**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**

«ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ВИРТУАЛИЗАЦИИ»

**Выполнили:**

Ахраров Али Рустамович, студент группы N3250

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Калабишка Михаил Михайлович

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Оглавление

[СОДЕРЖАНИЕ 3](#_Toc181326780)

[2 Введение 4](#_Toc181326781)

[3 Цели и задачи 5](#_Toc181326782)

[4 Ход работы 6](#_Toc181326783)

[4.1 Выбор технологии виртуализации и контейнеризации: 6](#_Toc181326784)

[4.2 Установленные средства защиты в Oracle VM VirtualBox: 6](#_Toc181326785)

[4.3 Требования законодательства к защите виртуализированной среды: 6](#_Toc181326786)

[4.4 Обеспечение защиты виртуализации согласно требованиям документа 7](#_Toc181326787)

[4.4.1 *ЗСВ.1: Идентификация и аутентификация в Oracle VirtualBox* 7](#_Toc181326788)

[4.4.2 *ЗСВ.2*: Управление доступом в Oracle VirtualBox 8](#_Toc181326789)

[4.4.3 *ЗСВ.3: Регистрация событий безопасности в Oracle VirtualBox* 10](#_Toc181326790)

[4.4.4 *ЗСВ.4: Управление потоками информации в виртуальной инфраструктуре* 10](#_Toc181326791)

[4.4.5 *ЗСВ.5: Доверенная загрузка в Oracle VirtualBox* 12](#_Toc181326792)

[4.4.6 *ЗСВ.6: Управление перемещением виртуальных машин в Oracle VirtualBox* 12](#_Toc181326793)

[4.4.7 *ЗСВ.7: Контроль целостности виртуальной инфраструктуры в Oracle VirtualBox* 13](#_Toc181326794)

[4.4.8 *ЗСВ.8: Резервное копирование данных и программного обеспечения в Oracle VirtualBox* 14](#_Toc181326795)

[4.4.9 *ЗСВ.9: Реализация антивирусной защиты в Oracle VirtualBox* 14](#_Toc181326796)

[4.4.10 *ЗСВ.10: Сегментирование виртуальной инфраструктуры в Oracle VirtualBox* 15](#_Toc181326797)

[5 Заключение 16](#_Toc181326798)

Введение

**Термины и определения:**

**Виртуализация** — это совокупность технологий, которые преобразуют формат или параметры программных и сетевых запросов к компьютерным ресурсам, чтобы обеспечить независимость процессов обработки данных от программной или аппаратной платформы информационной системы.

**Виртуальная машина (ВМ)** — вычислительная система, функционирующая на основе виртуальных устройств для обработки, хранения и передачи данных. Она также может включать в себя программное обеспечение и пользовательские данные.

**Гипервизор (монитор виртуальных машин)** — программное обеспечение, создающее среду для выполнения других программ (включая гипервизоры), путем имитации аппаратных средств вычислительной системы, управления этими средствами и гостевыми операционными системами, работающими в данной среде.

**Гипервизор I типа** — гипервизор, который устанавливается непосредственно на аппаратное обеспечение и выполняет функции системного программного обеспечения.

**Гипервизор II типа** — гипервизор, запускаемый в среде хостовой операционной системы в виде прикладного программного обеспечения.

# Цели и задачи

**Цель работы** — изучение механизмов обеспечения защиты виртуализации.

Для достижения этой цели необходимо выполнить следующие задачи:

* Выбрать подходящую технологию виртуализации;
* Исследовать механизмы защиты, применяемые в выбранной технологии;
* Определить, соответствуют ли механизмы гипервизора и системы требованиям законодательства;
* Обеспечить защиту технологии в соответствии с нормативными требованиями документа;
* Проверить реализацию всех предусмотренных механизмов;
* Составить отчет по выполненной работе.

# Ход работы

## Выбор технологии виртуализации и контейнеризации:

Для реализации виртуализации в данном проекте мы остановились на гипервизоре второго типа — Oracle VM VirtualBox. Далее будет проведен анализ уже установленных в гипервизоре и гостевой системе средств защиты, которые соответствуют требованиям Приказа ФСТЭК России от 11 февраля 2013 г. №17.

## Установленные средства защиты в Oracle VM VirtualBox:

* *Изоляция виртуальных машин (VM Isolation):* VirtualBox автоматически создает изолированное окружение для каждой виртуальной машины. Это повышает уровень безопасности, снижая риск того, что одна виртуальная машина может повлиять на другую.
* *Шифрование дисков (Disk Encryption*): VirtualBox поддерживает шифрование виртуальных дисков, что помогает защитить данные от несанкционированного доступа как в состоянии хранения, так и при передаче данных.
* *Настройки сетевого адаптера (Network Adapter Settings):* Возможность настройки сетевых адаптеров, таких как NAT, сетевой мост, внутренняя сеть и другие, предоставляет обширные возможности для контроля и ограничения доступа к виртуальным машинам, что значительно усиливает уровень безопасности.

