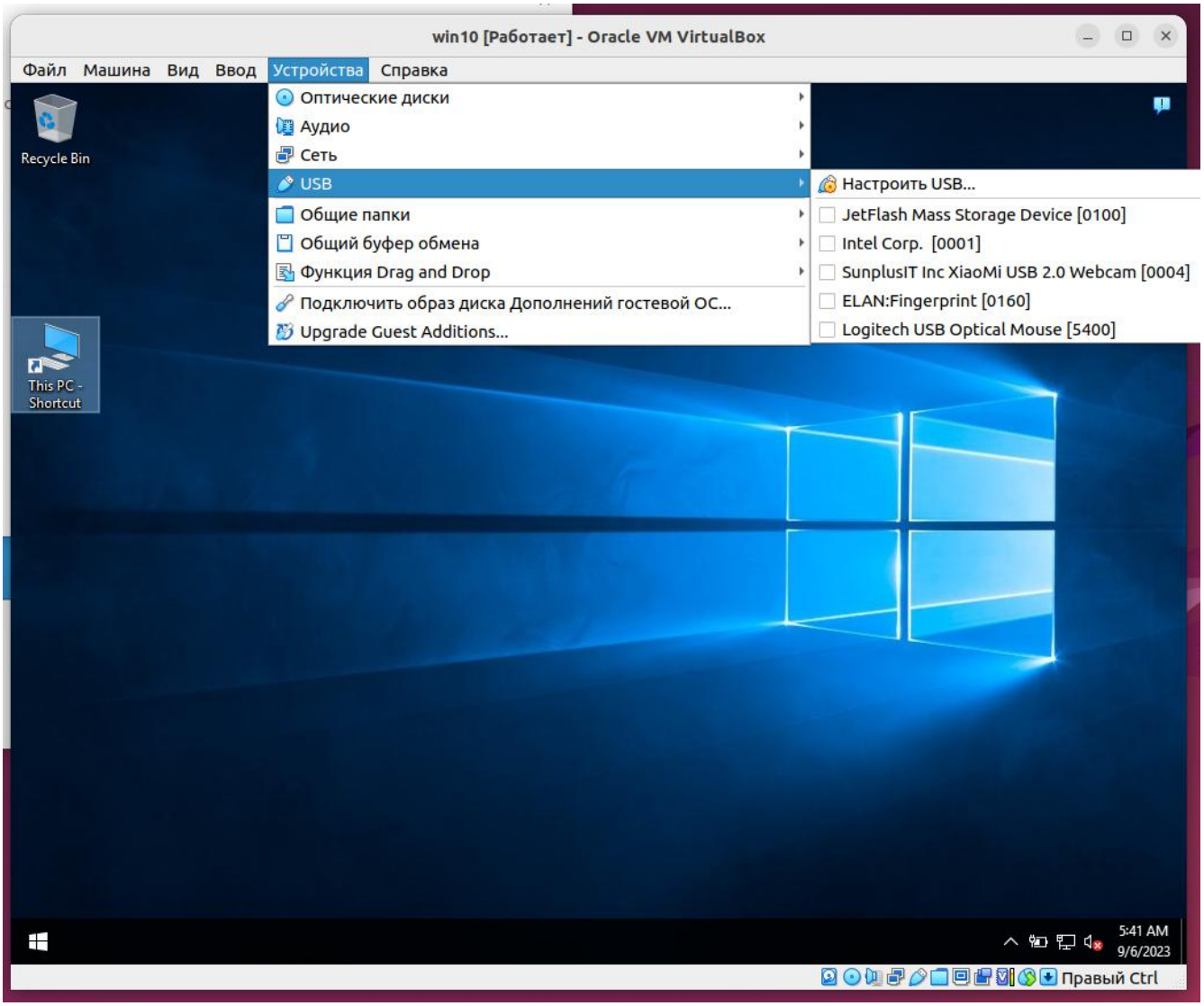

Рисунок 14. Добавление USB-накопителя

Убедитесь, что произошло подключение USB-накопителя.

Рисунок 15. Подключенный USB-накопитель

1.4. Работа с USB-устройствами

Скопируйте на вашу виртуальную ОС программу USB Oblivion.

https://disk.yandex.ru/d/cX87aySlAm1OMA

Запустите сканирование USB-обливион. ВНИМАНИЕ! Галочка “Do real clean” должна быть снята.

