Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий Дисциплина:

«Программно-аппаратные средства защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

«Виртуализация и контейнеризация»

Выполнили:

Нгуен Тхе Вьет, студент группы N3347

Чу Ван Доан, студент группы N3347

Доан Тхи Хоай Тхыонг, студентка группы N3345

Чан Бао Линь, студентка группы N3346

Проверил:

Калабишка Михаил Михайлович, Преподаватель ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2024 г

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель работы – обеспечение защиты виртуализации.

Для достижения поставленной цели необходимо решить следующие задачи:

- выбрать технологию виртуализации/контейнеризации,
- изучить механизмы защиты выбранной технологии,
- определить выполняют ли механизмы технологии виртуализации требования законодательства,
- обеспечить защиту технологии в соответствии с требованиями документа,
- проверить все реализованные механизмы,
- составить отчет.

ОБЩИЕ ПОЛОЖЕНИЯ

Виртуализация представляет собой создание вычислительной среды, в которой разные виртуальные машины могут работать на одних и тех же физических ресурсах, полностью изолированные друг от друга. Иными словами, это возможность создания программных аналогов различных физических объектов, таких как компьютеры, хранилища данных, сети, серверы и приложения. Примером этого может служить использование нескольких операционных систем на одном устройстве, при этом все ОС и их вычислительные процессы находятся в изоляции друг от друга.

Контейнеризация — метод, с помощью которого программный код упаковывается в единый исполняемый файл вместе с библиотеками и зависимостями, чтобы обеспечить его корректный запуск. Такие файлы называют контейнерами. Контейнеры можно разворачивать в разных средах и там управлять их работой. Если код разрабатывается в определенной вычислительной среде (например, при переносе на новый сервер), часто возникают ошибки связанные с тонкостями настройки. При контейнеризации таких проблем значительно меньше. Ведь контейнер не зависит от настроек основной операционной системы и может работать на любой платформе или в облаке.

1. ХОД РАБОТЫ

1.1 Выбрать технологию виртуализации/контейнеризации

В своей работе для рассмотрения мы выбрали технологию виртуализации. В качестве программного обеспечения виртуализации мы выбрали Oracle VM VirtualBox. В качестве гостевой операционной системы был взят Windows 7.

1.2 Изучить механизмы защиты выбранной технологии

При оценке соответствия законодательным требованиям мы руководствовались аспектами безопасности информации, которые были классифицированы по категориям объектов защиты и описаны в разделе 6 стандарта ГОСТа Р 56938-2016 "Защита информации при использовании технологий виртуализации" [1]:

− защита средств создания и управления виртуальной инфраструктурой;

− защита виртуальных вычислительных систем;

− защита виртуальных систем хранения данных;

− защита виртуальных каналов передачи данных;

− защита отдельных виртуальных устройств обработки, хранения и передачи данных;

− защита виртуальных средств защиты информации и средств защиты информации, предназначенных для использования в среде виртуализации.

Согласно Приказу ФСТЭК России №17, системы виртуализации должны

соответствовать следующим требования для защиты информации (Таблица 1):

Таблица 1 – Требования ФСТЭК

ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей

1.2 Определить выполняют ли механизмы технологии виртуализации требования законодательства

Наличие и отсутствие мер непосредственно в VirtualBox приведено в таблице (таблица 2)

Таблица 2 – Перечень мер Приказа ФСТЭК №17, реализованных в VirtualBox

Условное обозначение и номер меры	Наличие реализации меры непосредственно в VirtualBox
ЗСВ.1	+
ЗСВ.2	+
ЗСВ.3	+
ЗСВ.4	+
ЗСВ.5	+
ЗСВ.6	+
ЗСВ.7	+
ЗСВ.8	+
ЗСВ.9	–
ЗСВ.10	+

ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.

Логирование и аутентификация присутствуют в VirtualBox по умолчанию (Рисунок1).