## Требования законодательства к защите виртуализированной среды:

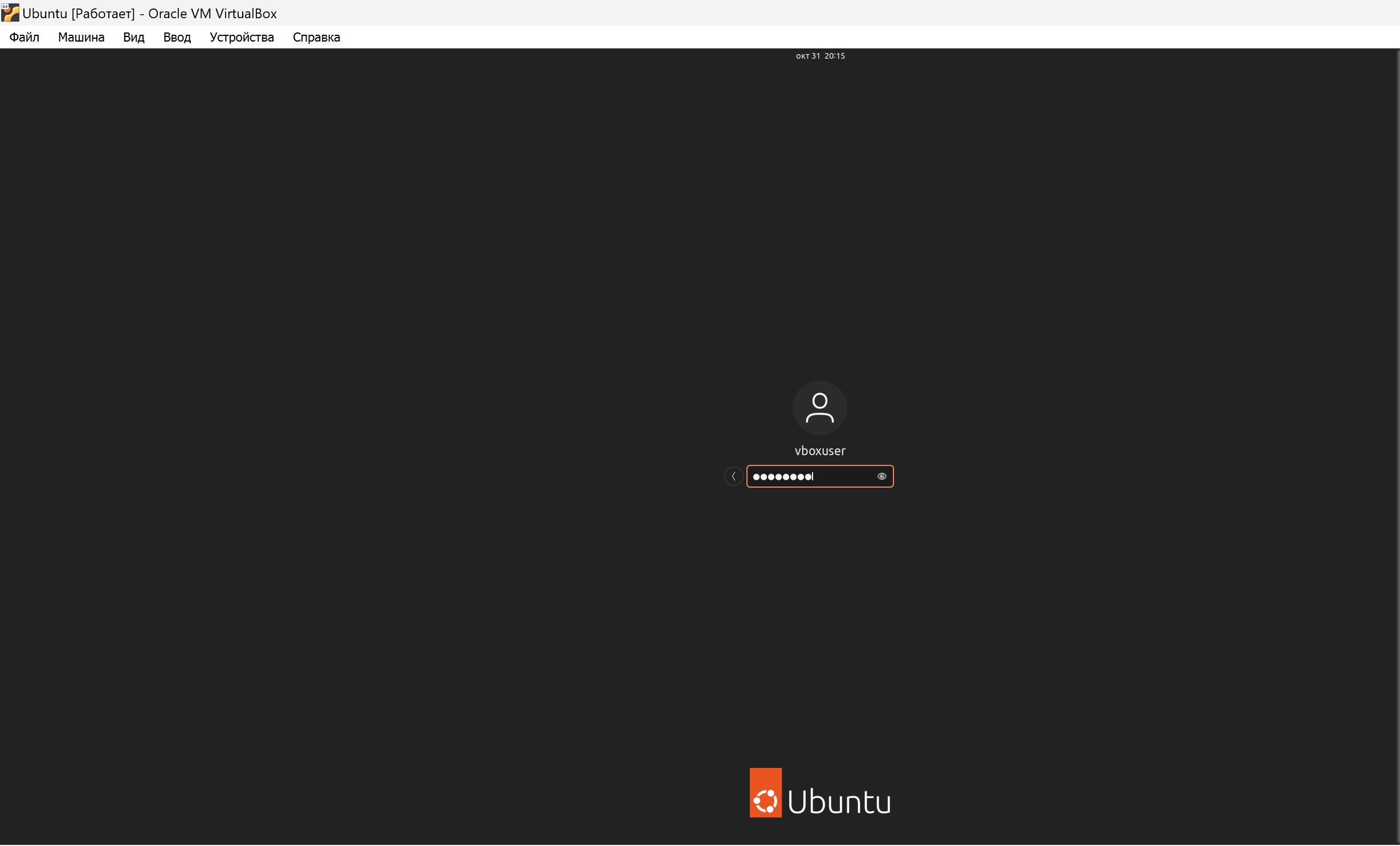
Для обеспечения безопасности виртуализированной среды в Oracle VM VirtualBox были рассмотрены требования Приказа ФСТЭК РФ №17. Средства виртуализации должны выполнять следующие меры защиты:

1. *ЗСВ.1* — Идентификация и аутентификация субъектов и объектов доступа в виртуальной инфраструктуре, включая администраторов, управляющих средствами виртуализации.
2. *ЗСВ.2* — Управление доступом субъектов к объектам виртуальной инфраструктуры, включая внутренние элементы виртуальных машин.
3. *ЗСВ.3* — Регистрация событий безопасности в пределах виртуальной инфраструктуры.
4. *ЗСВ.4* — Управление потоками информации между компонентами виртуальной инфраструктуры и на её периметре (фильтрация, маршрутизация, контроль соединений, однонаправленная передача).
5. *ЗСВ.5* — Доверенная загрузка серверов виртуализации, виртуальных машин (контейнеров) и серверов управления виртуализацией.
6. *ЗСВ.6* — Управление перемещением виртуальных машин (контейнеров) и данных, обрабатываемых на них.
7. *ЗСВ.7* — Контроль целостности виртуальной инфраструктуры и её конфигураций.
8. *ЗСВ.8* — Резервное копирование данных, резервирование технических и программных средств виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры.
9. *ЗСВ.9* — Реализация и управление антивирусной защитой в виртуальной инфраструктуре.
10. *ЗСВ.10* — Разделение виртуальной инфраструктуры на сегменты для обработки информации отдельными пользователями или группами пользователей.