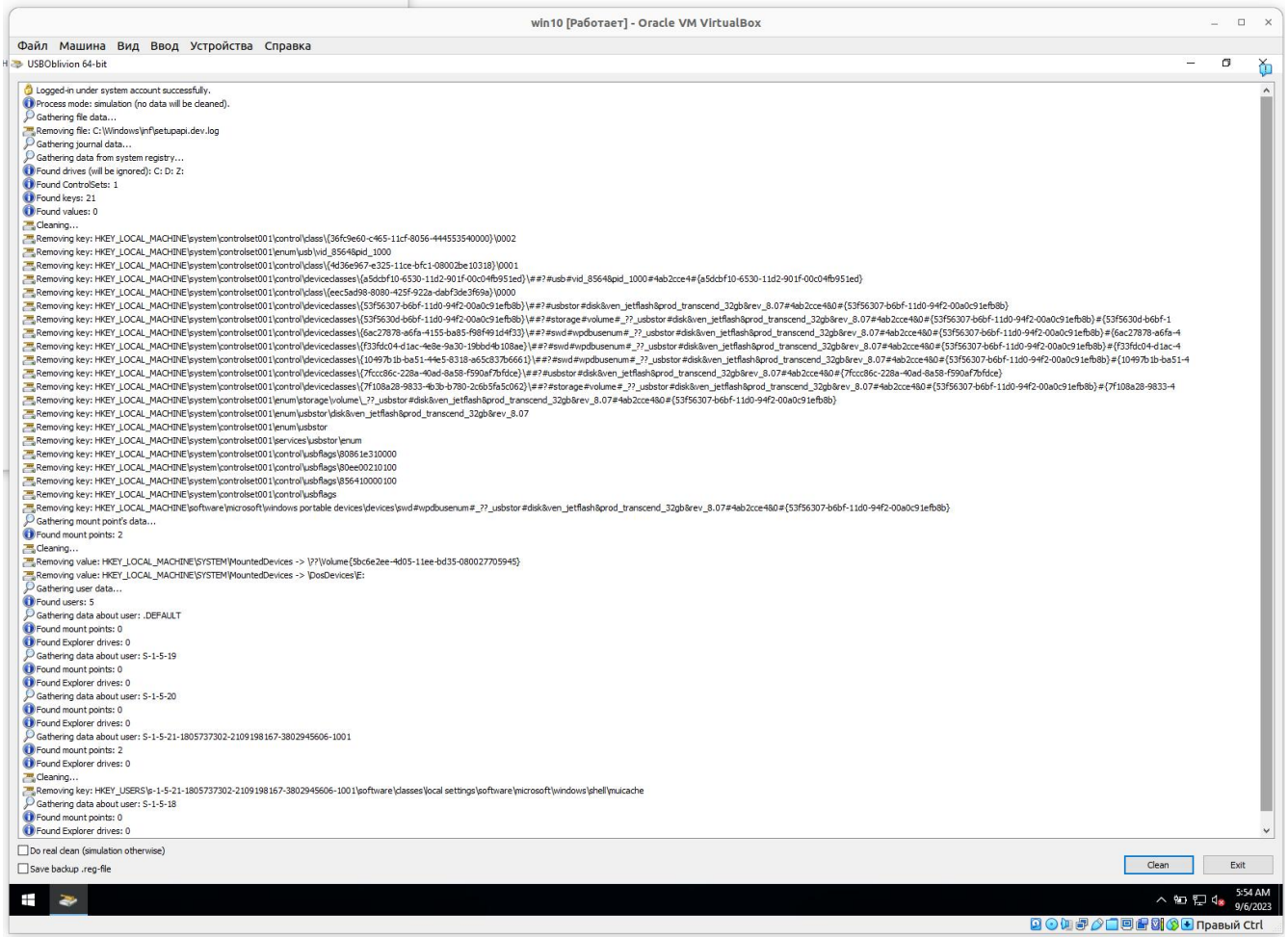

Рисунок 16. Работа программы USB Oblivion

Среди полученных результатов найдите VID, PID, Серийный номер подключенного ранее USB-накопителя и добавьте его в отчет.