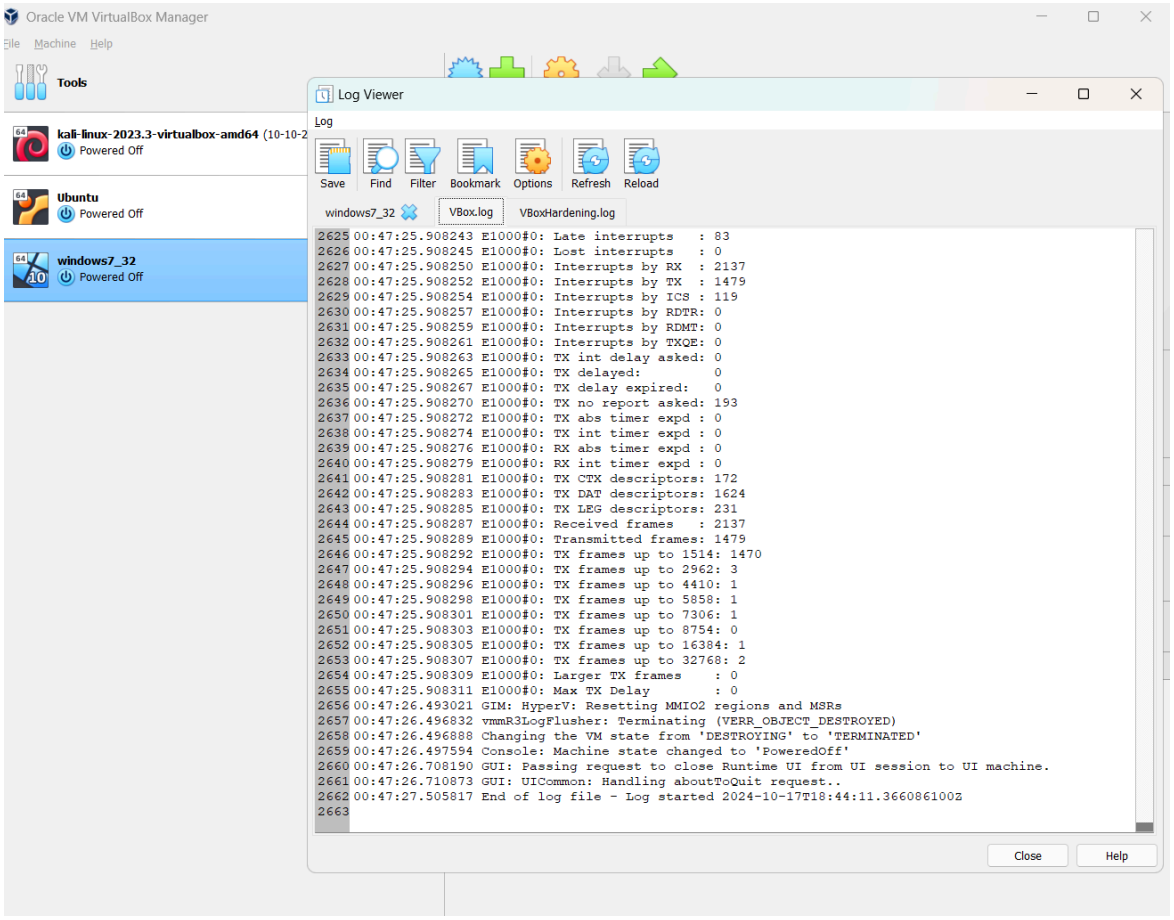

Рисунок 1 – Логи VirtualBox.

Также, можно выбрать пароль, для входа в виртуальную систему (Рисунок 2).

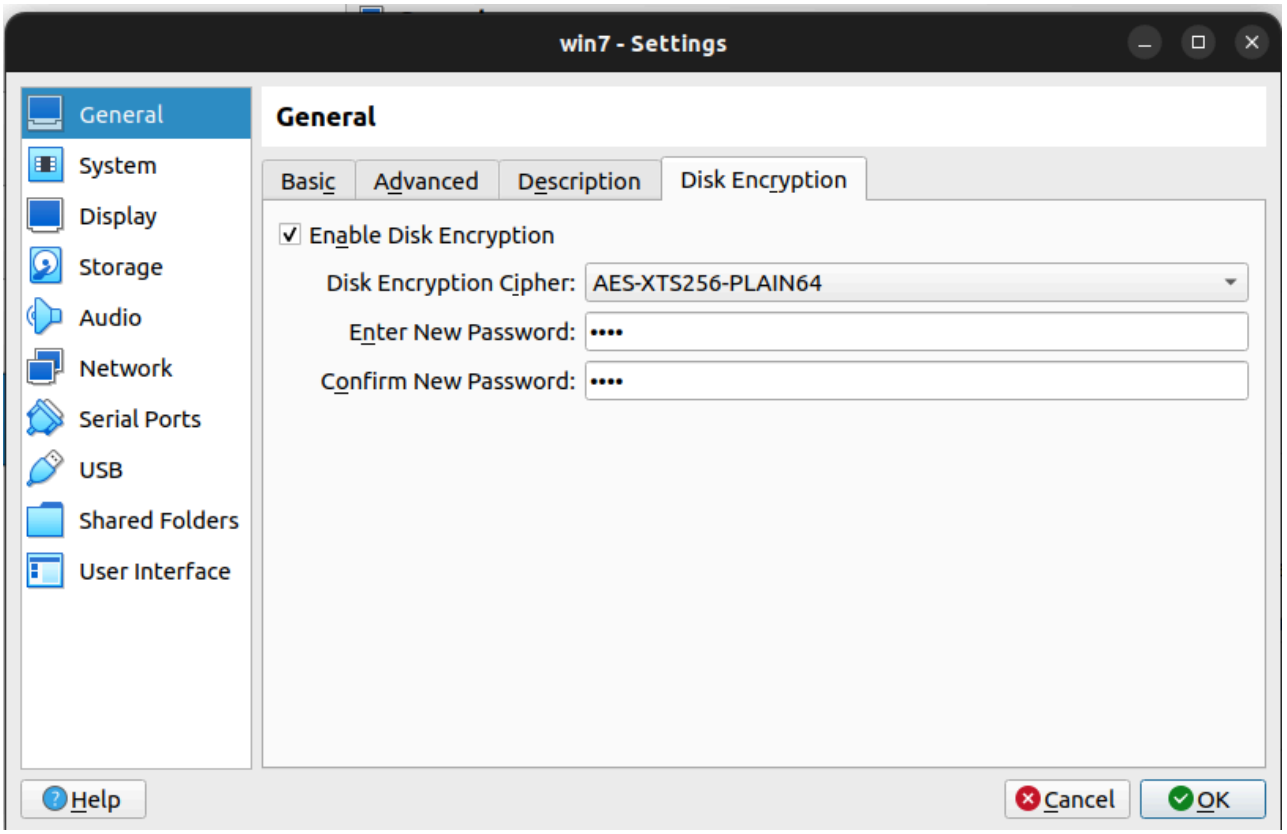

Рисунок 2 – Настройка аутентификации для доступа к виртуальной машине.

При установке виртуальной системы есть возможность создания пароля для входа в гостевую ОС (Рисунок 3).