## Обеспечение защиты виртуализации согласно требованиям документа

### *ЗСВ.1: Идентификация и аутентификация в Oracle VirtualBox*

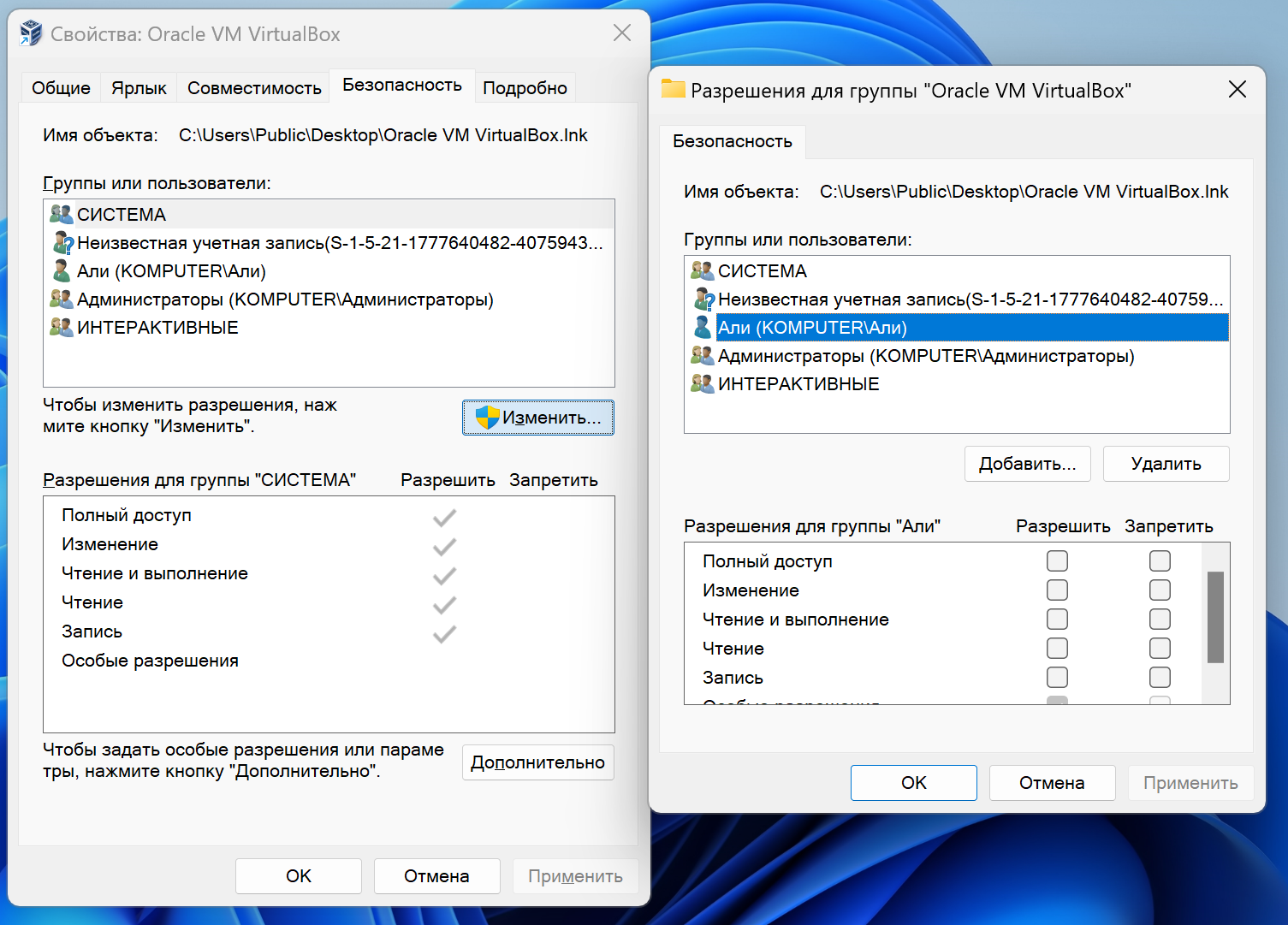
В Oracle VirtualBox отсутствуют встроенные механизмы для идентификации и аутентификации пользователей и объектов доступа на уровне самого приложения, включая администраторов управления средствами виртуализации. Однако эта задача решается за счет идентификации и аутентификации, предоставляемых операционной системой хоста.



*Рис. 1* - Процесс идентификации и аутентификации в операционной системе.