Скопируйте и установите на вашу виртуальную ОС программу DeviceLock.

https://disk.yandex.ru/d/a_nTBzPcjIIV-Q

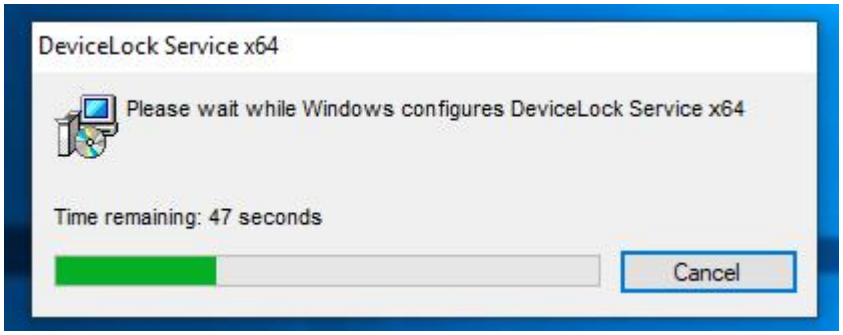

Рисунок 17. Установка программы DeviceLock

Подключите к гостевой ОС любой USB-накопитель. В отчете о проделанной работе дайте описание принципа работы программы Device Lock.

1.5. Восстановление удаленных файлов

В этом разделе мы будем удалять файлы на виртуальной ОС и будем пытаться их восстановить разными способами. Перенесите на вашу виртуальную ОС несколько файлов разных типов.

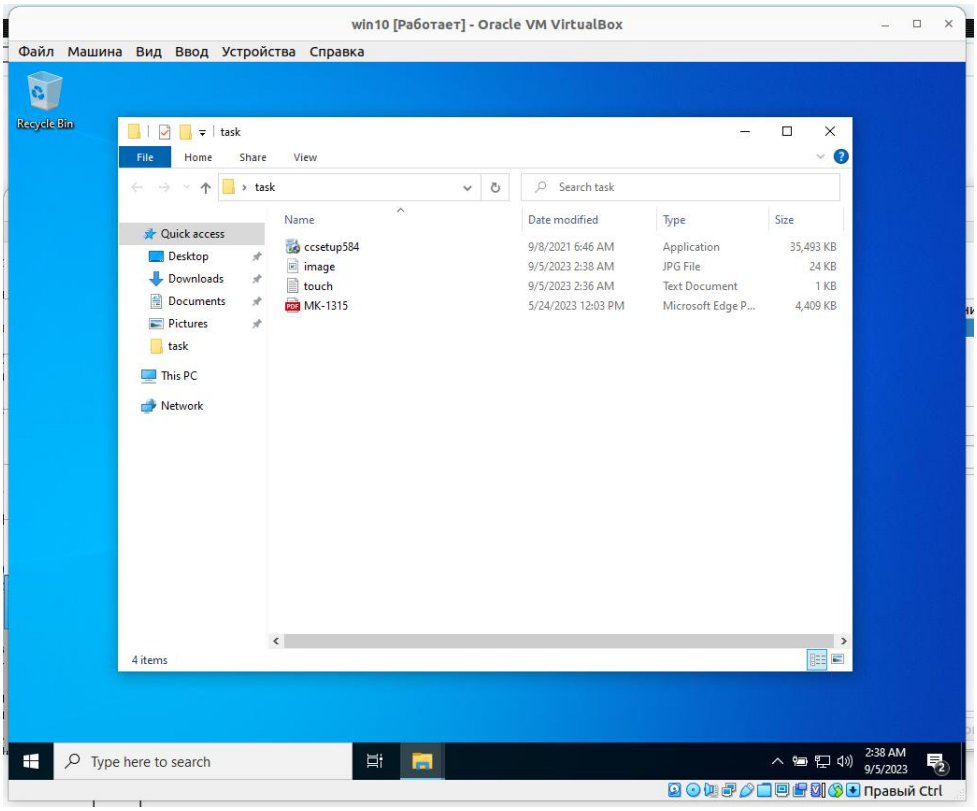

Рисунок 18. Подготовка файлов

Удалите эти файлы любым удобным для вас способом (через Корзину или

напрямую через сочетание клавиш Shift+Del).

