МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра ИБ

ОТЧЕТ

по практической работе №1
по дисциплине «Технология разработки информационных систем в защищенном исполнении»
Тема: Настройка системы защиты информации от несанкционированного доступа «Dallas Lock»

Студентка гр. 5362 _____ Болтнева Е.Г.

Студент гр. 5362 _____ Суслопаров И.А.

Преподаватель _____ Краснов С.А.

Санкт-Петербург
2020

Цель работы.

Получить практические навыки настройки СЗИ НСД «Dallas Lock».

Задание.

1) Создать пользователей системы (субъект доступа);
2) Выполнить настройки идентификации и аутентификации;
3) Создать защищаемые каталоги (объект доступа);
4) Установить объектам доступа права разграничения доступа по отношению к субъектам доступа;
5) Выполнить настройку очистки остаточной информации;
6) Выполнить настройку регистрации событий для объектов доступа;
7) Выполнить настройку контроля целостности файловой системы и программно-аппаратной среды;
8) Выполнить настройку внешних носителей информации;
9) Всю информацию собрать в единый документ, являющийся отчетом о настройке СЗИ НСД.

Основные теоретические положения.

СЗИ НСД «Dallas Lock» предназначена для предотвращения получения защищаемой информации заинтересованными лицами с нарушением установленных норм и правил, обладателями информации с нарушением установленных правил разграничения доступа к защищаемой информации и осуществления контроля за потоками информации, поступающими в автоматизированную систему и выходящими за её пределы. А также для обеспечения защиты информации в АС посредством её фильтрации.

Система защиты Dallas Lock представляет собой программный комплекс средств защиты информации в ОС семейства «Windows» с возможностью подключения аппаратных идентификаторов.

Использование системы защиты Dallas Lock в проектах по защите информации позволяет привести АС в соответствие требованиям

законодательства РФ. Система защиты предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах (файловых, контроллерах домена и терминального доступа).

Система защиты Dallas Lock состоит из следующих основных компонентов:

Программное ядро (Драйвер защиты). Является ядром системы защиты и выполняет основные функции СЗИ НСД:

- обеспечивает мандатный (для редакции «С») и дискреционный режимы контроля доступа к объектам файловой системы и устройствам;
- обеспечивает доступ к журналам, параметрам пользователей и параметрам СЗИ НСД в соответствии с правами пользователей;
- обеспечивает работу механизма делегирования полномочий;
- обеспечивает проверку целостности СЗИ НСД, объектов ФС, программно-аппаратной среды и реестра;
- драйвер защиты осуществляет полную проверку правомочности и корректности администрирования СЗИ НСД.

Драйвер защиты автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы. Драйвер осуществляет управление подсистемами и модулями системы защиты и обеспечивает их взаимодействие. С драйвером защиты взаимодействуют защитные подсистемы, перечисленные ниже.

Подсистема администрирования. Включает в себя:

- подсистему локального администрирования. Обеспечивает возможности по управлению СЗИ НСД, аудиту и настройке параметров, просмотру, фильтрации и очистке журналов. Включает в себя подсистему внедрения в интерфейс «Windows» Explorer («проводник»). Обеспечивает отображение пунктов в контекстном меню объектов, необходимых для назначения прав доступа к объектам ФС, вызова функции принудительной зачистки объектов ФС, преобразования.

- подсистему удаленного администрирования. Позволяет выполнять настройку системы защиты с удалённого компьютера.
- подсистему централизованного управления. Позволяет объединять защищенные компьютеры в Домен безопасности для централизованного и оперативного управления клиентами.

Подсистема управления доступом. Включает в себя:

- подсистему аппаратной идентификации. Осуществляет работу с различными типами аппаратных идентификаторов;
- подсистему доступа к файловой системе, реестру и устройствам, в составе которой:
    - подсистема дискреционного доступа;
    - подсистема мандатного доступа (для редакции «С»);

Подсистема регистрации и учета. Включает в себя:

- подсистему аудита. Обеспечивает ведение аудита и хранение информации 8-ми категорий событий в журналах;
- подсистему печати. Обеспечивает разграничение доступа к печати, добавление штампа на документы, сохранение их теневых копий, регистрацию событий печати.

Подсистема идентификации и аутентификации. Обеспечивает идентификацию и аутентификацию локальных, доменных, терминальных и удаленных пользователей на этапе входа в операционную систему.

Подсистема гарантированной зачистки информации. Обеспечивает зачистку остаточной информации.

Подсистема преобразования информации. Обеспечивает:

- преобразование информации в файлах-контейнерах;
- преобразование сменных накопителей для защиты от доступа в обход СЗИ НСД;
- работу с данными при одновременном их преобразовании в файлдисках;

- прозрачное преобразование жестких дисков (для редакции «С») для предотвращения доступа к данным, расположенным на жестких дисках, в обход СЗИ НСД.

Подсистема контроля устройств. Обеспечивает возможность разграничения доступа к подключаемым на ПК устройствам для определенных пользователей или групп пользователей и ведения аудита событий данного доступа.

Подсистема межсетевого экранирования. Обеспечивает контроль, а также фильтрацию потоков информации, поступающих в автоматизированную систему и выходящих за её пределы.

Подсистема обнаружения вторжений. Обеспечивает обнаружение и блокирование основных угроз безопасности, выполняет одновременно функции и сетевой, и хостовой системы обнаружения вторжений, дополнительно детально анализирует некоторые отдельные сетевые протоколы.

Подсистема контроля целостности. Обеспечивает контроль целостности файловой системы, программно-аппаратной среды и реестра, периодическое тестирование СЗИ НСД, наличие средств восстановления СЗИ НСД, восстановление файлов и веток реестра в случае нарушения их целостности.

Подсистема восстановления после сбоев. Предусматривает процедуры восстановления после сбоев и отказов оборудования, которые должны обеспечивать полное и оперативное восстановление свойств СЗИ НСД. Реализована возможность возвращения всех настроек СЗИ НСД к исходным (установка параметров по умолчанию), что равносильно переустановке СЗИ НСД.

Подсистема развертывания (установочные модули). Выполняет все необходимые функции по установке СЗИ НСД на рабочую станцию и удалению с нее. В процессе развертывания реализована возможность установки конфигурации по умолчанию и другой рабочей конфигурации СЗИ НСД. В

процессе развертывания реализована возможность автоматического ввода рабочей станции под управление сервера безопасности.

В ходе данной практической работы выполняется настройка системы защиты. Выполнение работ при установке и настройке системы защиты информации для действующей информационной системы в общем случае разделяется на следующие этапы:

1) Подготовка средств вычислительной технике к настройке;
2) Установка и настройка общесистемного программного обеспечения;
3) Установка и настройка прикладного программного обеспечения;
4) Установка и настройка сетевого оборудования;
5) Установка и настройка периферийного оборудования;
6) Установка и настройка средств антивирусной защиты;
7) Установка и настройка системы защиты информации от несанкционированного доступа.

В этой работе подробно рассмотрен последний 7-ой этап работ. В этом случае этап подготовки к установке и настройке СЗИ НСД включает в себя:

1) Проверку наличия дистрибутива СЗИ НСД последней версии.
2) Проверку наличия лицензионного ключа и формуляра.
3) Проверку наличия матрицы доступа.

Выполнение работы.

Создадим пользователей системы (субъекты доступа):

- откроем оболочку администратора системы защиты,
- перейдем к категории «Учетные записи»-> «Создать»,
- в появившемся окне заполним необходимые поля (рисунок 1),
- установим включенными следующие параметры: «Запретить работу при нарушенной целостности», «Запретить смену пароля пользователем»,
- добавим пользователя в созданную ранее в категории «Группы» (рисунок 2) группу «Работники» во вкладке «Группы» (рисунок 3),

- нажатием на кнопку «Ок» перейдем к форме ввода пароля, зададим пароль (рисунок 4).

Также в окне создания учетной записи пользователя имеется возможность разрешить работу с системой по определенному расписанию путем нажатия на «Расписание работы» (рисунок 5).