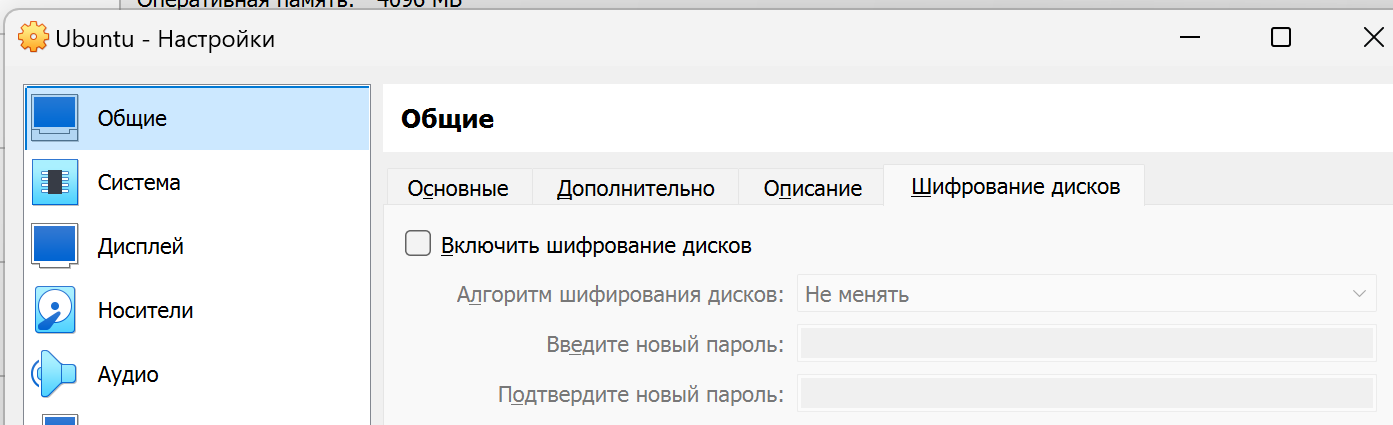
### ***ЗСВ.2*: Управление доступом в Oracle VirtualBox**

Описывается отсутствие встроенных механизмов управления доступом пользователей к объектам виртуальной инфраструктуры в Oracle VirtualBox. Однако управление доступом можно реализовать через операционную систему хоста, а также использовать настройки безопасности в гостевых операционных системах, установленных на виртуальных машинах.



*Рис. 2* - Ограничение обычным пользователям на доступ к VirtualBox.

На **Рис. 2** продемонстрировано, как ограничить обычным пользователям доступ к VirtualBox, используя настройки прав доступа в операционной системе Windows. Это позволяет настроить разрешения на изменение, чтение, выполнение и другие действия для различных пользователей или групп.