Для восстановления файлов воспользуемся утилитой Recuva.

https://disk.yandex.ru/d/BDzBnfT1dKCbfw

Установите ее на виртуальную ОС.

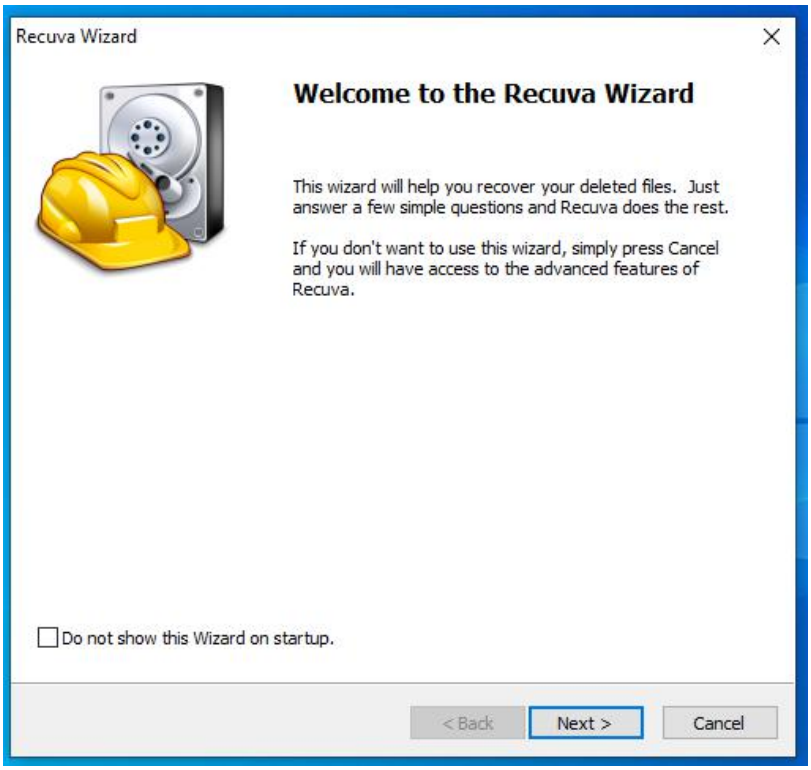

Рисунок 19. Утилита для восстановления файлов Recuva

Для восстановления файлов выберите тип файлов, локацию, где они находились и не забудьте поставить галочку “Enable Deep scan” для углубленного сканирования файловой системы.

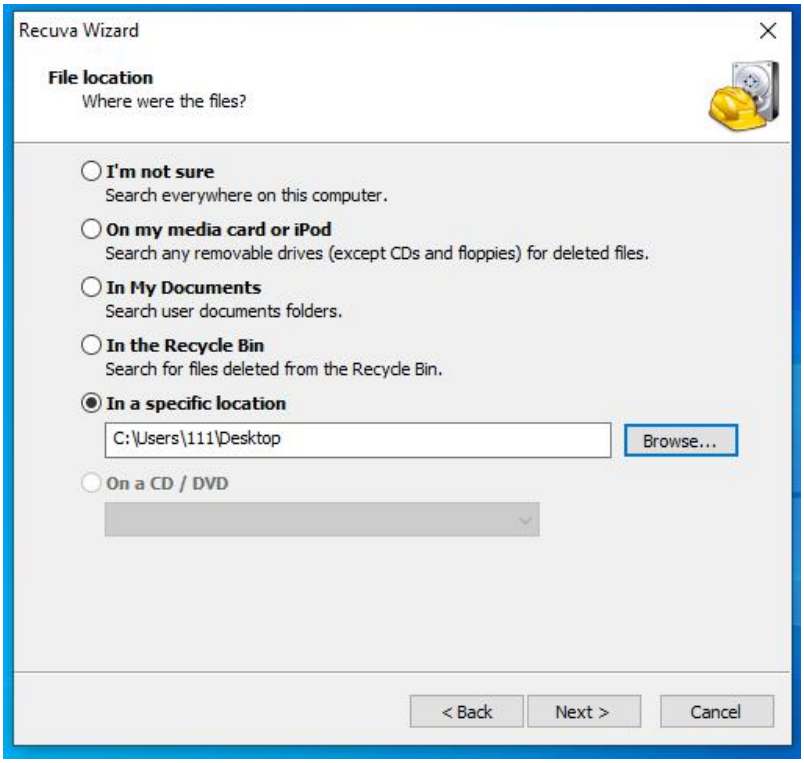

Рисунок 20. Утилита для восстановления файлов Recuva

Проверьте результат восстановления файлов.