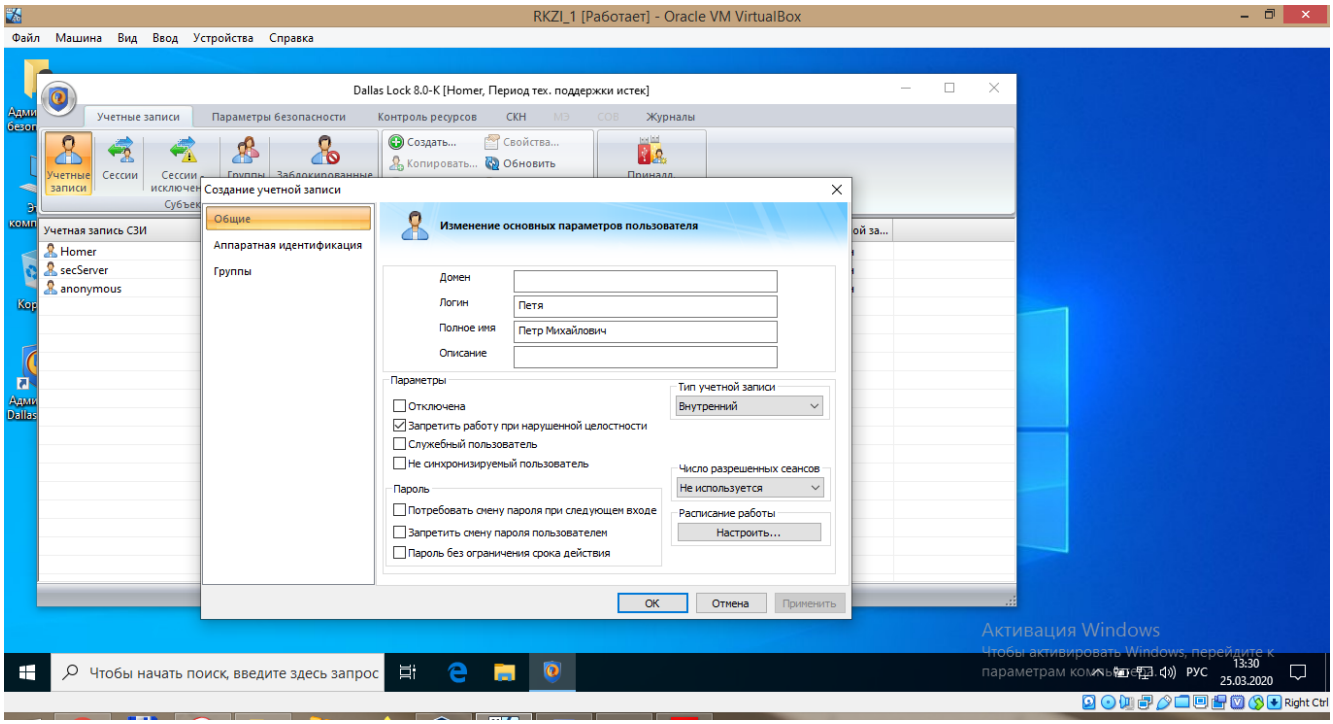

Рисунок 1

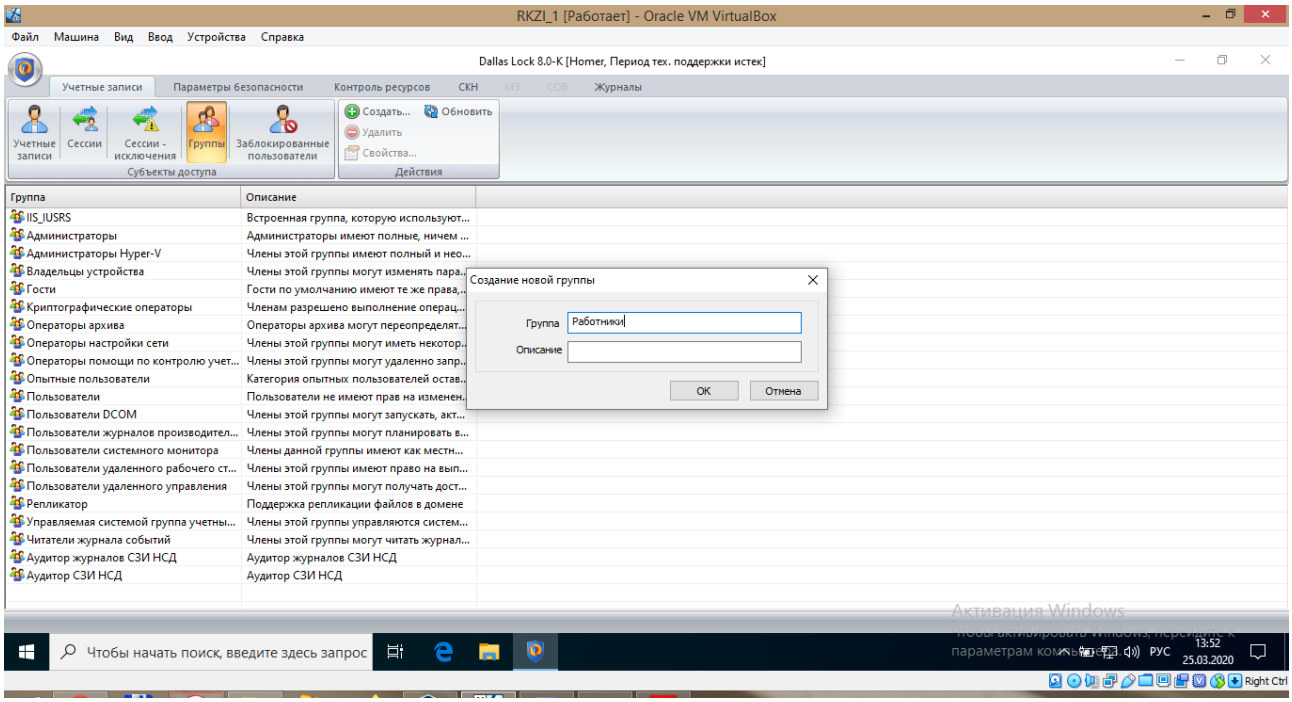

Рисунок 2

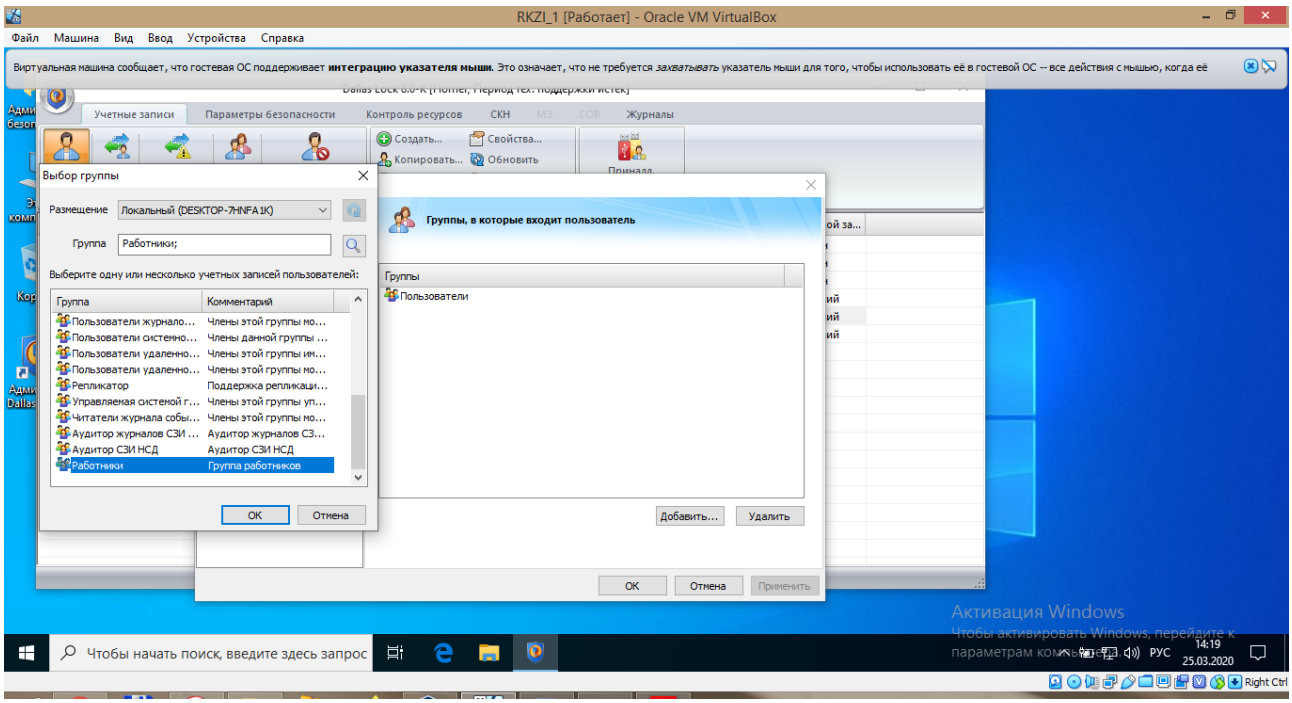

Рисунок 3

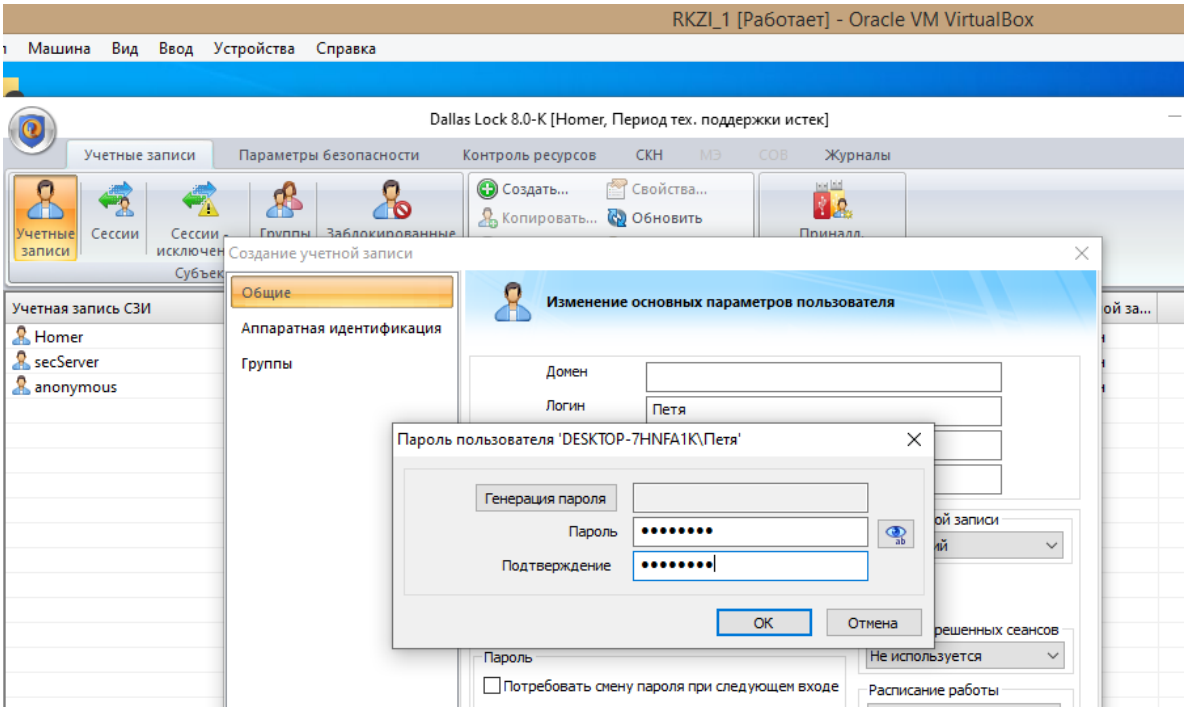

Рисунок 4

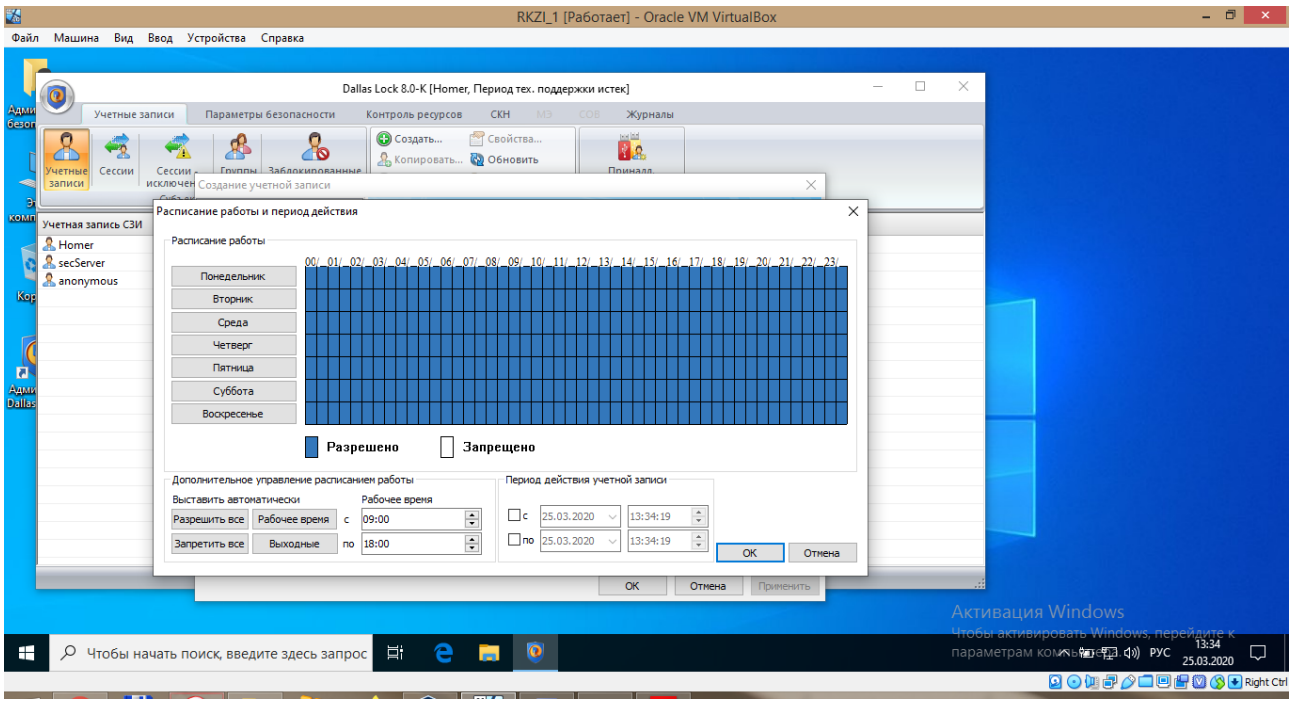

Рисунок 5

Аналогично было создано еще два субъекта доступа, результаты представлены на рисунке 6.

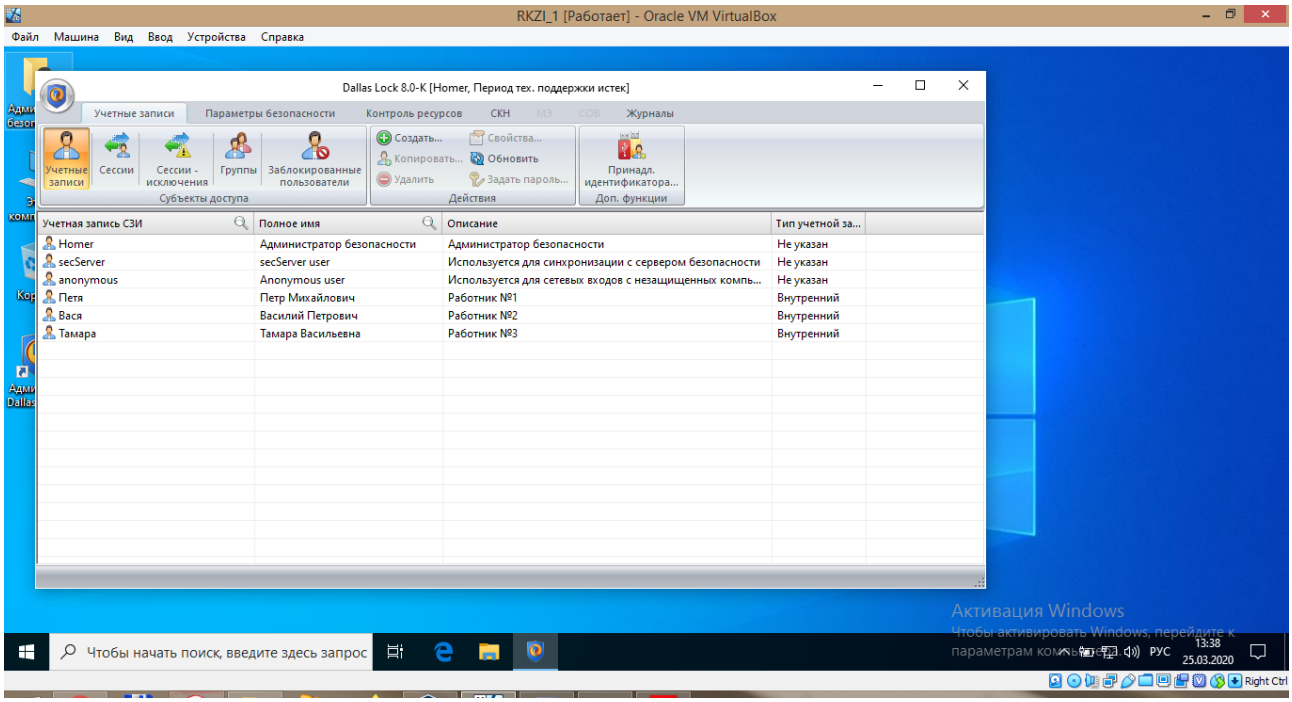

Рисунок 6

Выполним настройки идентификации и аутентификации:

- откроем оболочку администратора системы защиты;
- перейдем во вкладку «Параметры безопасности», «Вход»;

- настроим все параметры, расположенные в списке параметров «Вход», «Пароли» (рисунок 7).