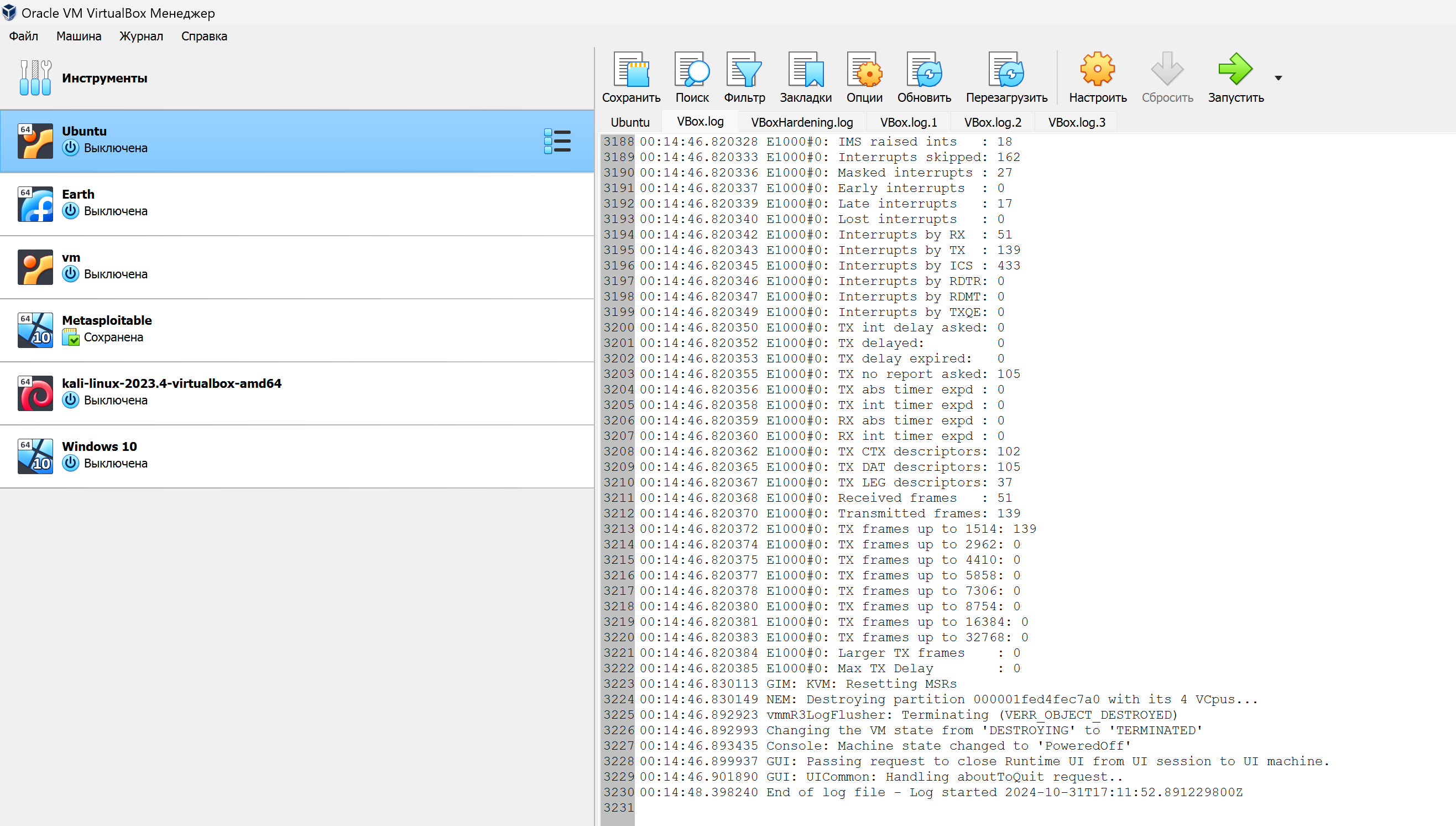


*Рис. 3* - Шифрование дисков в VirtualBox.

На **Рис. 3** изображена настройка шифрования дисков в Oracle VirtualBox. В этой настройке можно включить шифрование диска, выбрать алгоритм шифрования (например, AES-XTS256-PLAIN64), и установить пароль для защиты данных. Это один из ключевых элементов обеспечения безопасности данных виртуальных машин, что помогает предотвратить несанкционированный доступ к информации.

### *ЗСВ.3: Регистрация событий безопасности в Oracle VirtualBox*

В Oracle VirtualBox имеются встроенные механизмы для регистрации событий безопасности, которые реализованы через файл VboxHardening.log. Этот файл ведет запись информации о так называемой "жесткой защите" (hardening), включая проверки целостности и безопасности различных компонентов VirtualBox. В нем также содержатся сообщения об ошибках и предупреждениях, которые помогают отслеживать безопасность работы виртуальной машины.



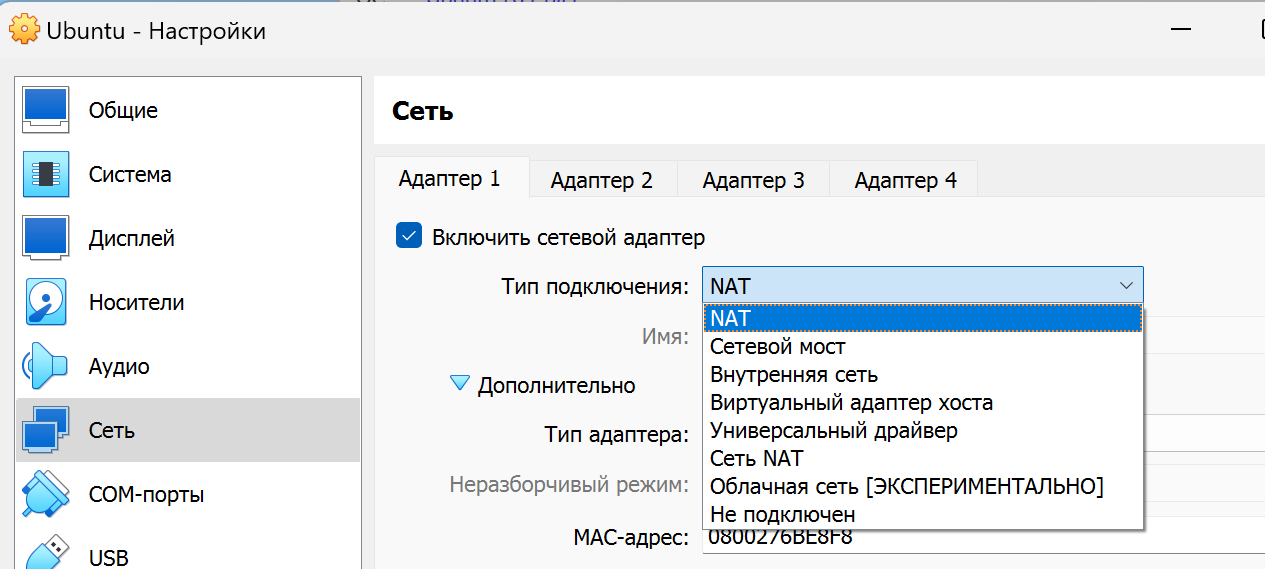
*Рис. 4* - Регистрация событий безопасности в виртуальной инфраструктуре.