Заново скопируйте исходные файлы на гостевую ОС, удалите их и проведите восстановление удаленных файлов используя Live CD (раздел “Восстановление данных”).

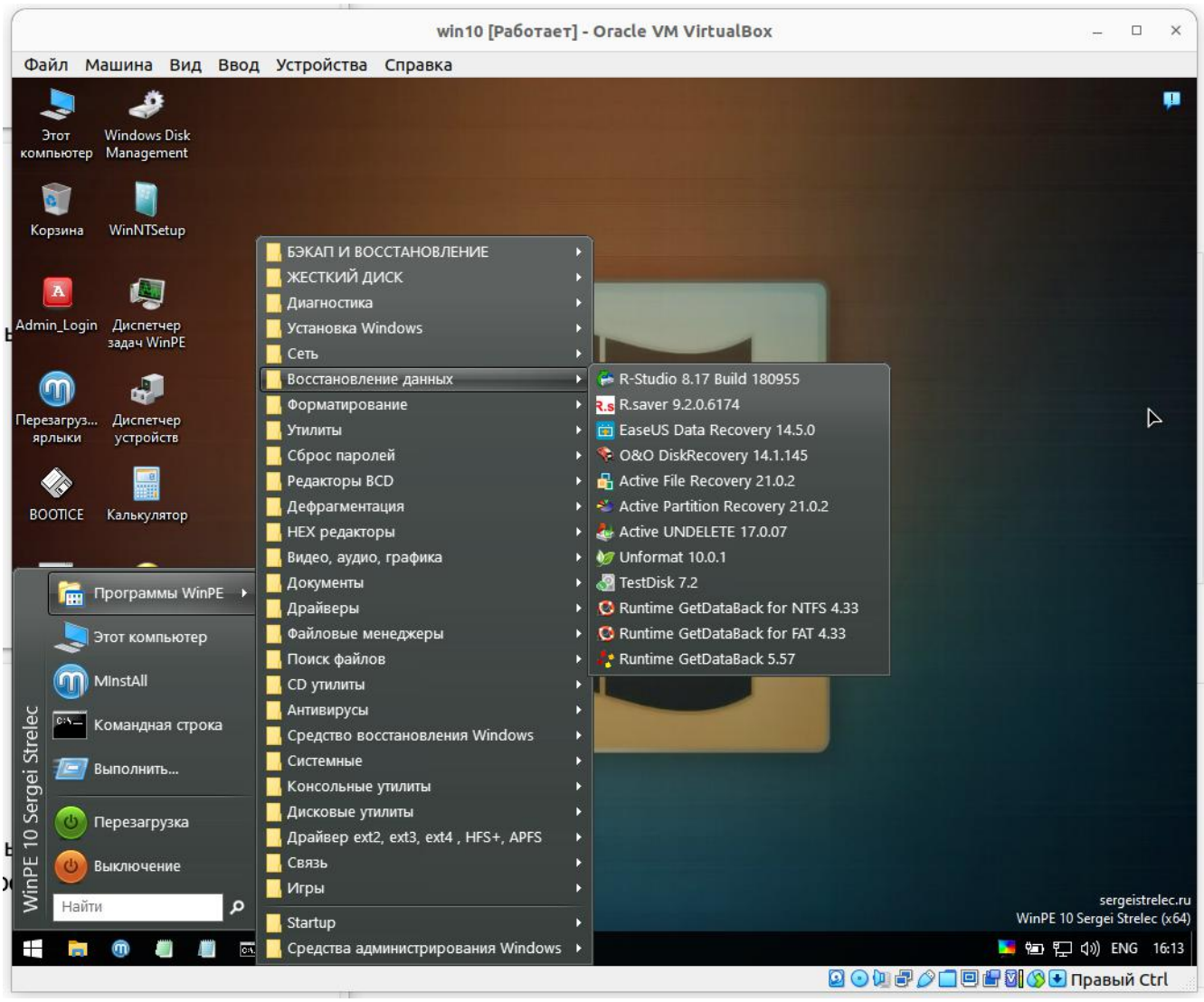

Рисунок 21. Восстановление данных через Live CD

Для восстановления файлов через программу R-STUDIO выберите ваш диск (C:), перейдите по каталогу до папки, где хранились файлы, выберите нужные файлы и нажмите кнопку “Восстановить”.