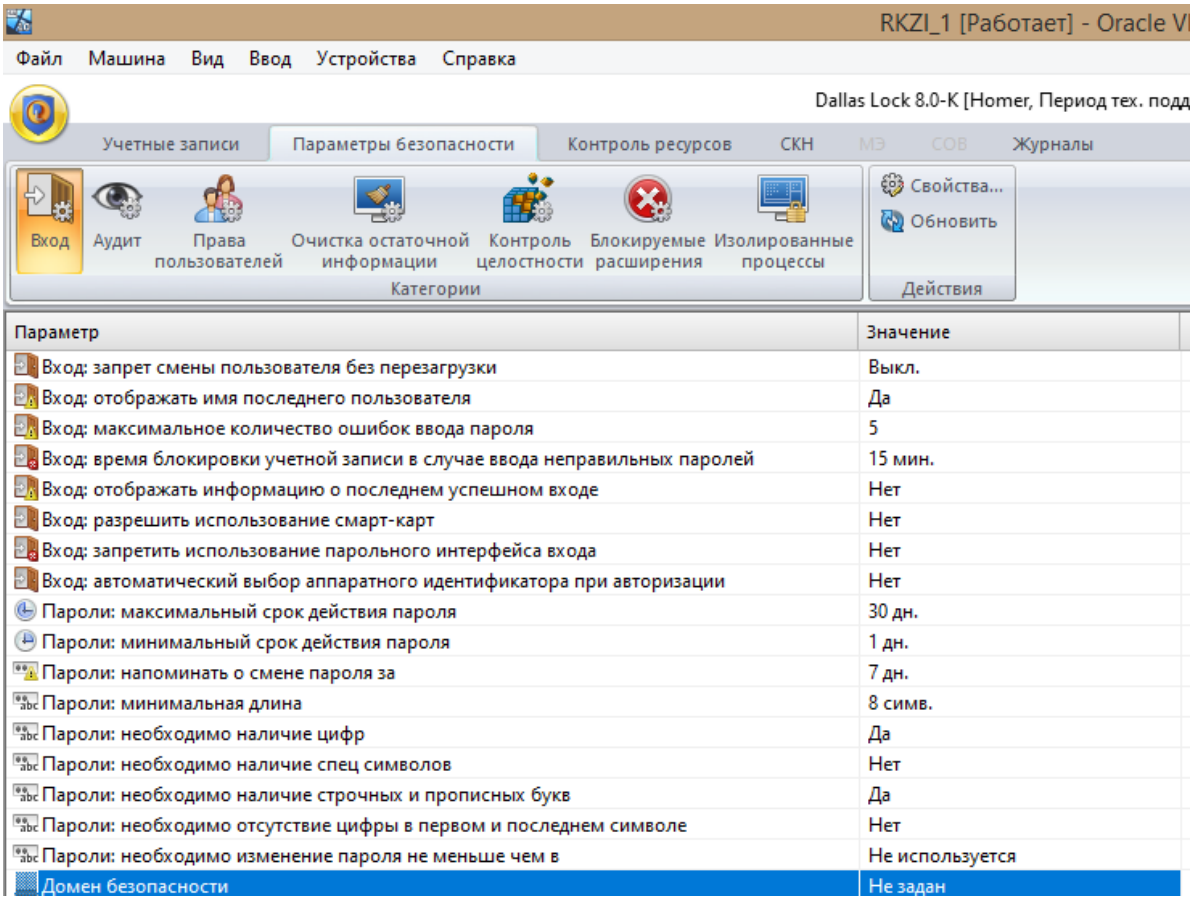

Рисунок 7

Создадим защищаемые каталоги (рисунок 8).

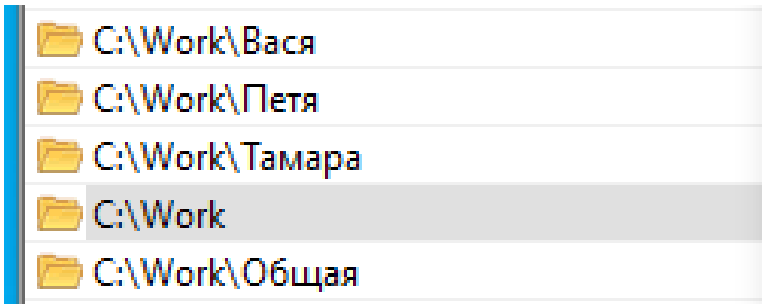

Рисунок 8

Установим объектам доступа права разграничения доступа по отношению к субъектам доступа («Дискреционный доступ» -> «Контроль ресурсов», затем добавляем созданные ранее субъекты и переходим к настройкам безопасности).

Для каталогов «Вася» (рисунок 9-10), «Петя» (рисунок 11-12) и «Тамара» (рисунок 13-14) выполняем следующие настройки:

- владельцу папки разрешаем «Чтение», «Запись», «Удаление» и «Чтение разрешений»;
- остальным пользователям системы запрещаем всё.

Для каталога «Общая» (рисунок 15) настройки аналогичны предыдущим:

- группе «Работники» (в нее входят Петя, Вася и Тамара) разрешаем «Чтение», «Запись», «Удаление» и «Чтение разрешений»;
- остальным пользователям системы запрещаем всё.

Для каталога «Work» (в котором расположены «Вася», «Петя», «Тамара» и «Общая») настройки представлены на рисунке 16.