### *ЗСВ.4: Управление потоками информации в виртуальной инфраструктуре*

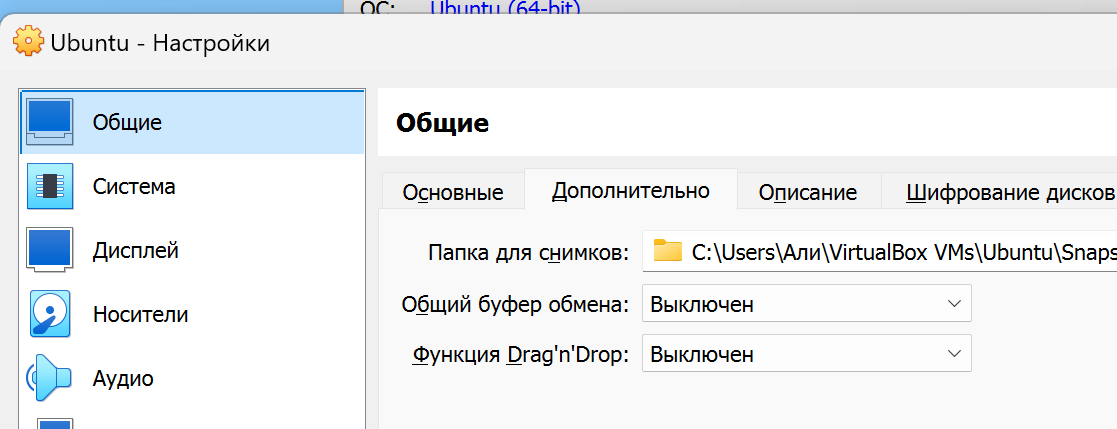
В Oracle VirtualBox доступна функция настройки сетевых адаптеров виртуальных машин, что позволяет управлять потоками информации и изолировать передачи данных между виртуальными машинами и хостовой операционной системой. Это достигается использованием различных типов сетевых подключений:

Сетевые настройки:

* NAT (Сетевой адресный перевод**)**: В этом режиме виртуальная машина (ВМ) функционирует, как компьютер, находящийся за маршрутизатором. Гостевая операционная система (ОС) становится частью закрытой подсети ВМ, а её IP-адрес не доступен извне. Такой режим позволяет подключаться к интерфейсу loopback хостовой ОС, обеспечивая базовую изоляцию виртуальной машины.
* Bridged Networking (Мостовое сетевое соединение): В данном режиме ВМ ведет себя как отдельный компьютер, подключенный к той же сети, что и хост. Таким образом, гостевая ОС получает доступ к сетевым ресурсам, доступным хосту. Для защиты гостевой ОС от прямого доступа извне необходимо правильно настроить межсетевой экран, чтобы предотвратить возможные угрозы.
* Internal Networking (Внутреннее сетевое соединение): В этом режиме ВМ может обмениваться данными с другими виртуальными машинами, расположенными на том же хосте и подключенными к одной внутренней сети. Это позволяет создавать закрытые сети для обмена информацией между ВМ, не подключая их к внешним сетям.
* Host-Only Networking (Сетевое соединение только с хостом): В данном режиме ВМ может взаимодействовать с другими ВМ, находящимися на том же хосте и подключенными к одной внутренней сети, а также с хостовой ОС. Это позволяет изолировать ВМ от внешней сети, обеспечивая высокий уровень безопасности данных и защищая виртуальные машины от возможных внешних угроз.



*Рис. 5* - Выбор сетевого соединения.

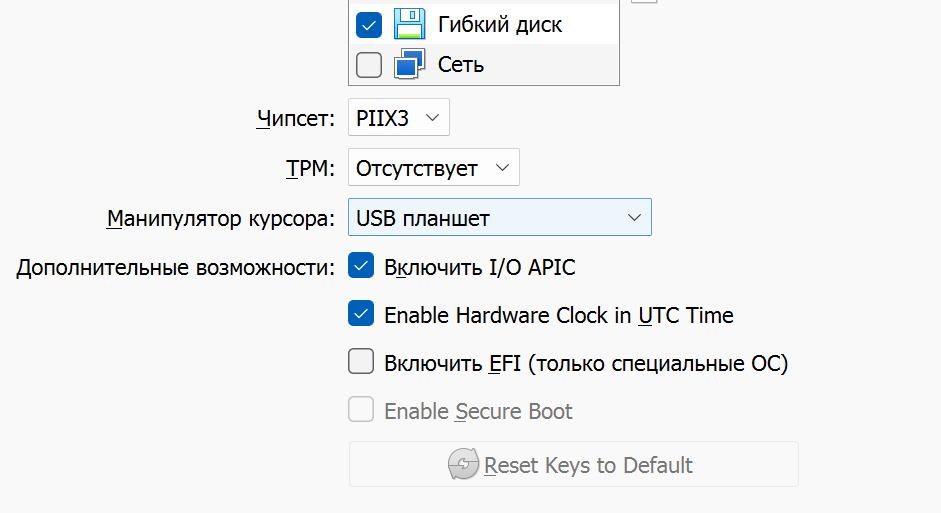


*Рис. 6 -*  Настройка общего буфера обмена и общих папок.