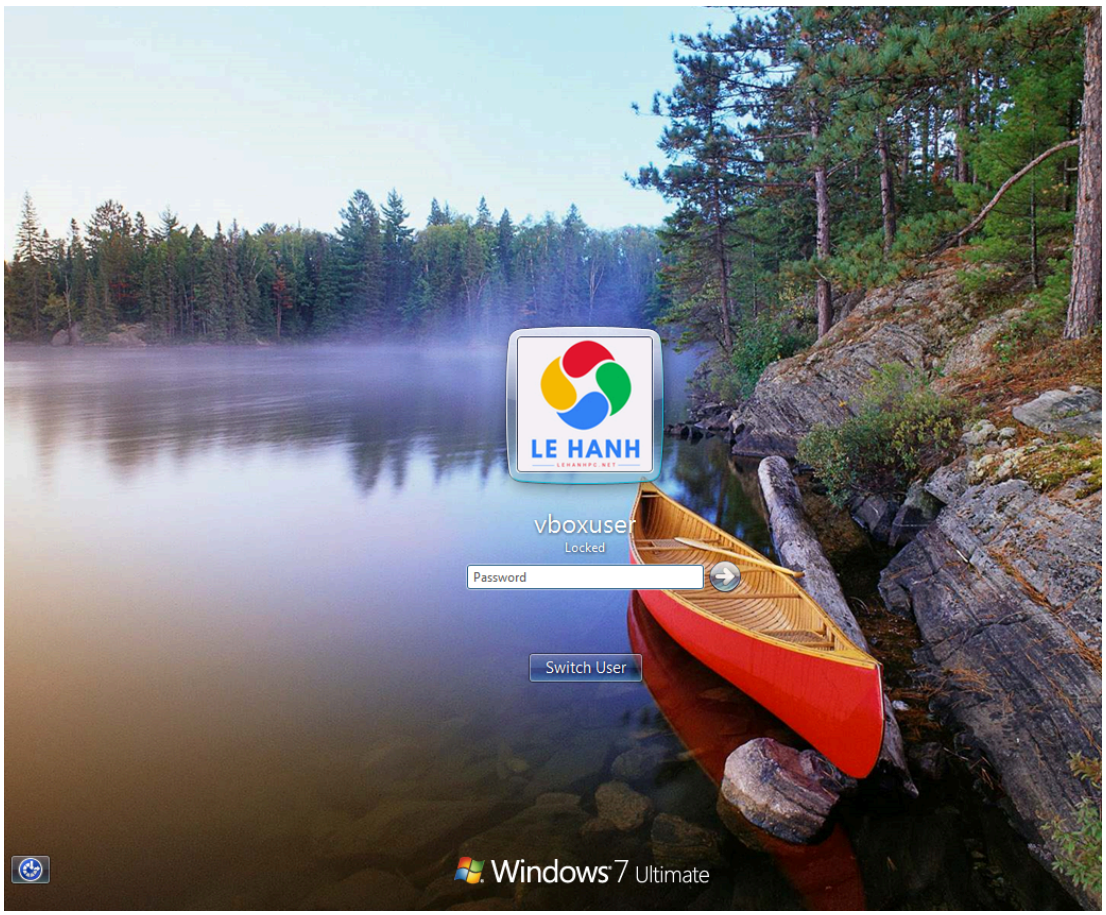

Рисунок 3 – Запрос пароля в гостевой ОС

ЗСВ.2 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин.

В самой виртуальной среде можно добавить учетную запись и дать права администратора, либо обычного пользователя (Рисунок 4).

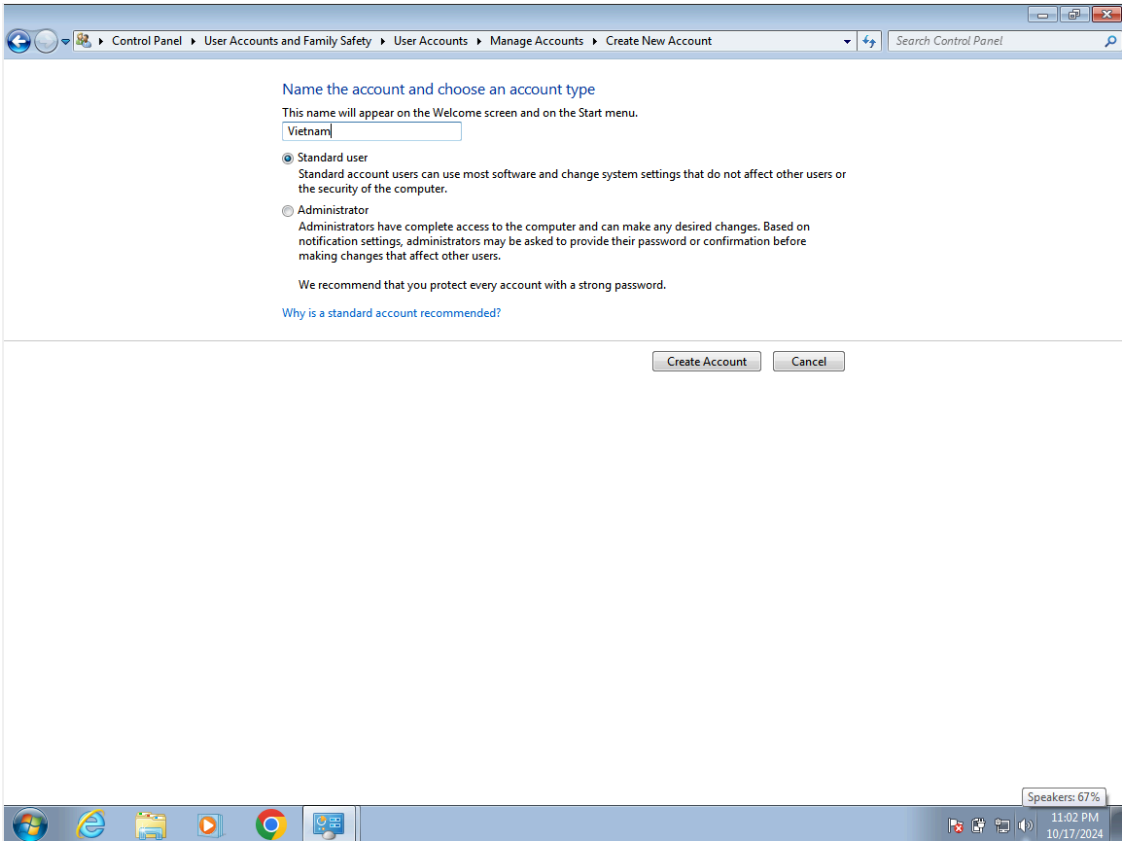

Рисунок 4 – Создание других учетных записей

ЗСВ.3 Регистрация событий безопасности в виртуальной инфраструктуре. По умолчанию есть в VirtualBox и в гостевой ОС (Рисунок 5).