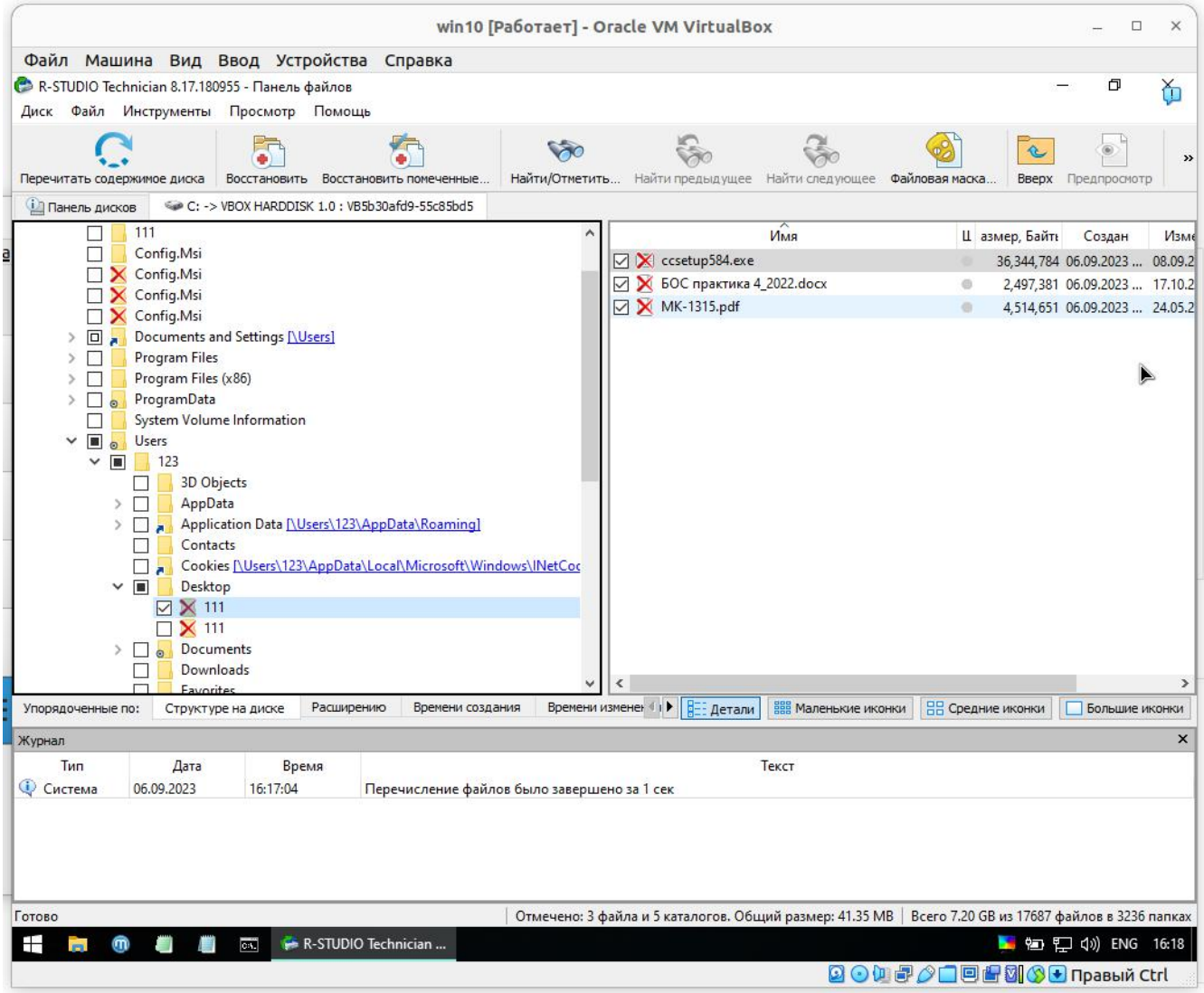

Рисунок 22. Восстановление данных через R-STUDIO

Сравните полученные результаты.