Эти режимы настройки сетевых адаптеров в VirtualBox позволяют обеспечить защиту потоков информации и контролировать передачу данных между виртуальными машинами и хостом, что помогает соответствовать требованиям к безопасности виртуализированной инфраструктуры.

### ***ЗСВ.5: Доверенная загрузка в Oracle VirtualBox***

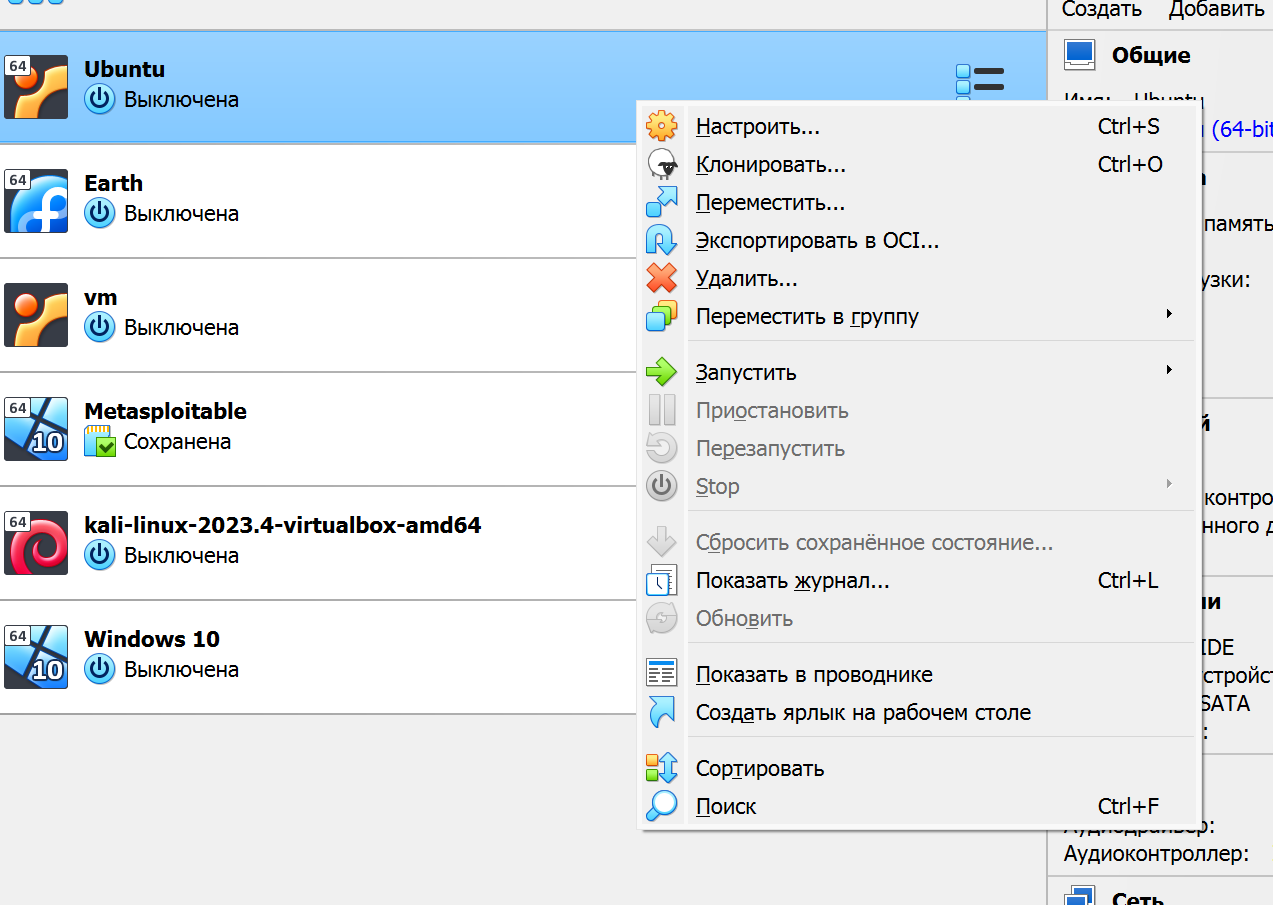
В Oracle VirtualBox предусмотрена возможность включить параметр "Enable Secure Boot", который обеспечивает безопасность виртуальных машин, разрешая загрузку только подписанных операционных систем и драйверов. Этот параметр можно включить через настройки виртуальной машины, в разделе "Система" на вкладке "Материнская плата". Там необходимо поставить галочку напротив "Включить безопасную загрузку" (Enable Secure Boot), чтобы защитить процесс загрузки виртуальной машины.