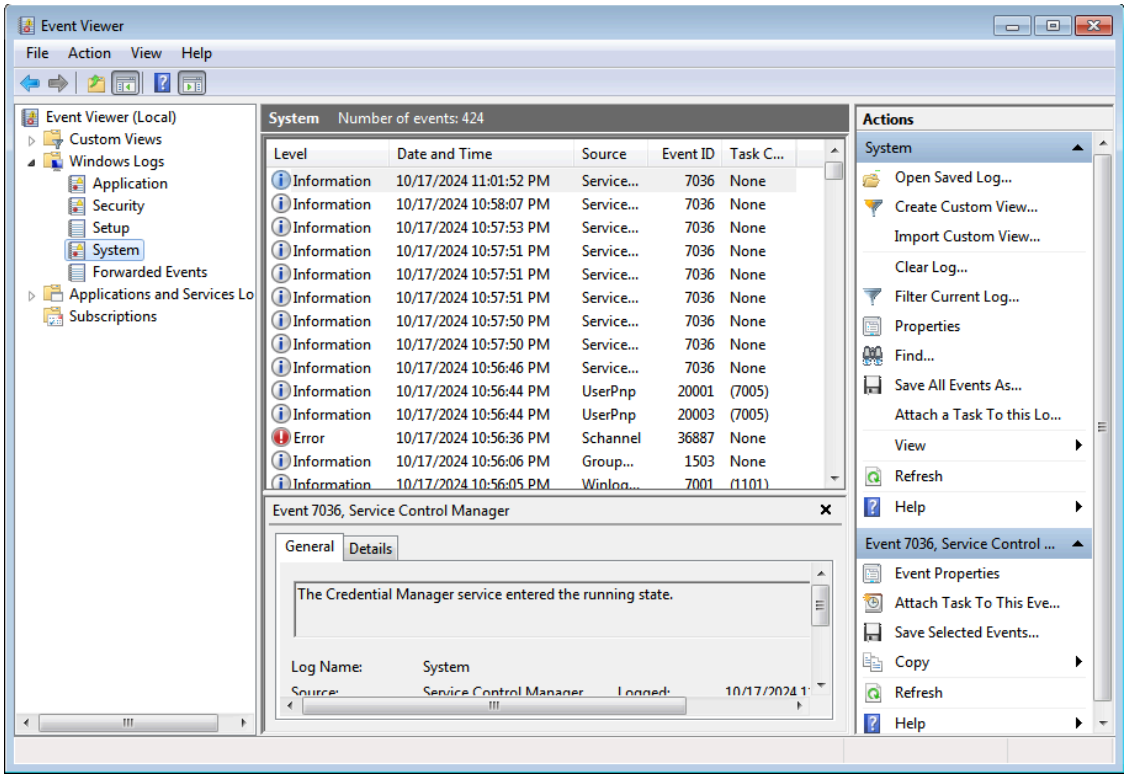

Рисунок 5 – Логирование событий в Windows7

ЗСВ.4 Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры.

В нашей, для примера взятой, гостевой ОС по умолчанию встроен Windows Firewall (Рисунок 6). В которой можно выборочно блокировать и ограничивать входящий и исходящий трафик. Также, на VirtualBox можно настроить возможность установки дополнительных адаптеров для виртуальной машины.

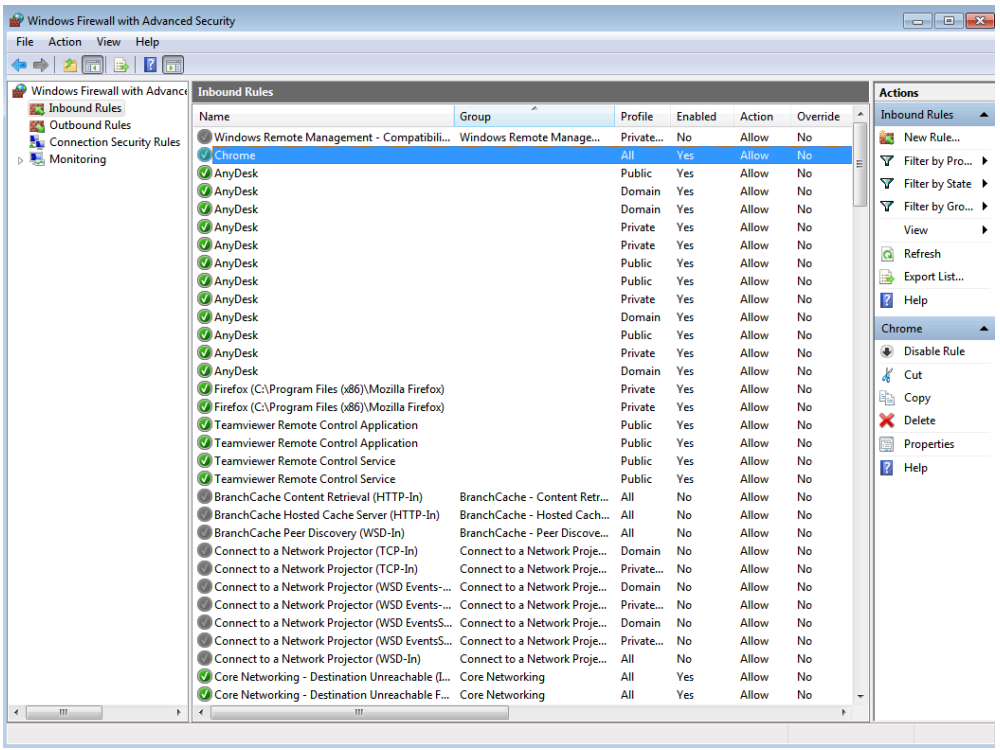

Рисунок 6 – Настройка фаервола

ЗСВ.5 Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией.

Мера предусматривает обеспечение доверенной загрузки серверов виртуализации, ВМ и серверов управления виртуализацией. Данная мера логически делится на две – с одной стороны, это доверенная загрузка физических серверов (гипервизора, системы управления виртуализацией и т.д.), с другой – доверенная загрузка ВМ. Первое выполняется с помощью классических аппаратных средств доверенной загрузки, второе – только с помощью наложенного средства защиты виртуализации. (Рисунок 7).