1.6. Стирание свободного пространства

Как вы уже убедились, файловая система NTFS не позволяет полностью удалить файлы с жесткого диска. Существуют программы, которые позволяют затереть свободное пространство на диске, чем значительно уменьшают шансы восстановить удаленные файлы.

Установите программу CCleaner.

https://disk.yandex.ru/d/caZW0LVQ7HY36w

Запустите CCleaner, перейдите в раздел “Tools” - “Drive Wiper”. Запустите стирание со следующими параметрами: Wipe - Free Space Only, Security - Advanced Overwrite (3 passes), Drives - Local Disk (C:).

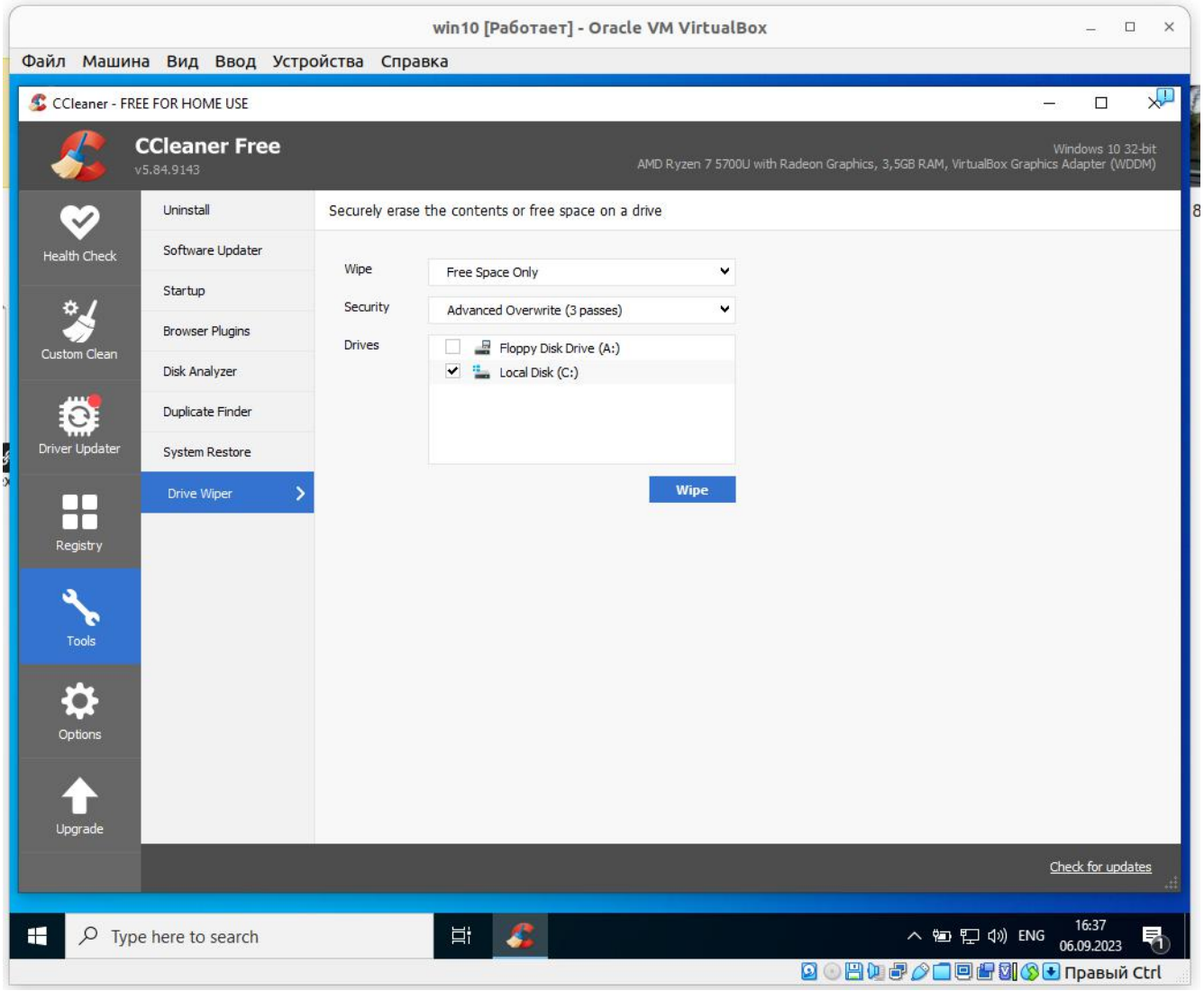

Рисунок 23. Стирание свободного пространства через CCleaner

По окончании процедуры стирания свободного пространства выполните восстановление удаленных файлов через Recuva и Live CD. Проанализируйте полученные результаты.