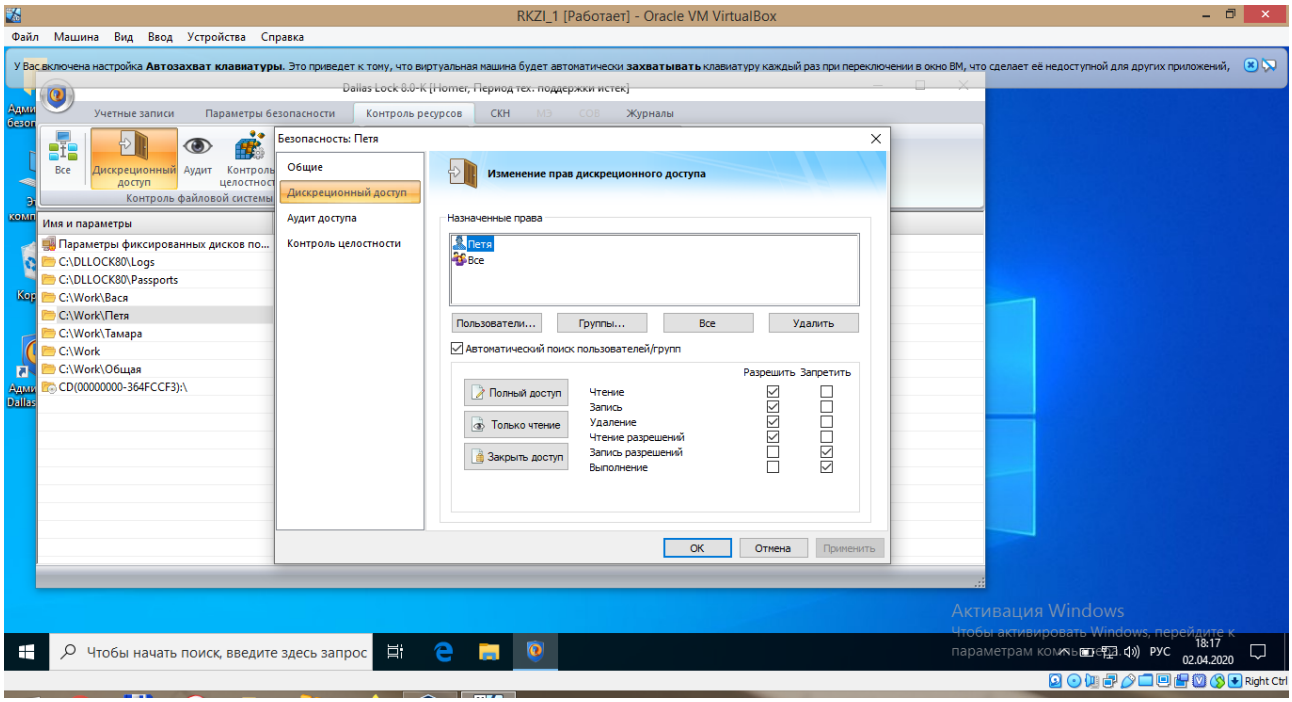

Рисунок 9

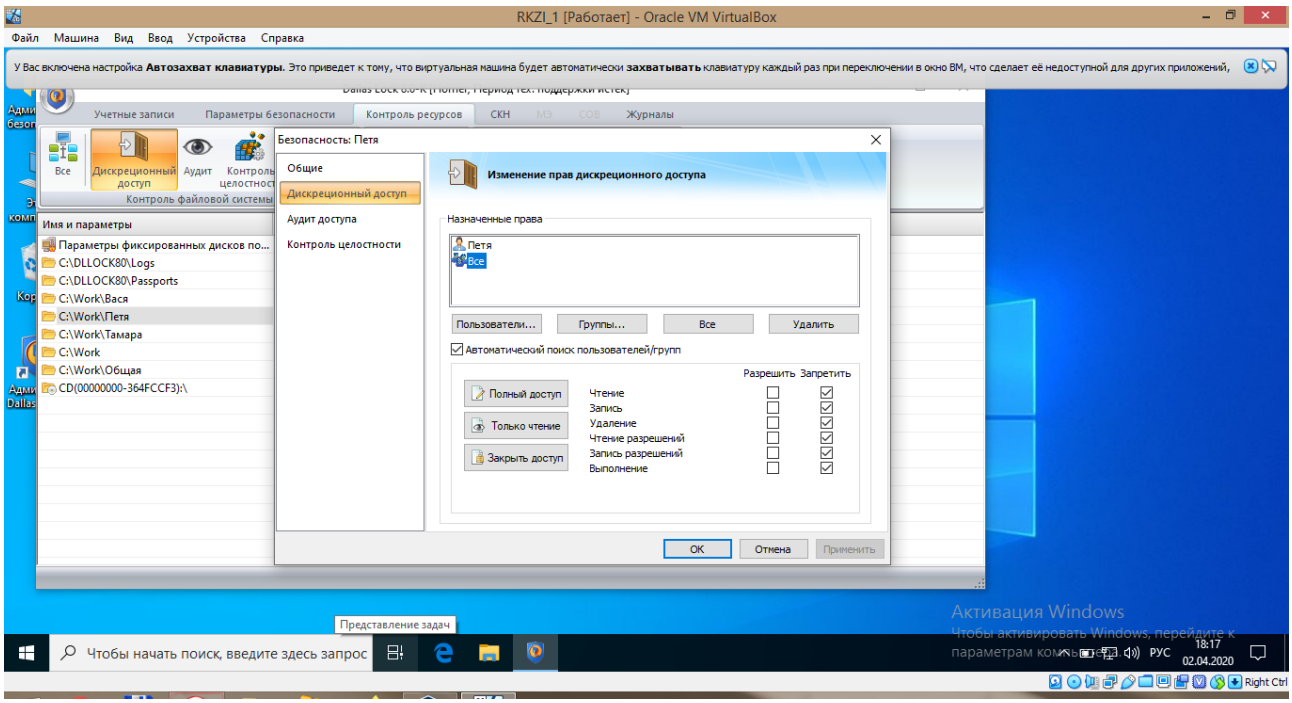

Рисунок 10

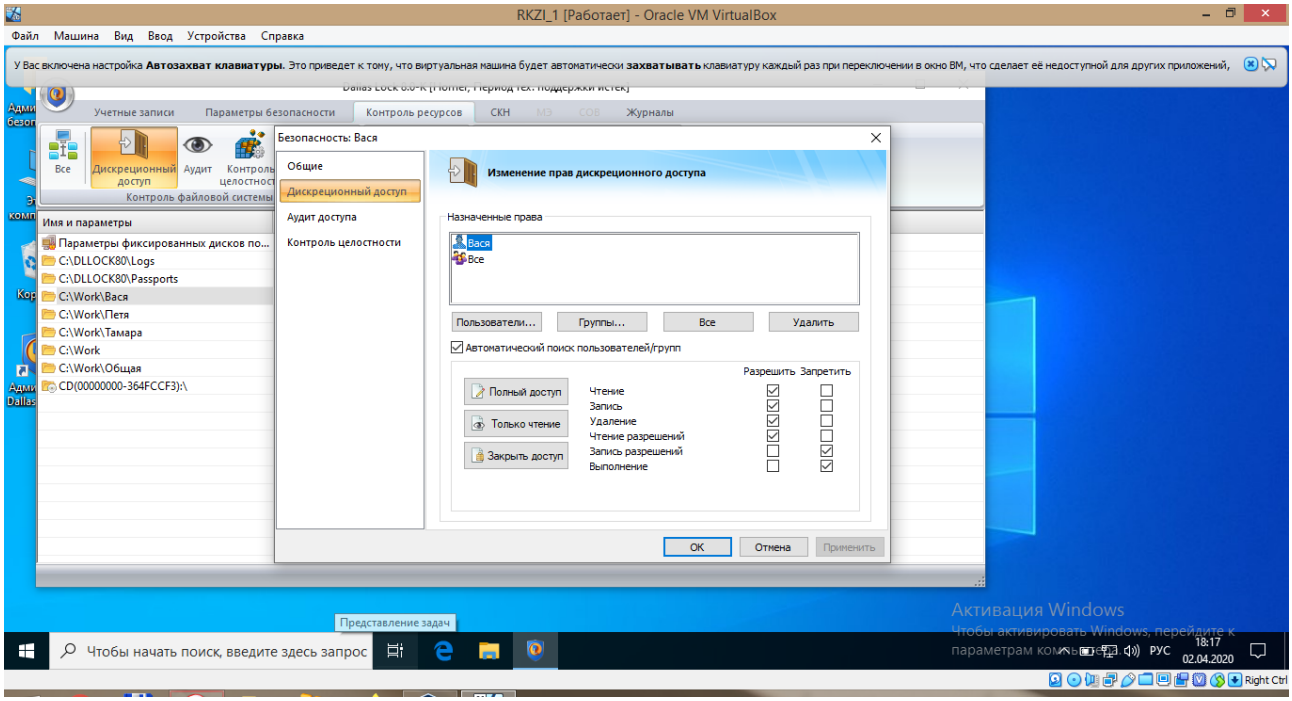

Рисунок 11

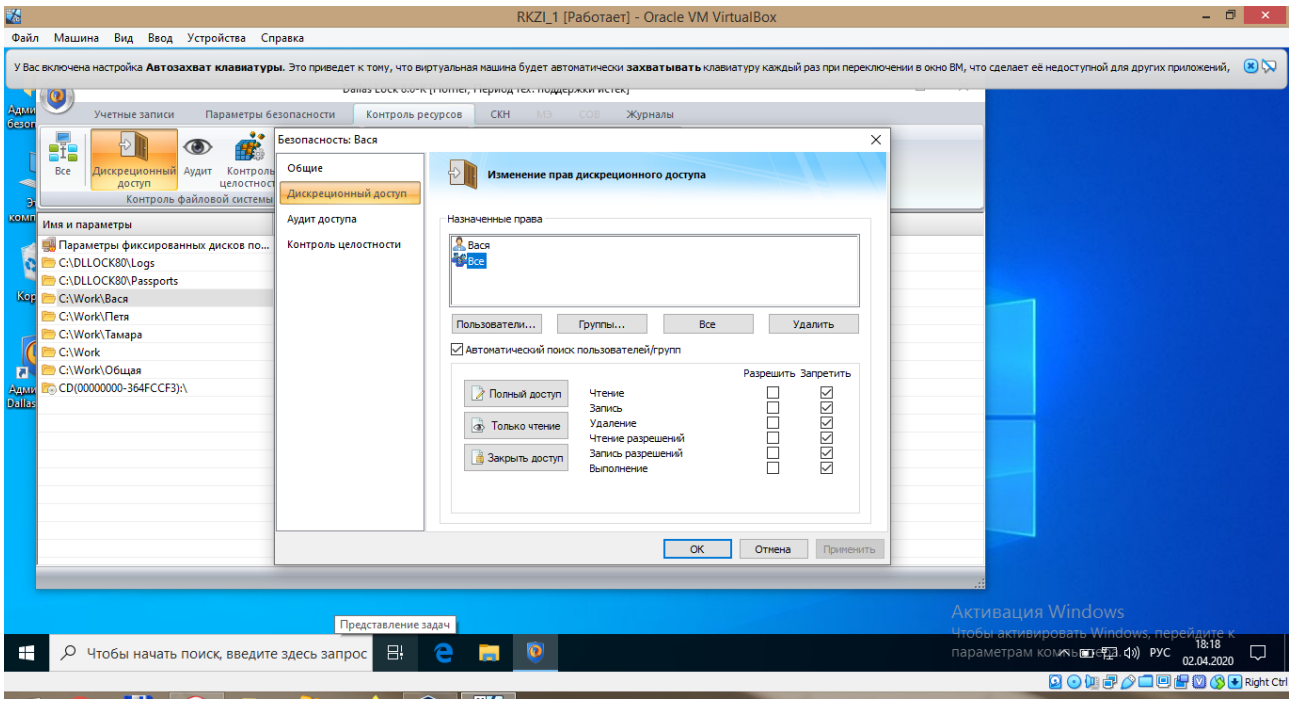

Рисунок 12

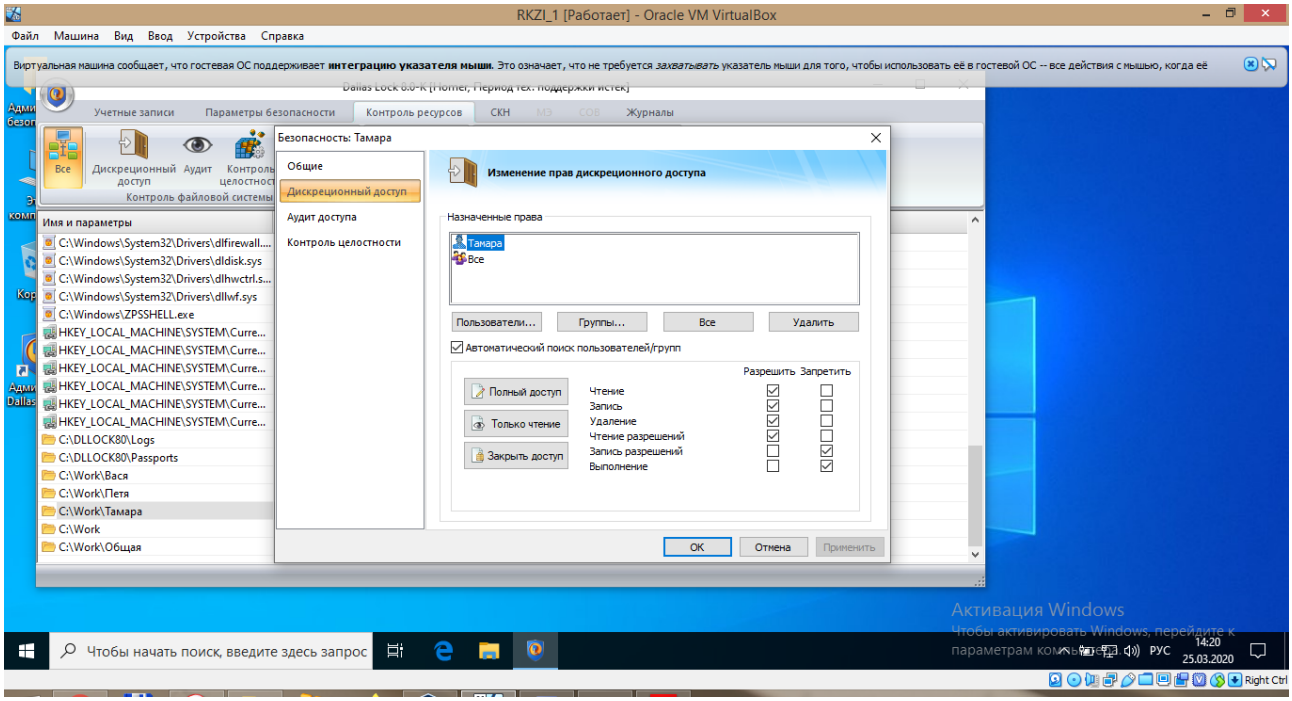

Рисунок 13

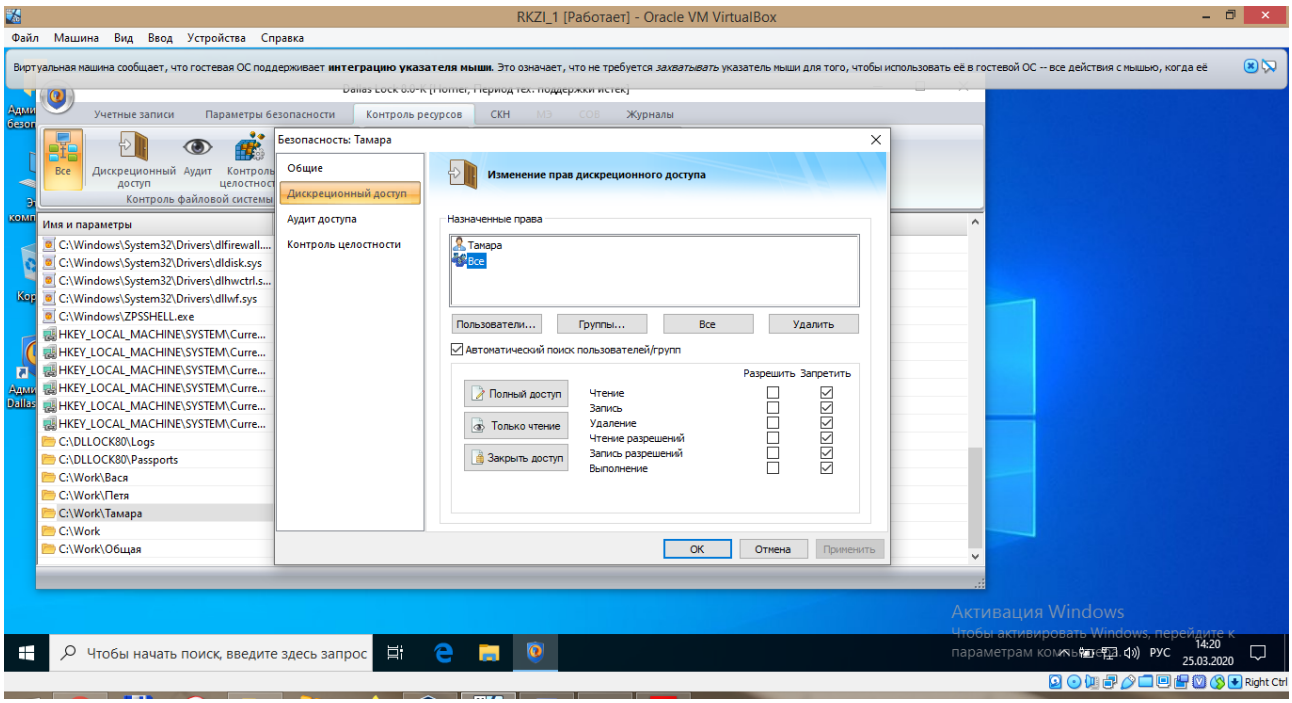

Рисунок 14

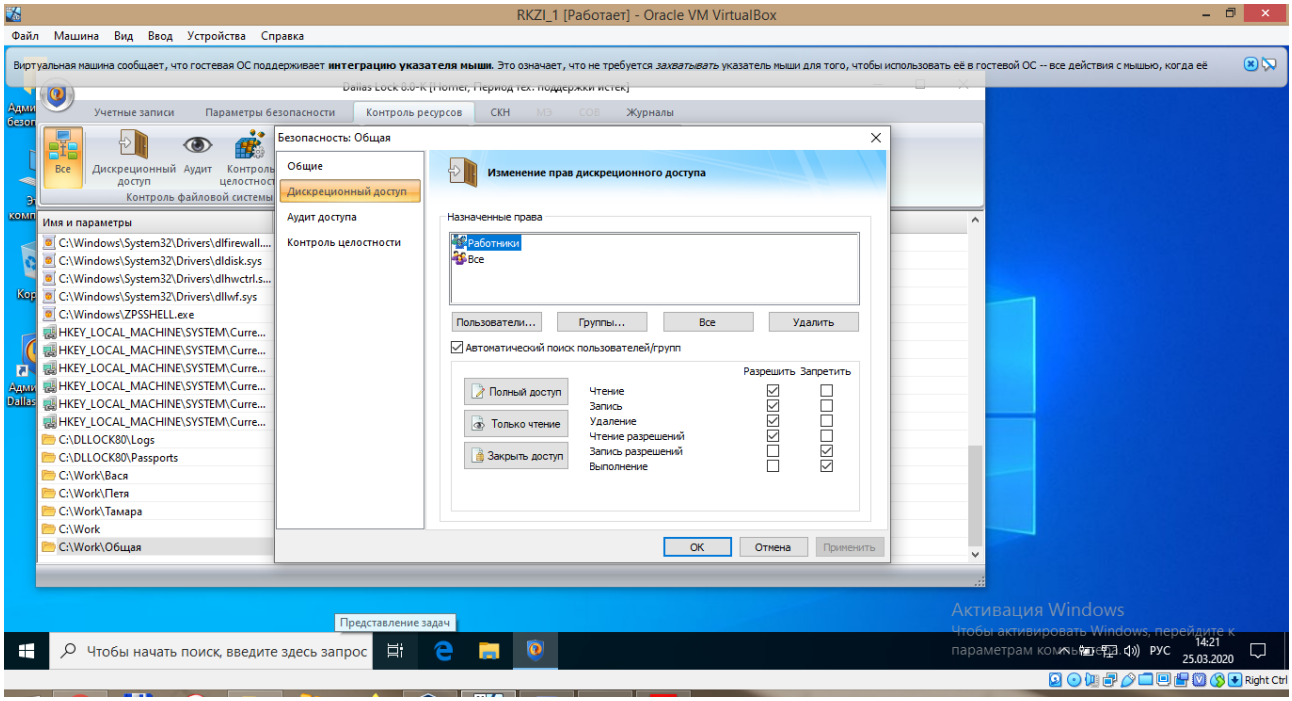

Рисунок 15

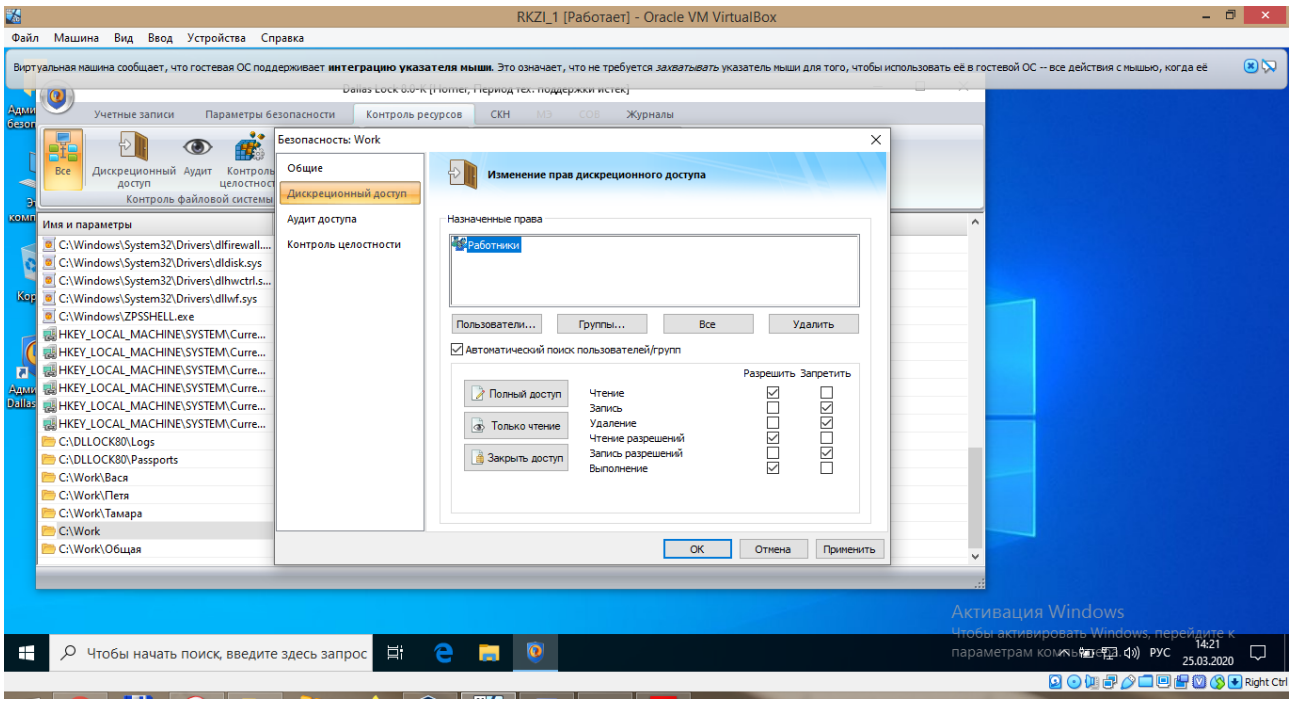

Рисунок 16

Выполним настройку очистки остаточной информации (рисунок 17):

- откроем оболочку администратора системы защиты;
- перейдем в категорию «Очистка остаточной информации» на вкладке «Параметры безопасности»;
- установим параметры очистки остаточной информации:
    - значение «Да» для следующих параметров: «Очищать освобождаемое дисковое пространство», «Очищать файл подкачки виртуальной памяти», «Проверять очистку информации»;
    - «Количество циклов затирания» в соответствии с требованиями политики безопасности.