***Рис. 7*** - Включение безопасной загрузки.

### ***ЗСВ.6: Управление перемещением виртуальных машин в Oracle VirtualBox***

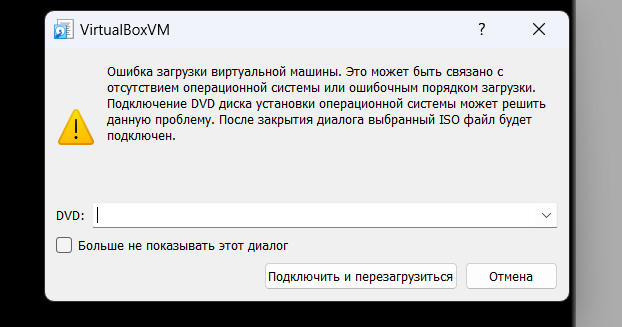
Oracle VirtualBox предоставляет возможность управления перемещением виртуальных машин. Например, можно клонировать виртуальные машины, создавая их полные копии, и переносить их между разными хостами с помощью функции экспорта и импорта в форматах OVA или OVF. Это позволяет обеспечивать мобильность виртуальных машин, сохраняя при этом их конфигурации и данные.



***Рис. 8 -*** Управление перемещением и клонированием ВМ.

### ***ЗСВ.7: Контроль целостности виртуальной инфраструктуры в Oracle VirtualBox***

В Oracle VirtualBox контроль целостности виртуальной инфраструктуры и её конфигураций осуществляется автоматически. Если конфигурационный файл виртуальной машины с расширением .vbox был изменен несанкционированно или поврежден, система выдаст ошибку, и запуск виртуальной машины станет невозможным. Это является дополнительным уровнем защиты, так как позволяет обнаруживать попытки вмешательства в настройки виртуальной машины и предотвращать дальнейшее использование скомпрометированной конфигурации.

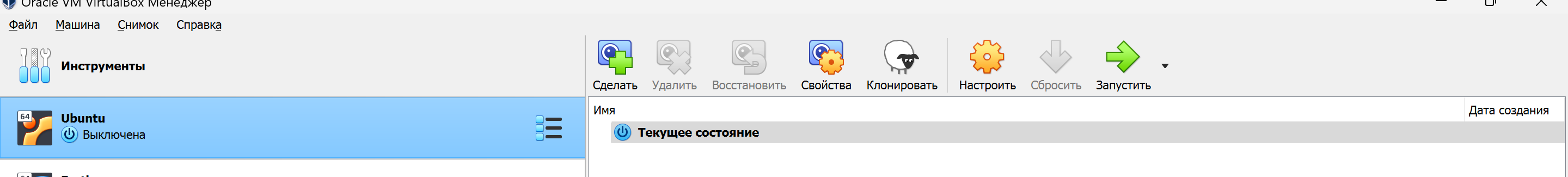


***Рис. 9*** - Контроль целостности ВМ.

Эти механизмы помогают обеспечивать доверенную загрузку и защиту конфигураций виртуальных машин, что соответствует требованиям законодательства к защите виртуализированной среды.

### ***ЗСВ.8: Резервное копирование данных и программного обеспечения в Oracle VirtualBox***

В Oracle VirtualBox резервное копирование данных и программного обеспечения осуществляется с помощью функции создания снимков состояния (snapshots). Эта функция позволяет сохранять текущее состояние виртуальной машины, которое затем можно восстановить в случае сбоя или повреждения данных. Создание снапшотов позволяет поддерживать актуальное резервное копирование, обеспечивая защиту данных и возможность отката изменений.



***Рис. 10*** - Снимок состояния виртуальной машины.

### ***ЗСВ.9: Реализация антивирусной защиты в Oracle VirtualBox***

Oracle VirtualBox не имеет встроенных механизмов антивирусной защиты, поэтому для обеспечения безопасности виртуальной инфраструктуры требуется устанавливать антивирусные программы как на хостовую операционную систему, так и на гостевые операционные системы. Это помогает минимизировать риски, связанные с вредоносным программным обеспечением, и обеспечивает более высокий уровень защиты виртуальных машин.

### ***ЗСВ.10: Сегментирование виртуальной инфраструктуры в Oracle VirtualBox***

Oracle VirtualBox предоставляет возможность делить виртуальную инфраструктуру на сегменты с помощью VLAN (Virtual Local Area Network). Это означает, что виртуальные машины можно разделить на отдельные сетевые группы, чтобы разные пользователи или группы пользователей могли обрабатывать информацию независимо друг от друга. Такое сегментирование обеспечивает дополнительную безопасность, позволяя ограничить доступ к сетевым ресурсам внутри инфраструктуры и разделить потоки данных по функциональным или организационным признакам.

Эти меры позволяют более гибко и безопасно управлять виртуальной инфраструктурой, соответствуя требованиям по разделению информации и минимизации рисков в виртуализированных средах.

# Заключение

В ходе выполнения данной работы были проанализированы и изучены методы защиты виртуализации от угроз, применимые для гипервизора Oracle VirtualBox и гостевой операционной системы Ubuntu. В рамках исследования выполнены следующие задачи:

* Изучены механизмы обеспечения безопасности виртуализации.
* Определено, что механизмы гипервизора и виртуальной инфраструктуры соответствуют требованиям законодательства.
* Обеспечена защита виртуализационной технологии в соответствии с установленными требованиями.
* Проверена реализация всех механизмов безопасности.

Все поставленные задачи были успешно выполнены, и цель работы достигнута.