В отчёте о выполненной работе необходимо указать:

- результаты восстановления файлов;
- результаты восстановления файлов после стирания свободного пространства.

1.7. Шифрование свободного пространства

В системе Windows существует встроенная программа для шифрования файлов. Полное описание можно посмотреть на сайте Microsoft

https://learn.microsoft.com/ru-ru/windows-server/administration/windows-commands/cipher

Заново скопируйте исходные файлы на гостевую ОС, удалите их, в командной строке выполните команду cipher /W:*\.

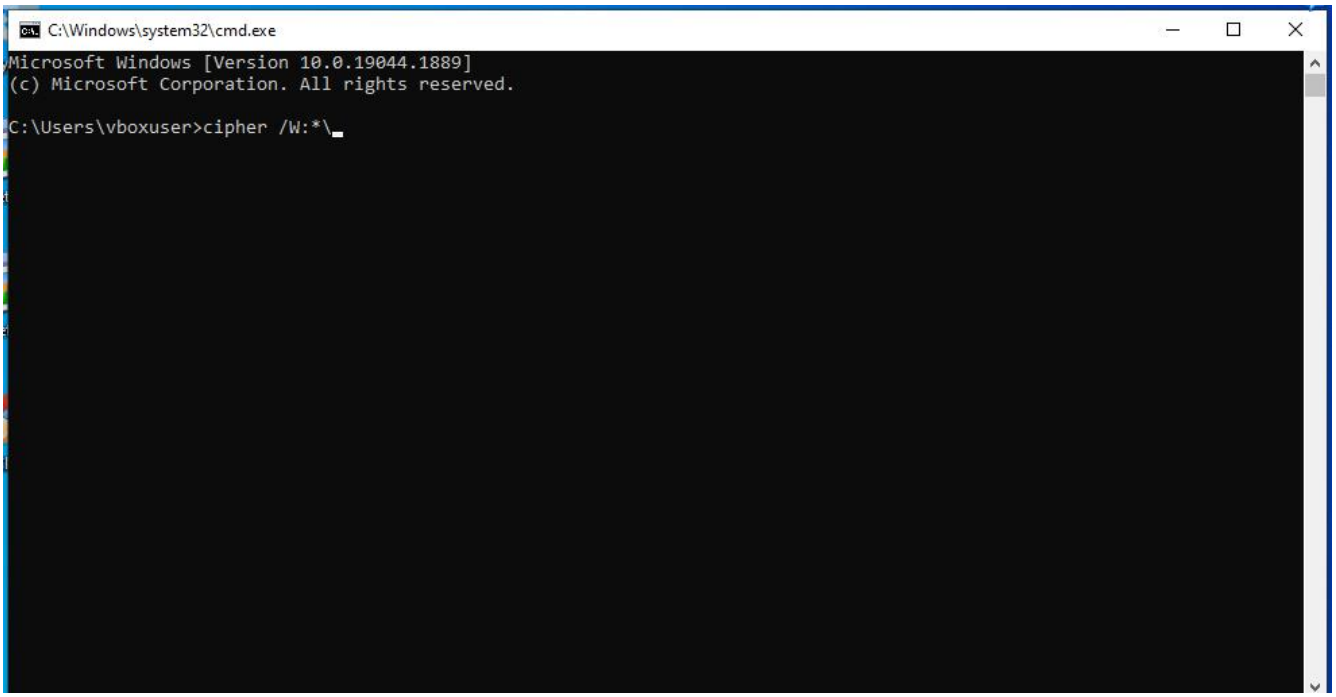

Рисунок 24. Использование программы cipher

В отчёте о выполненной работе необходимо указать:

- описание программы cipher;
- описание использованных ключей.