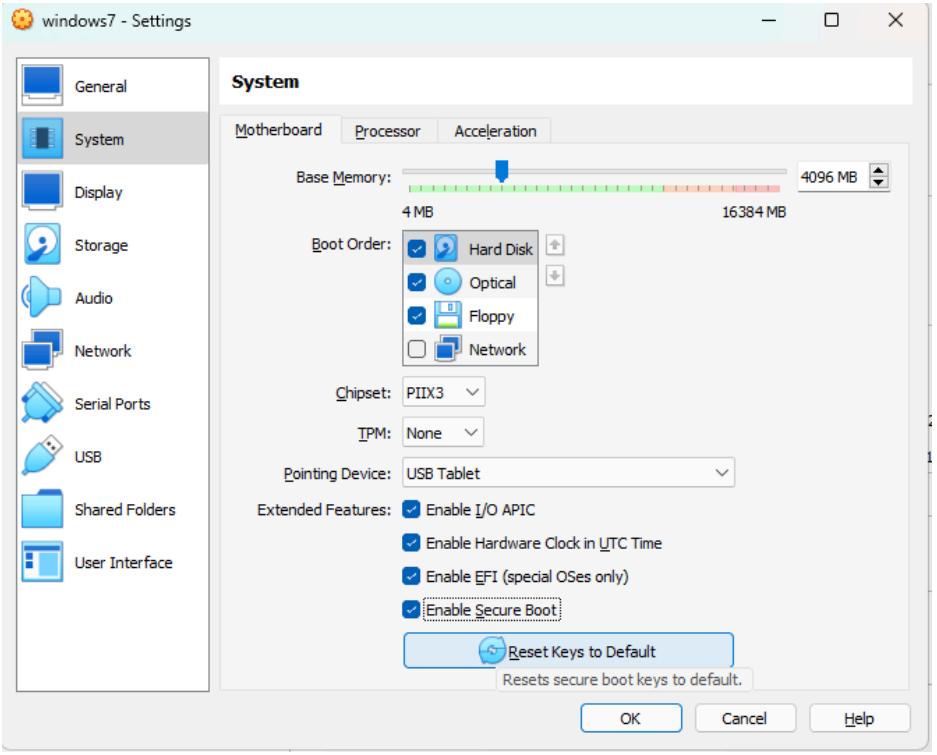

Рисунок 7 – Настройка доверенной загрузки.

ЗСВ.6 Управление перемещением виртуальных машин (контейнеров) обрабатываемых на них данных.

Конфигурацию ВМ можно экспортировать в облако. Также экспортировать конфигурацию можно и в основную систему или на съемный носитель (Рисунок 8).

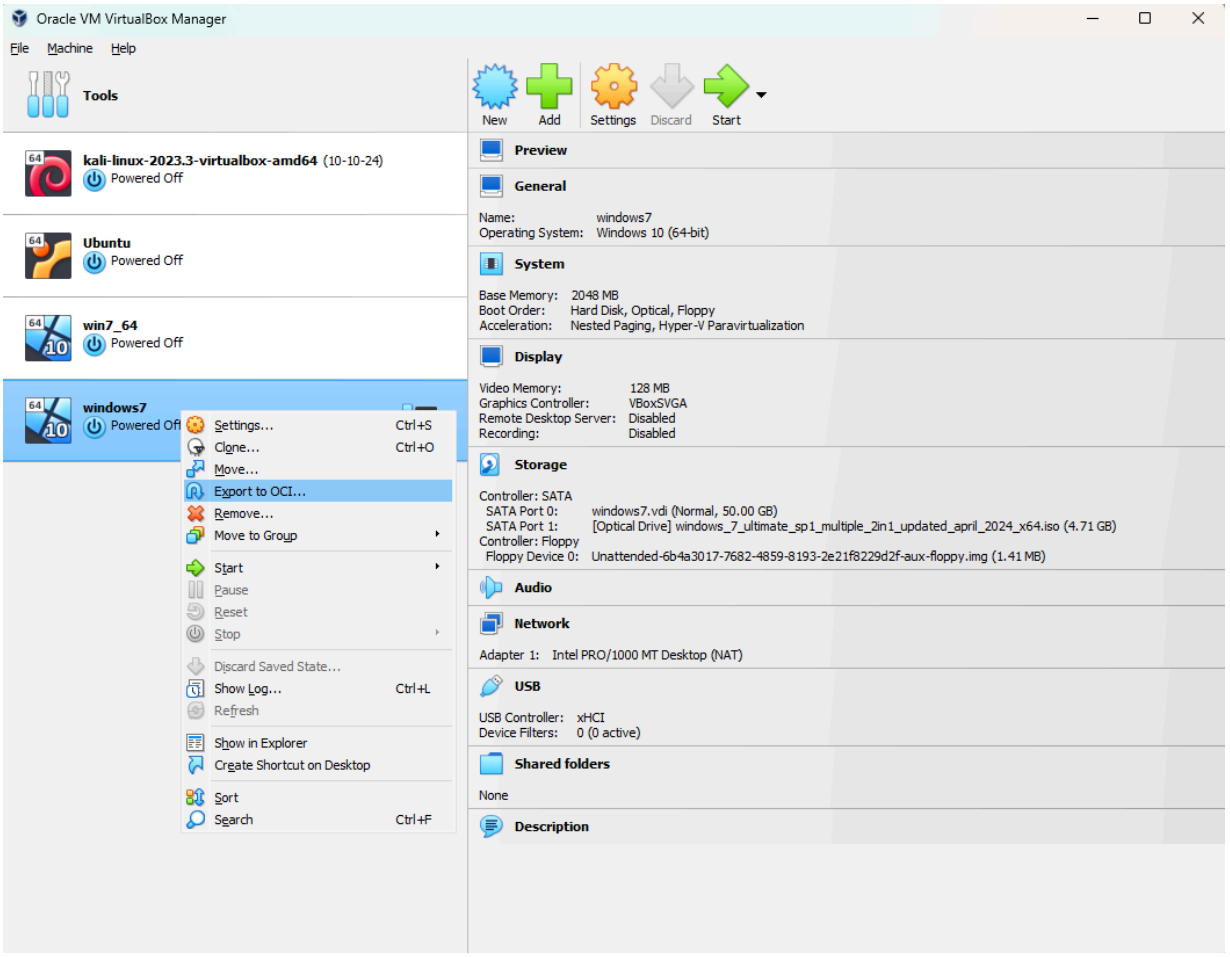

Рисунок 8 – Экспорт конфигурации ВМ

ЗСВ.7 Контроль целостности виртуальной инфраструктуры и ее конфигураций.

Контроль целостности встроен в VirtualBox. Например, при попытке изменить файл с расширением .vdi и открыть ВМ через VirtualBox мы получаем ошибку целостности (Рисунок 9).