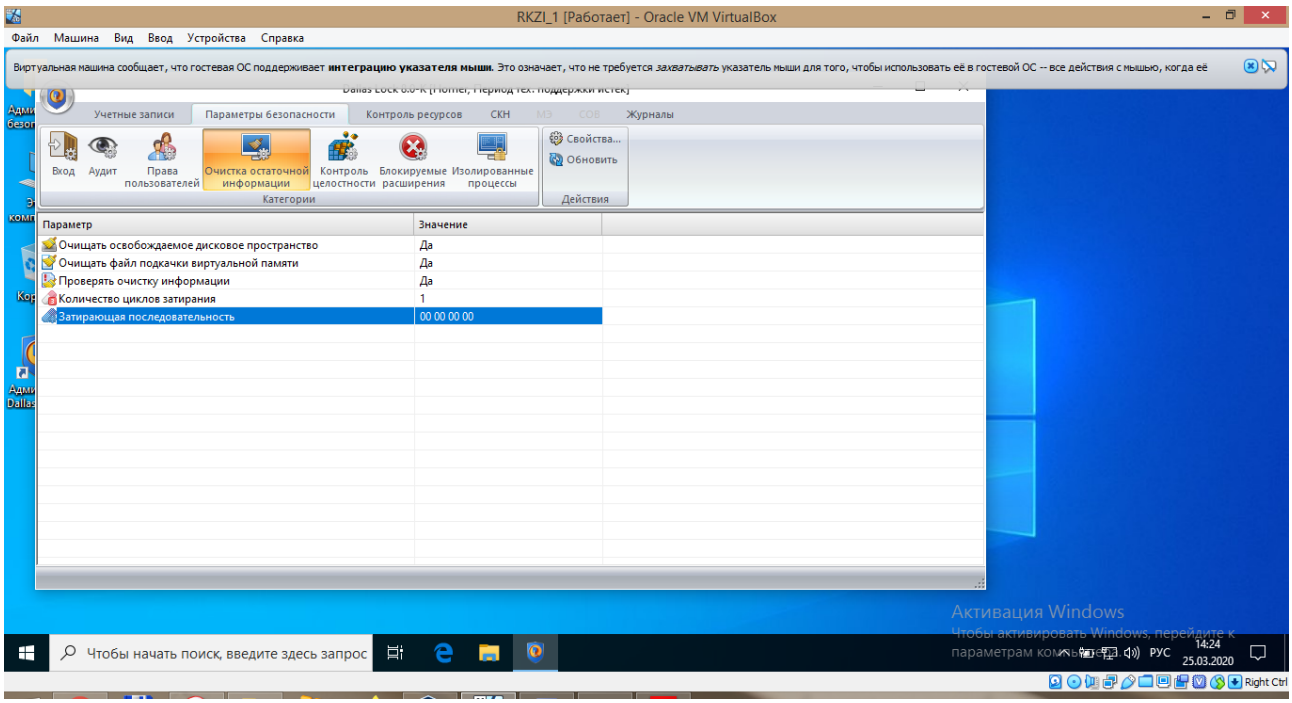

Рисунок 17

Выполним настройку регистрации событий для объектов доступа, для этого:

- откроем оболочку администратора системы защиты;
- перейдем в категорию «Аудит» на вкладке «Параметры безопасности»;
- для настройки аудита локальных объектов ФС необходимо перейти в категорию «Аудит» на вкладке «Контроль ресурсов», добавить необходимые объекты, перейти во вкладку «Аудит доступа».

Пример настройки полного объекта для локального объекта ФС C:\Work\Тамара представлен на рисунках 18-19: при открытии вкладки «Общие» параметров безопасности видно, что аудит выключен; необходимо включить его, установив флаг в поле «Аудит включен» во вкладке «Аудит доступа»; затем отметить необходимые события (в примере включен полный аудит).

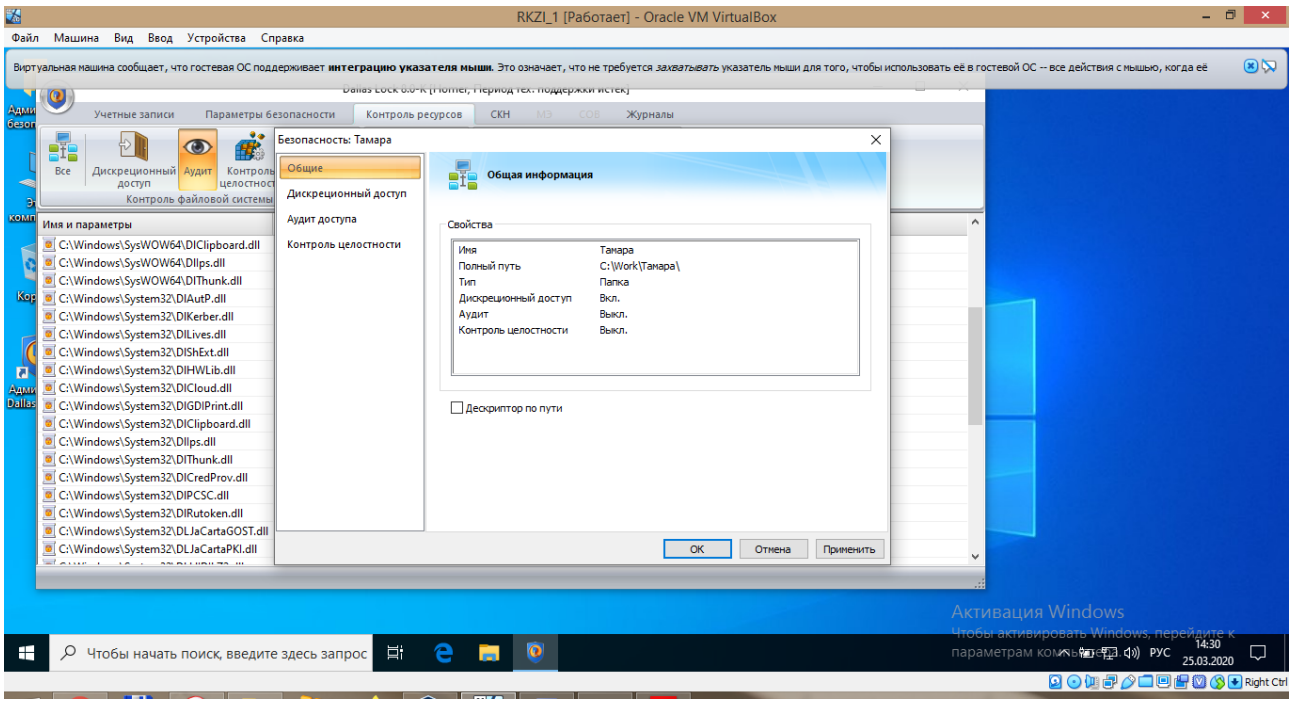

Рисунок 18

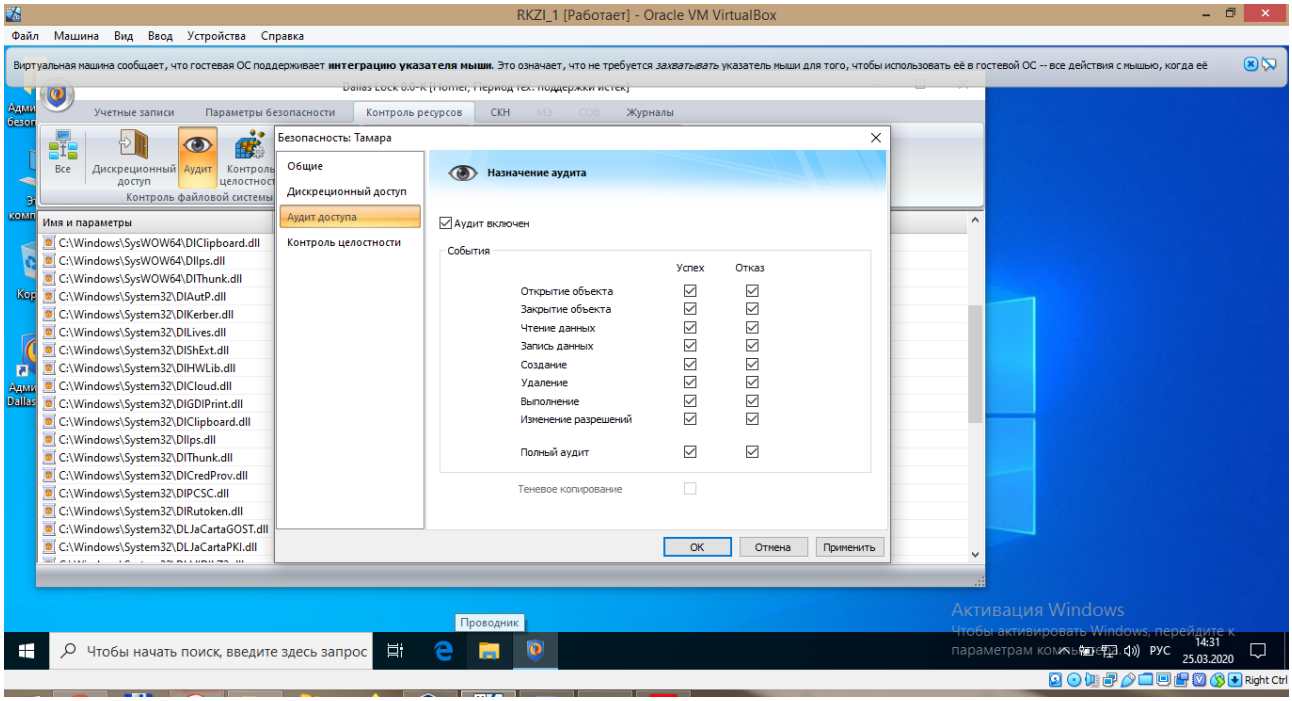

Рисунок 19

Выполним настройку контроля целостности файловой системы и программно-аппаратной среды.