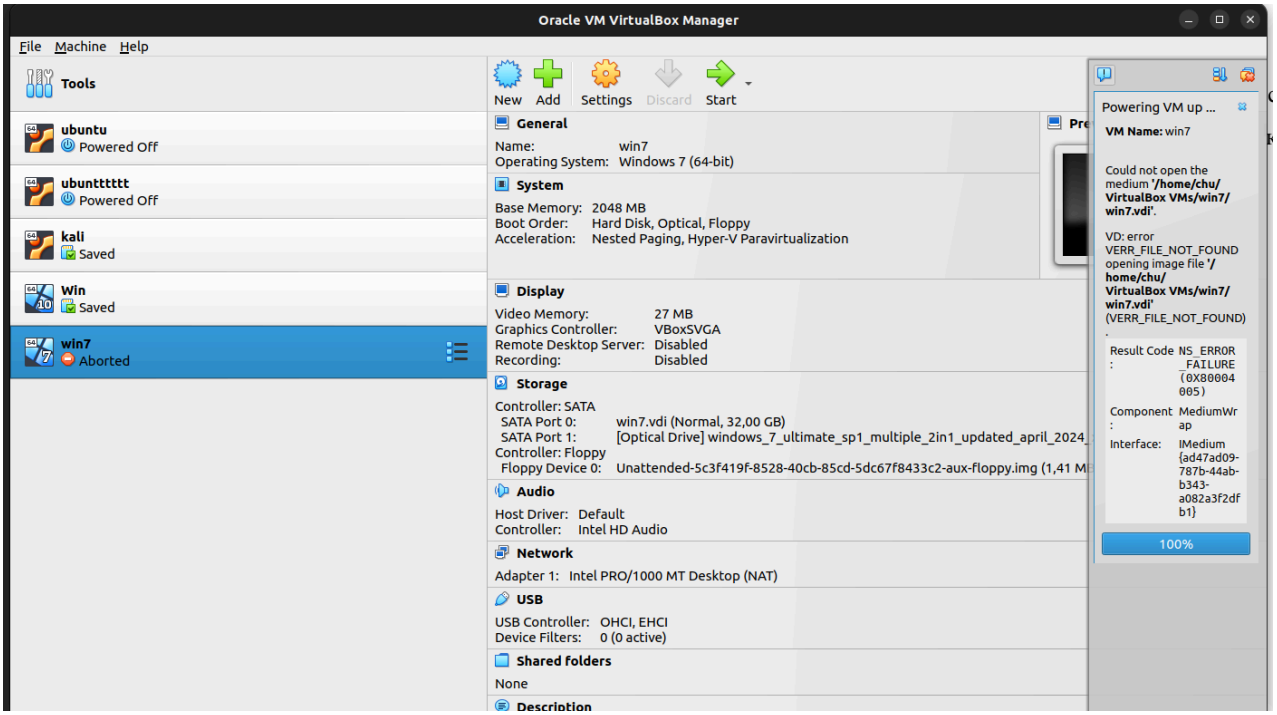

Рисунок 9 – Ошибка при контроле целостности

ЗСВ.8 Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры.

В VirtualBox есть резервное копирование внутри ВМ – создание Снимков (Рисунок 10).

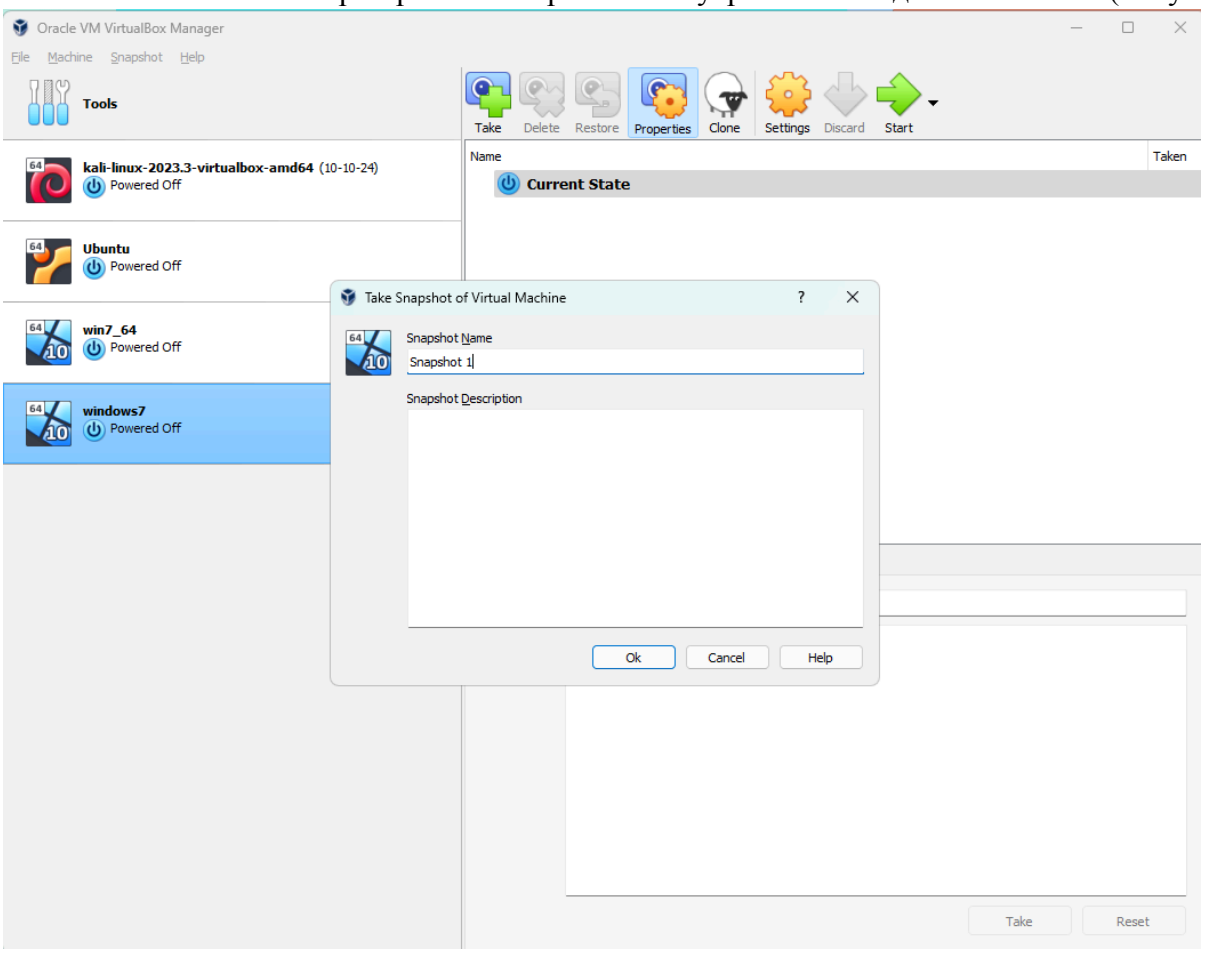

Рисунок 10 – Создание снимка

Присутствует возможность копирования конфигурационного файла ВМ через «Менеджер виртуальных носителей» (Рисунок 11).

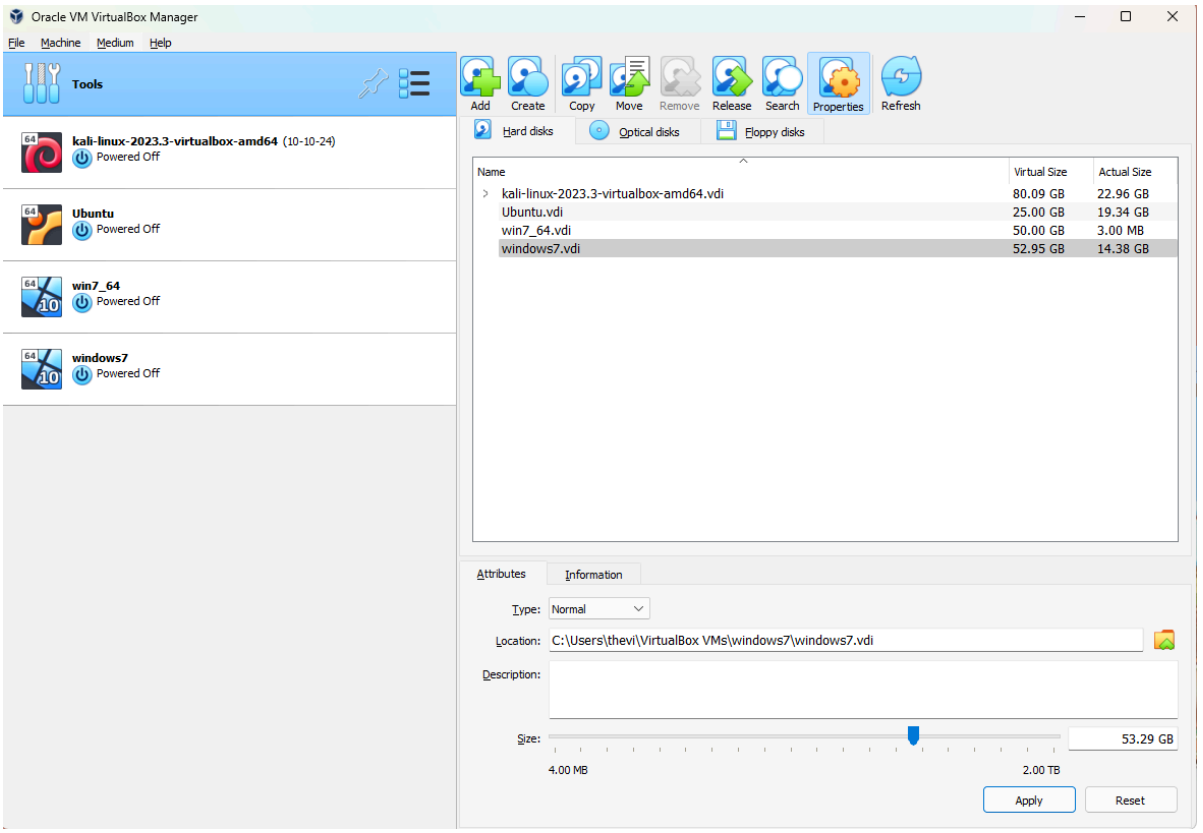

Рисунок 11 – Копирование через менеджер виртуальных носителей

ЗСВ.9 Реализация и управление антивирусной защитой в виртуальной инфраструктуре.

Напрямую в VirtualBox антивирус не встроен, поэтому его можно скачать отдельно в виртуальной среде.

ЗСВ.10 Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем (или) группой пользователей.

Мы можем на самой ВМ, например, настроить права доступа пользователей, тем самым сегментировать инфраструктуру (Рисунок 12) . Также есть возможность внутри самих ВМ настроить определенные локальные сети различных типов (Рисунок 13).