Откроем оболочку администратора системы защиты, для настройки общих параметров перейдем в категорию «Контроль целостности» на вкладке «Параметры безопасности», выполним необходимые настройки по

периодичности проверки целостности отдельно для объектов ФС, отдельно для объектов программно-аппаратной среды и отдельно для реестра (рисунок 20).

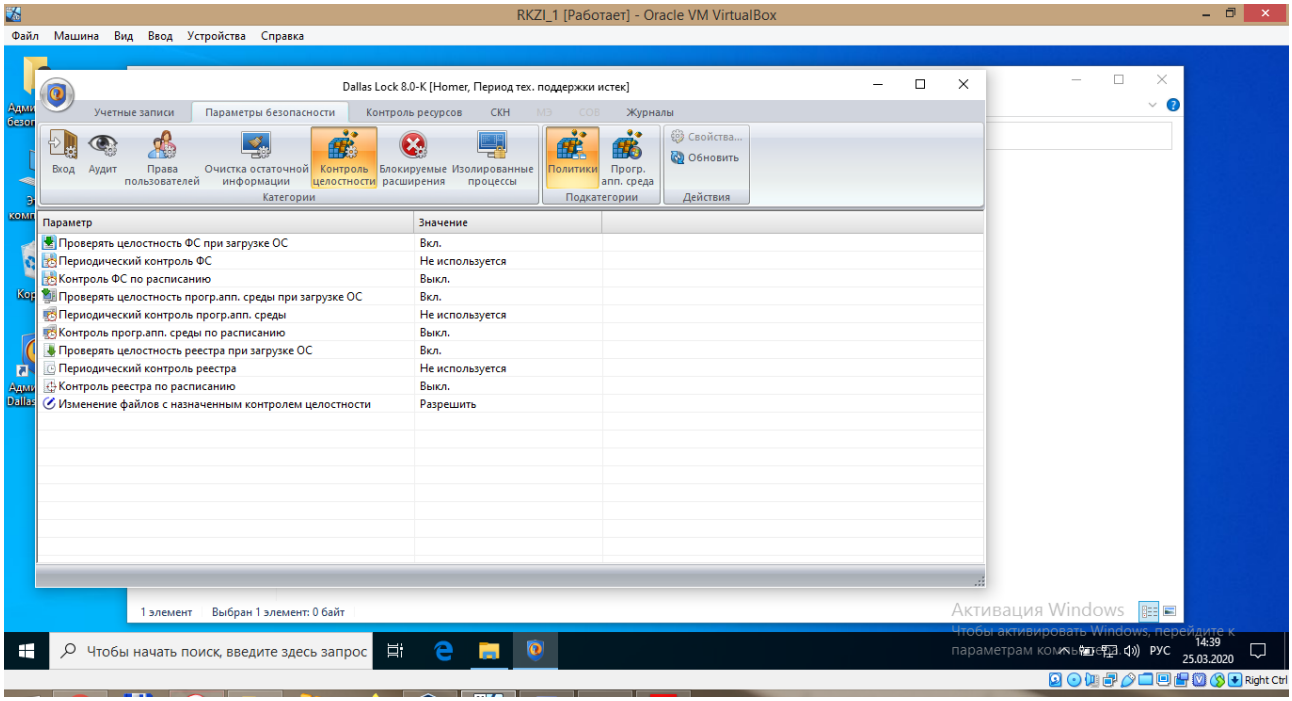

Рисунок 20

Перейдем во вкладку «Прогр. апп. среда», для выбранных параметров открываем «Редактирование параметров безопасности», снимаем флаг «Не используется» (рисунок 21), выбираем алгоритм расчета контрольной суммы (CRC32, ГОСТ Р 34.11- 94, MD5 – рисунок 22), нажимаем «Применить». Результаты настройки для объектов программно-аппаратной среды представлены на рисунке 23.

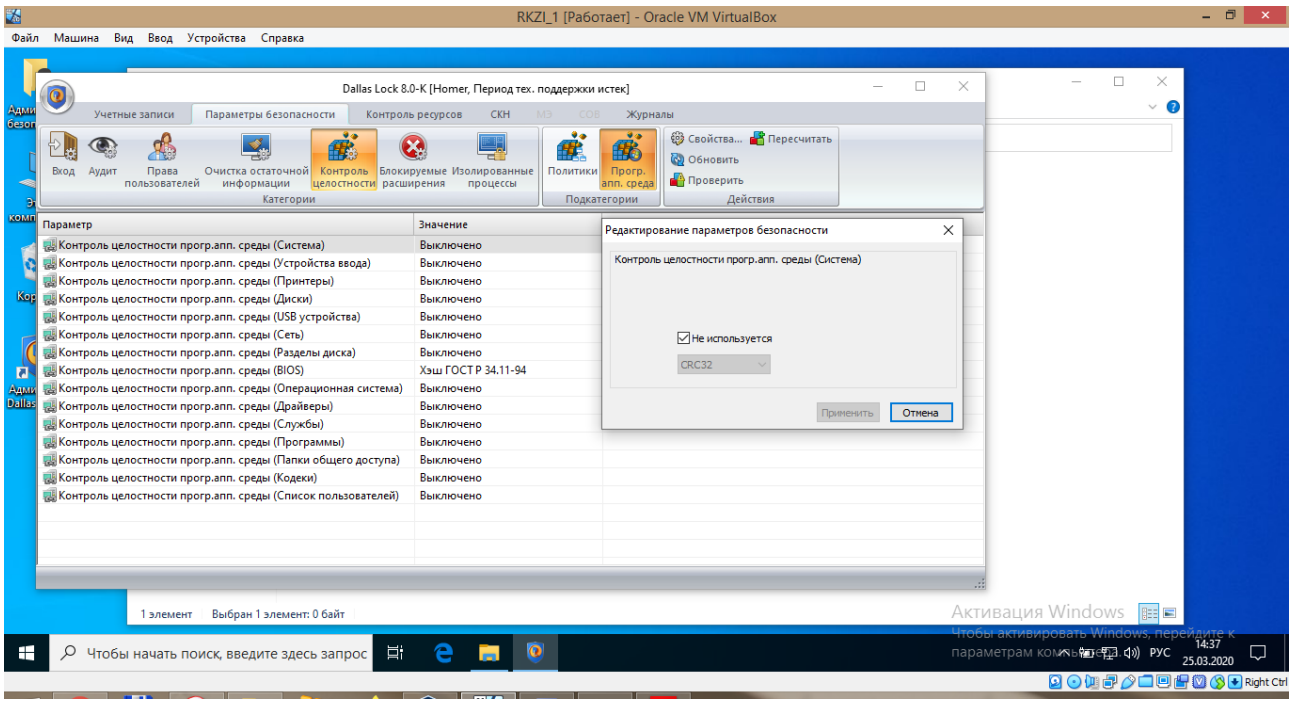

Рисунок 21

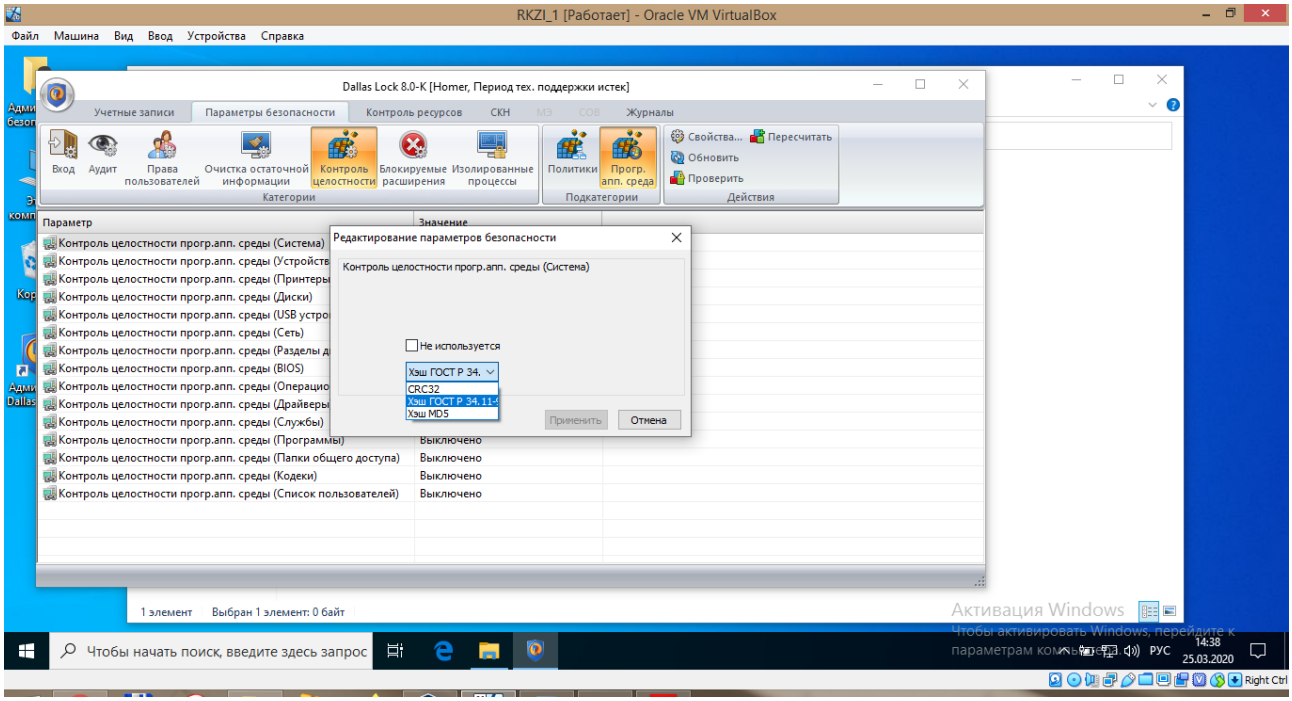

Рисунок 22

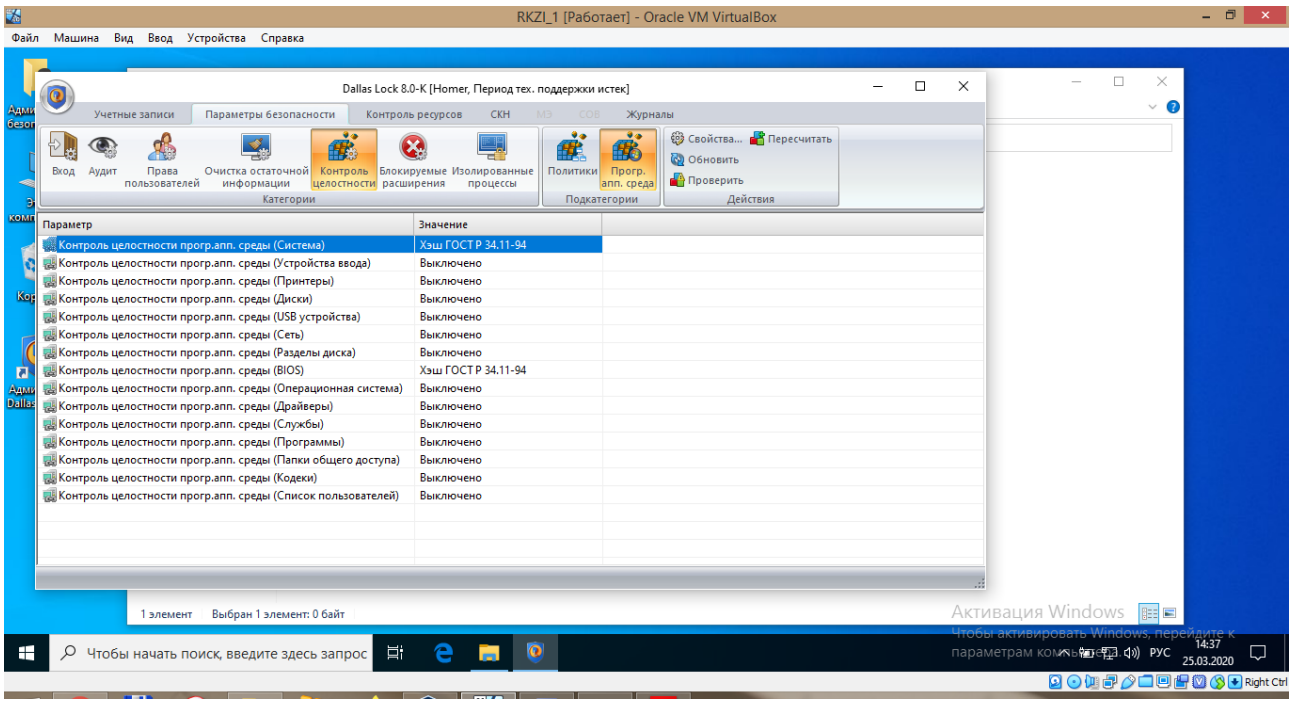

Рисунок 23

Для настройки контроля целостности объектов реестра выберем опцию «Добавить (Реестр)» в категории «Контроль целостности» на вкладке «Параметры безопасности» (рисунок 24), добавим для примера HKEY_USERS\DEFAULT\Control Panel\Cursors, выберем данный объект и в появившемся окне откроем вкладку «Контроль целостности». Отметим флажком поле «Контроль целостности включен», выберем алгоритм расчета контрольной суммы (рисунок 25) и нажмем кнопку «Пересчитать» (рисунок 26). Сохраним результат нажатием на «Применить» и «Ок».