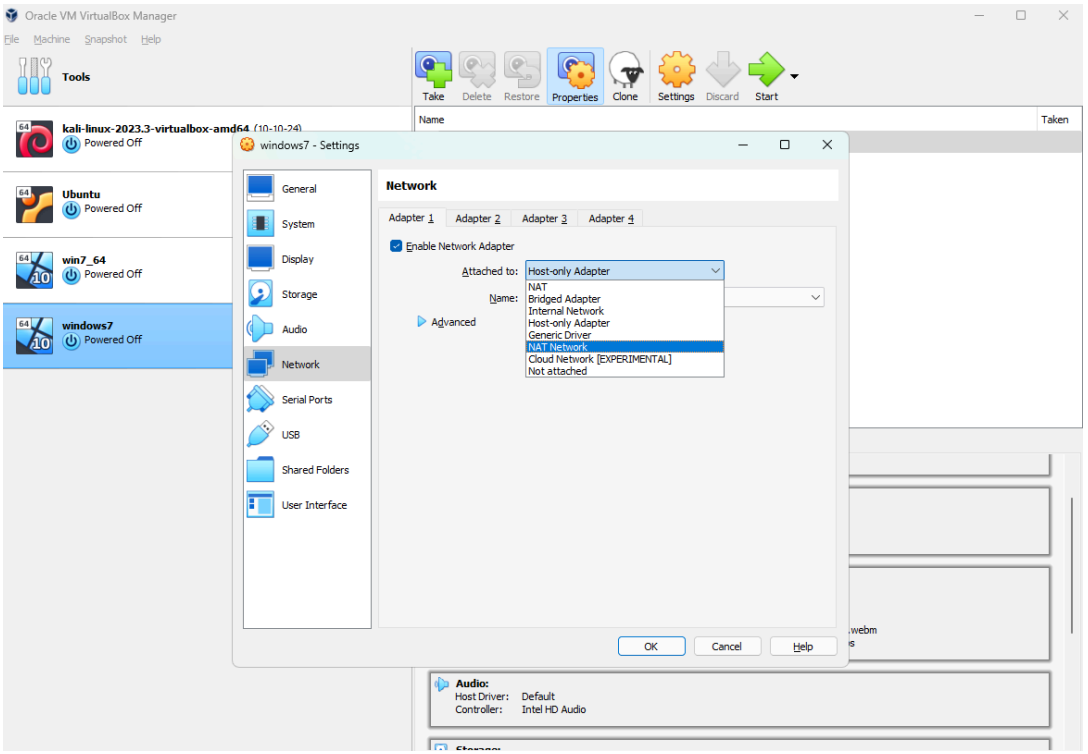

Рисунок 12 – Сегментирование сети

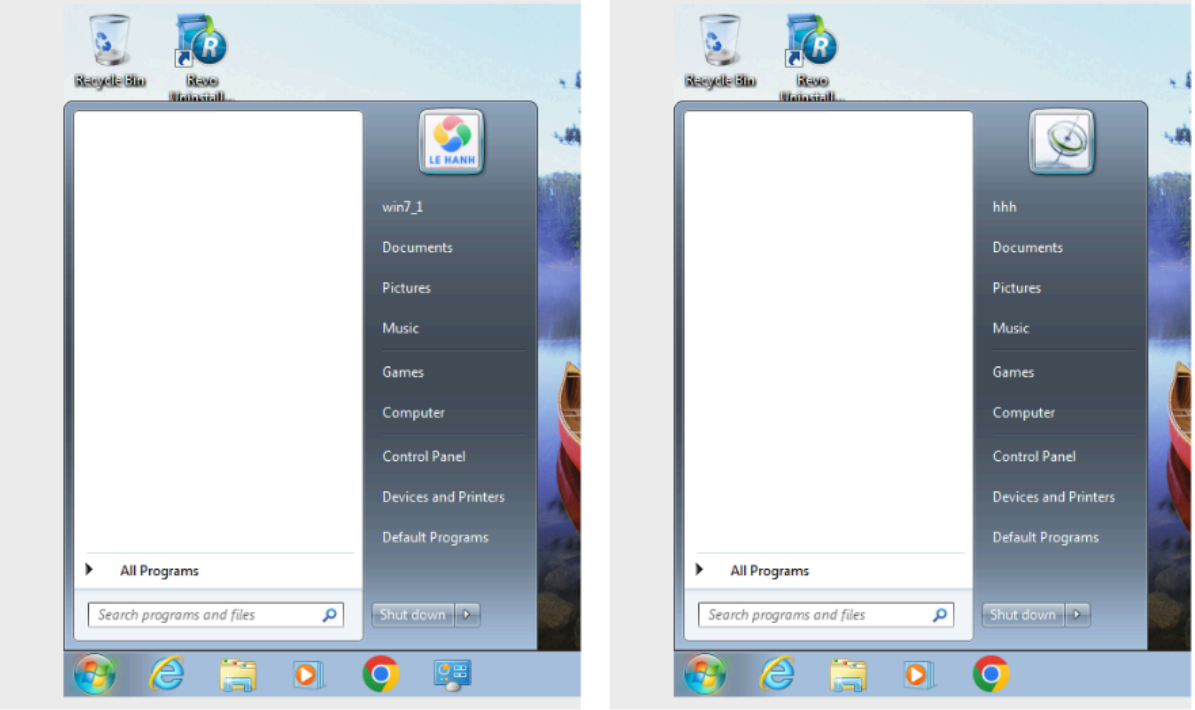

Рисунок 13 – Сегментирование контроля доступа

1.3 Обеспечить защиту технологию в соответствии с требованиями документа

Для того чтобы обеспечить защиту по ЗСВ.9 мы установили 360 Total Security антивирус на нашу виртуальную машину с Windows 7 и протестировали её (Рисунок 14).

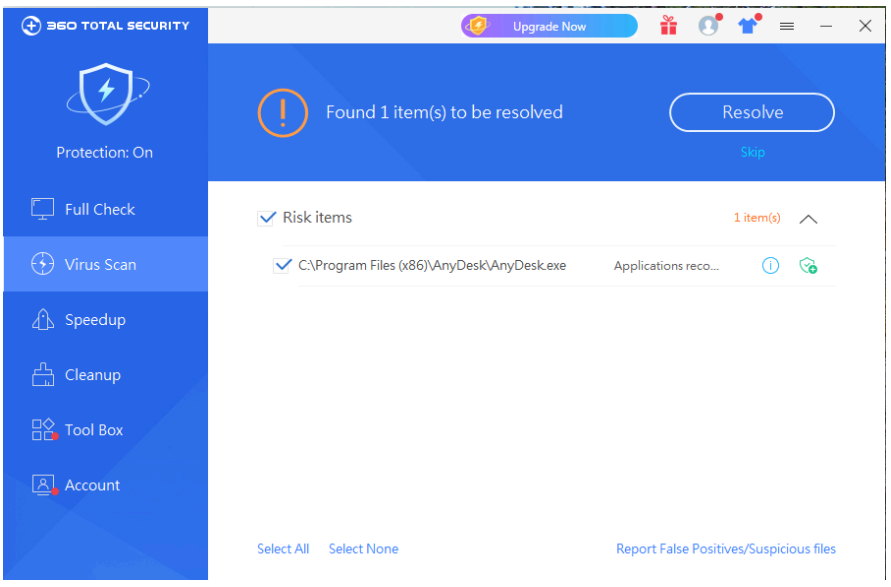

Рисунок 14 – Работа антивирусного ПО.

ЗАКЛЮЧЕНИЕ

В ходе работы была проанализирована технология виртуализации VirtualBox. После оценки соответствия требованиям Приказа ФСТЭК №17 нами было выявлено 9 пунктов, которые были реализованы самой технологией виртуализации. Таким образом, 1 мера защиты нами была реализована с помощью сторонних инструментов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения: введен в действие 2017-06-01. – 2с.
2. Приказ ФСТЭК России от 18 февраля 2013 г. N 17.
3. Remote Virtual Machines // VirtualBox Manual URL: https://www.virtualbox.org/manual/ch07.html#vbox-auth
4. u1035 / vbox-vm-backup // GitHub URL: https://github.com/u1035/vbox-vm-backup