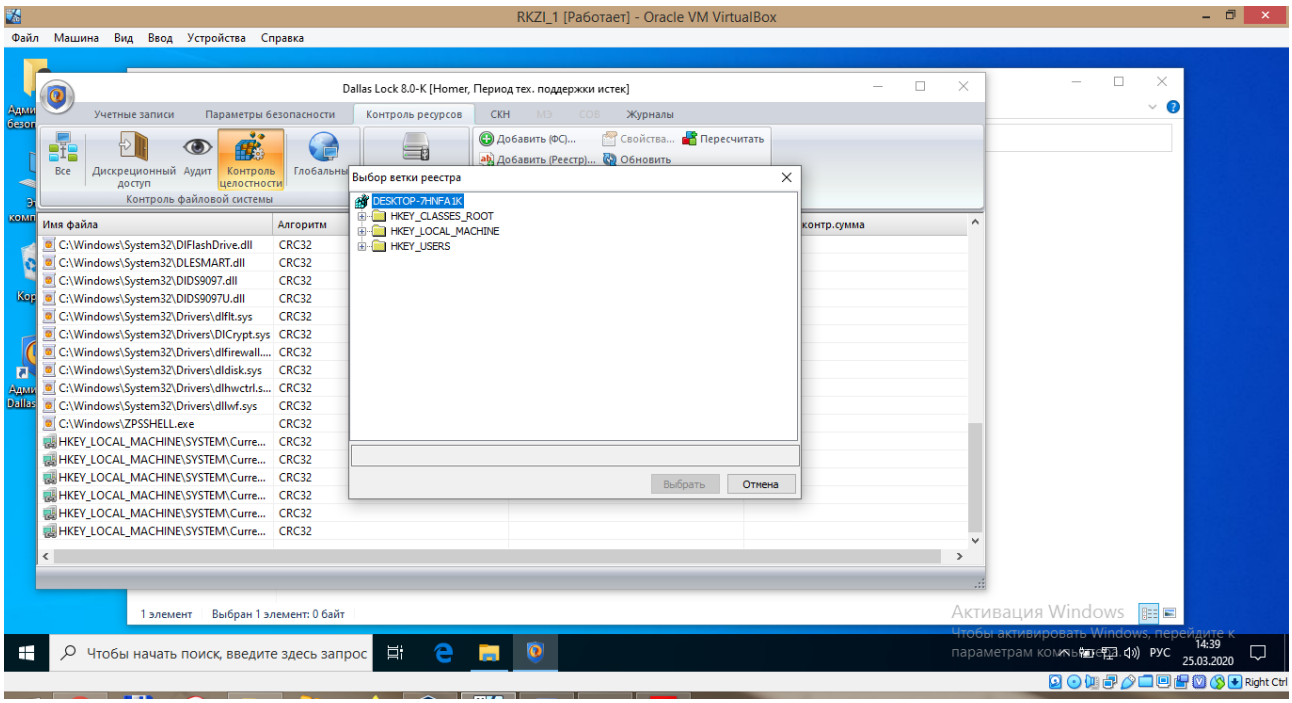

Рисунок 24

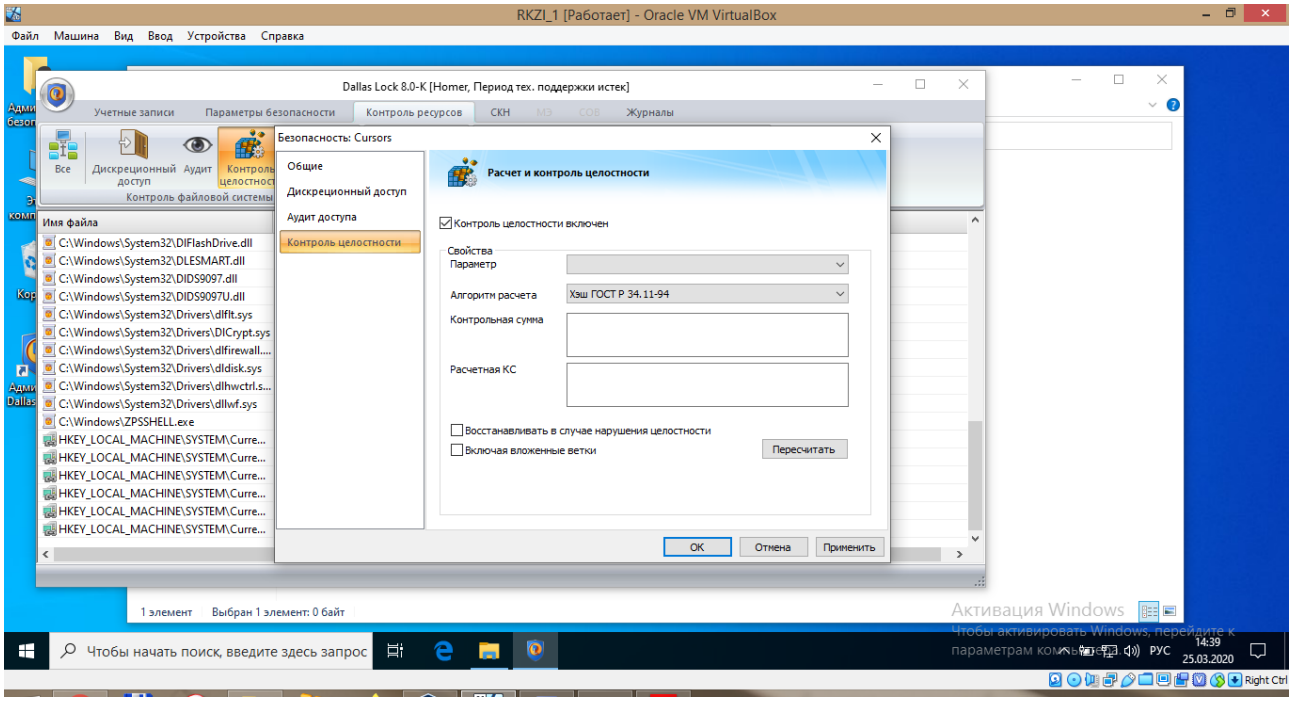

Рисунок 25

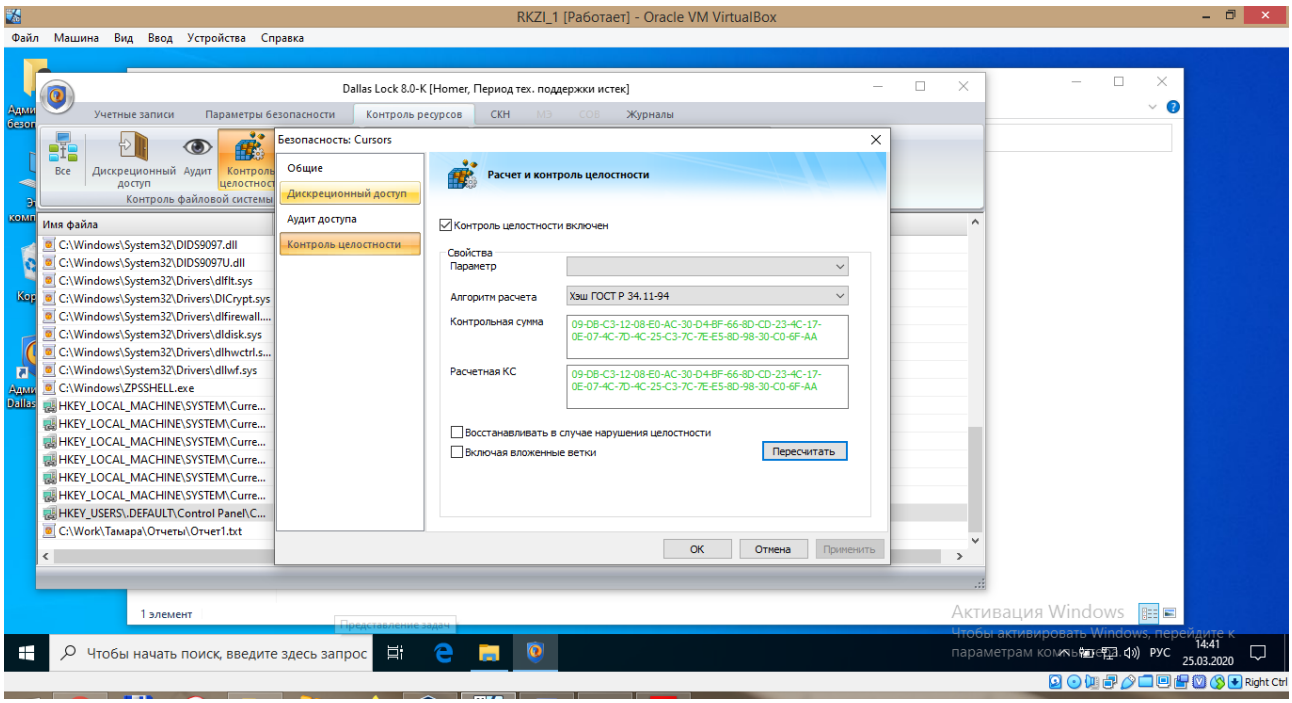

Рисунок 26

Для настройки контроля целостности объектов ФС выберем опцию «Добавить (ФС)» в категории «Контроль целостности» на вкладке «Параметры безопасности», выберем объект Отчет1.txt, находящийся в каталоге C:\Work\Тамара (рисунок 27).

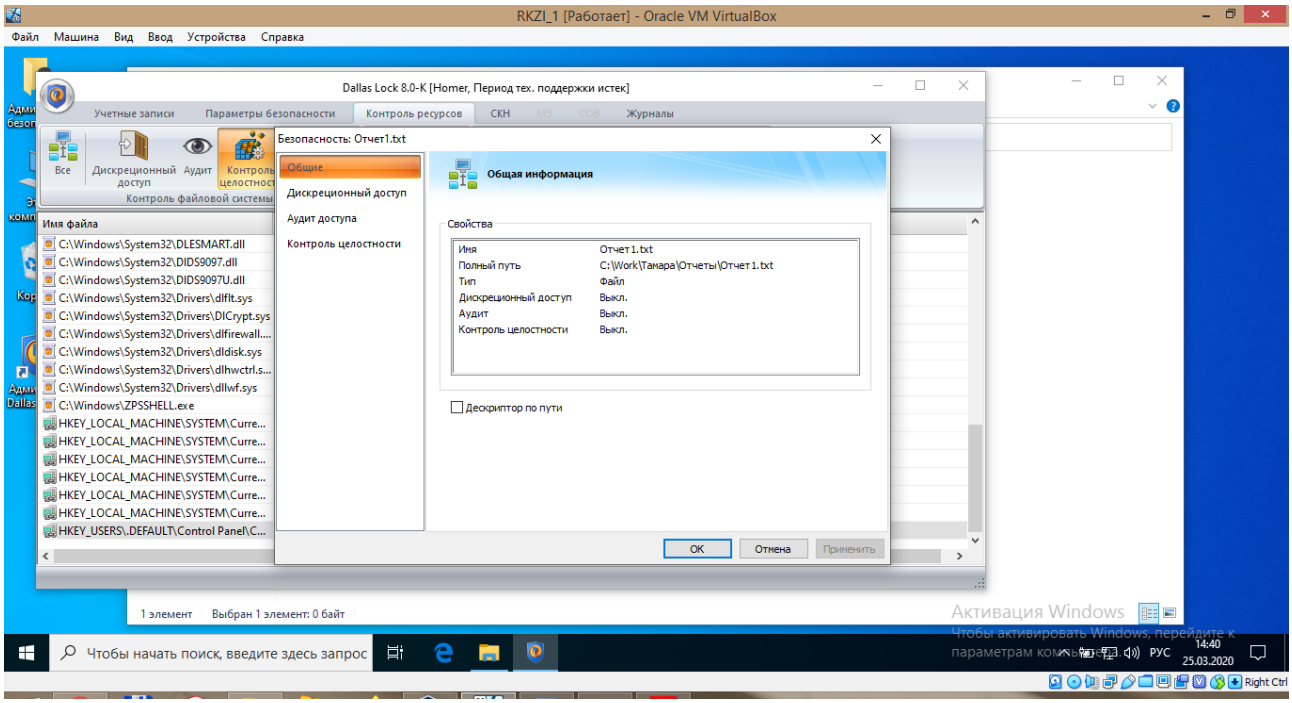

Рисунок 27

На вкладке «Контроль целостности» выполним действия, аналогичные тем, что применялись в настройке контроля целостности для объектов реестра (рисунок 28).

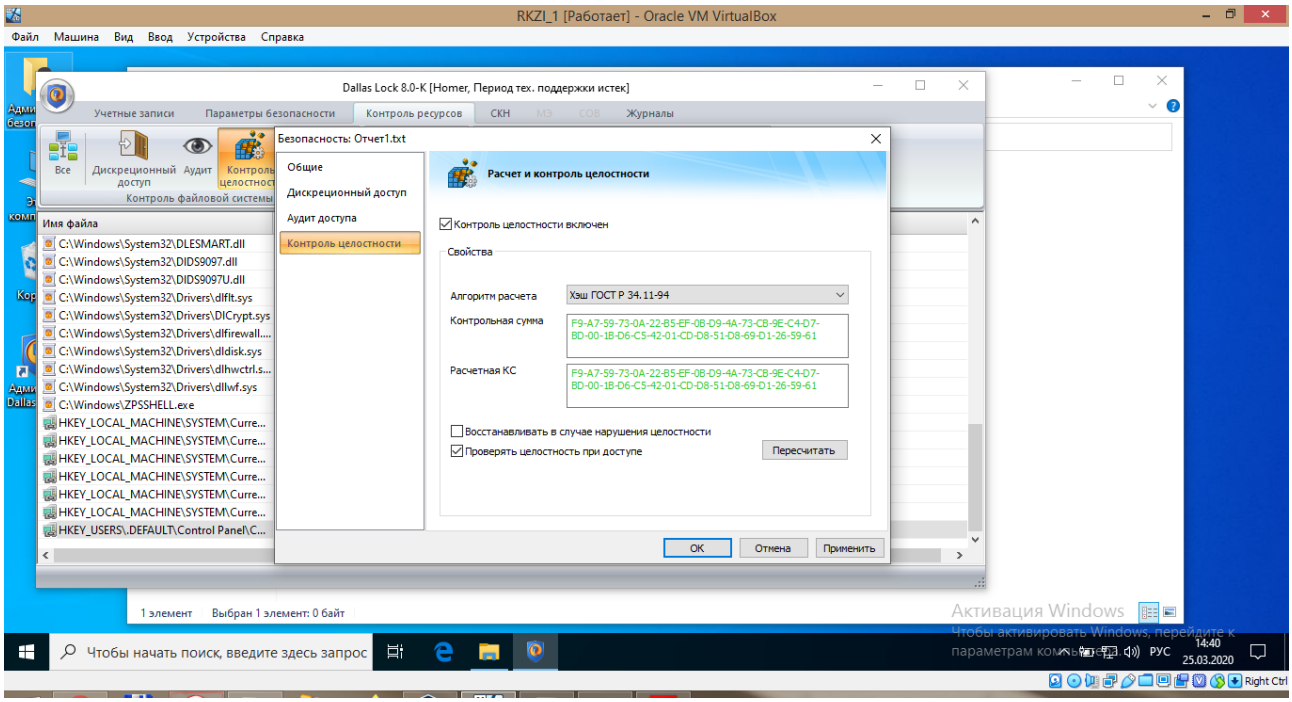

Рисунок 28

На рисунке 29 представлен результат настройки контроля целостности (в списке появились добавленные нами объекты).

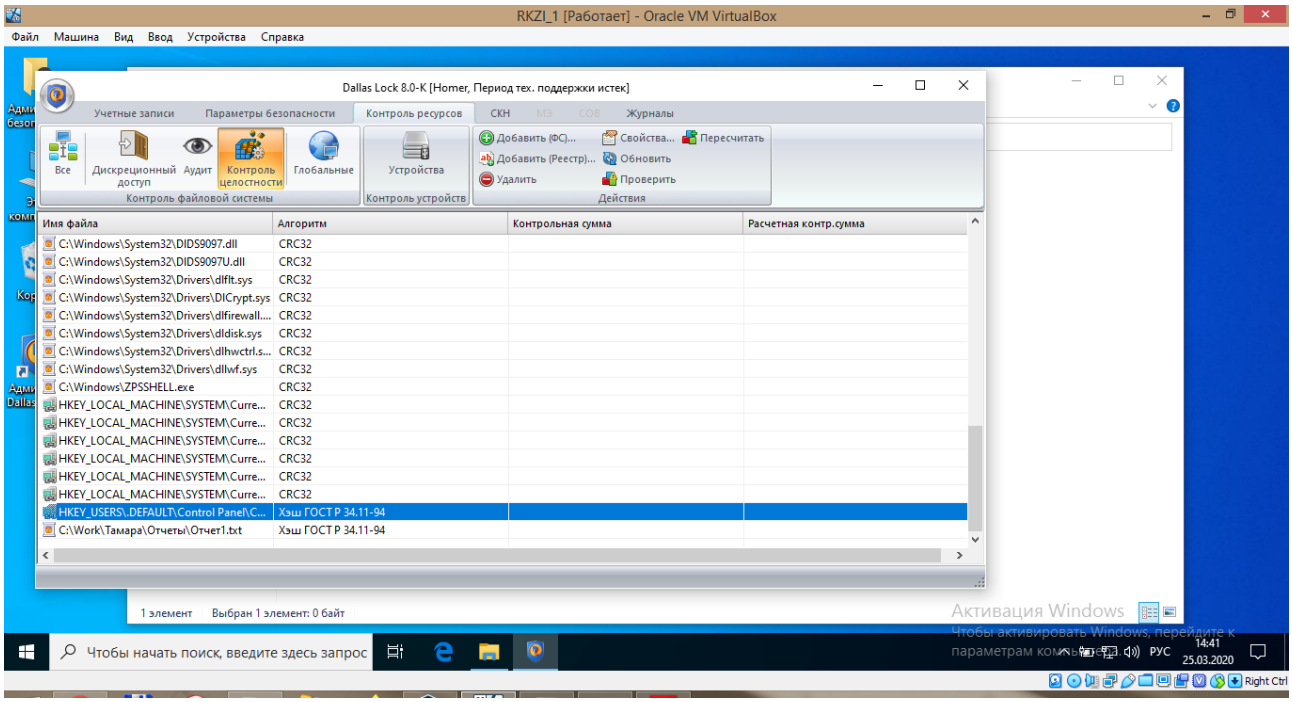

Рисунок 29

Выполним настройку внешних носителей информации:

- подключим внешний носитель;
- откроем оболочку администратора системы защиты;
- перейдем в категорию «Сменные накопители» на вкладке «СКН», нажмем кнопку «Добавить…» и выберем необходимый носитель информации (рисунок 30);
- перейдем в настройки безопасности выбранного носителя (рисунок 31);
- выполним настройку дискреционного доступа (рисунок 32): даем полный доступ администратору системы Homer, всем остальным запрещаем доступ.

Настроенный внешний носитель информации отображается в списке сменных накопителей, в графе «Назначенные права» отображается «Дискреционный доступ» (рисунок 33).

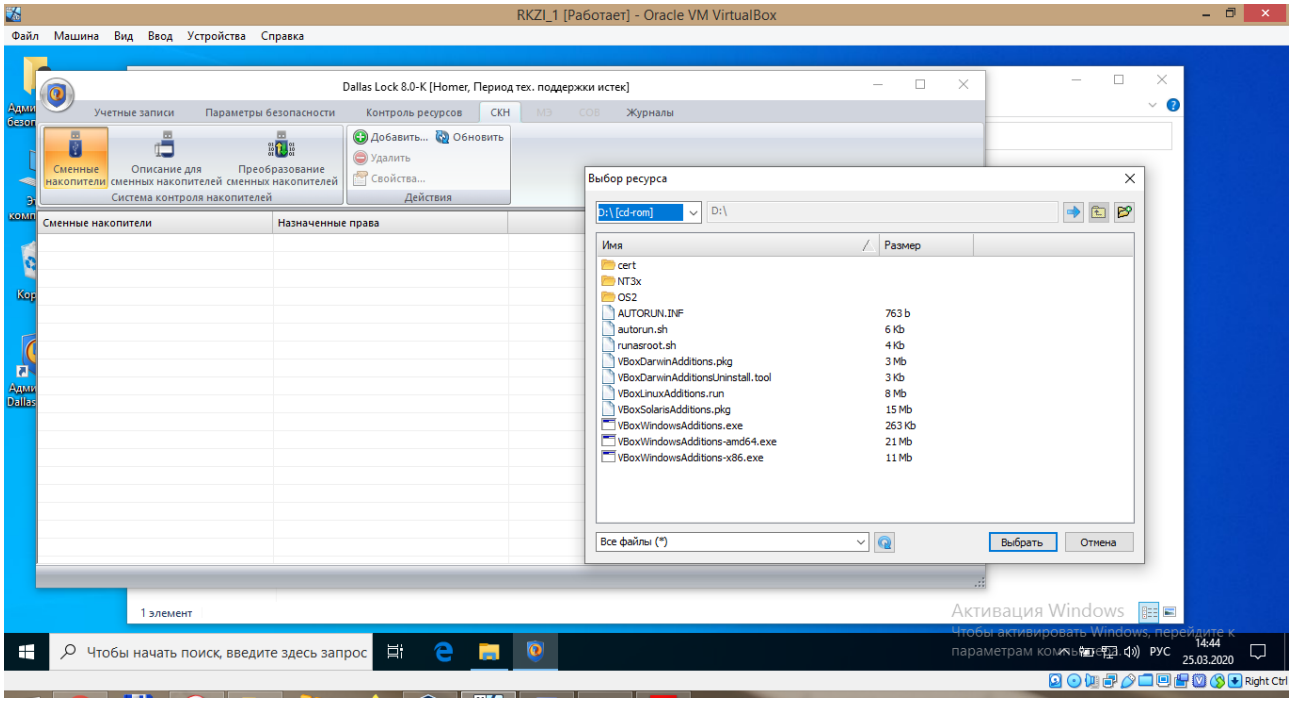

Рисунок 30

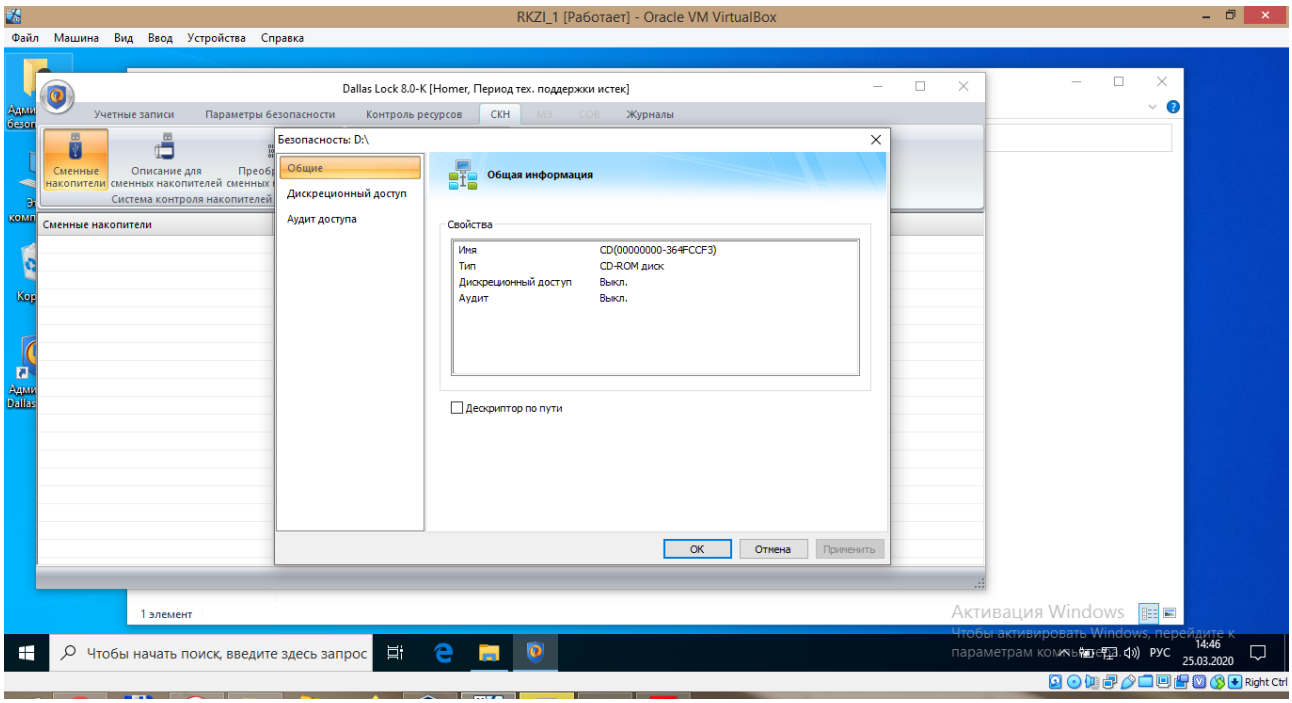

Рисунок 31

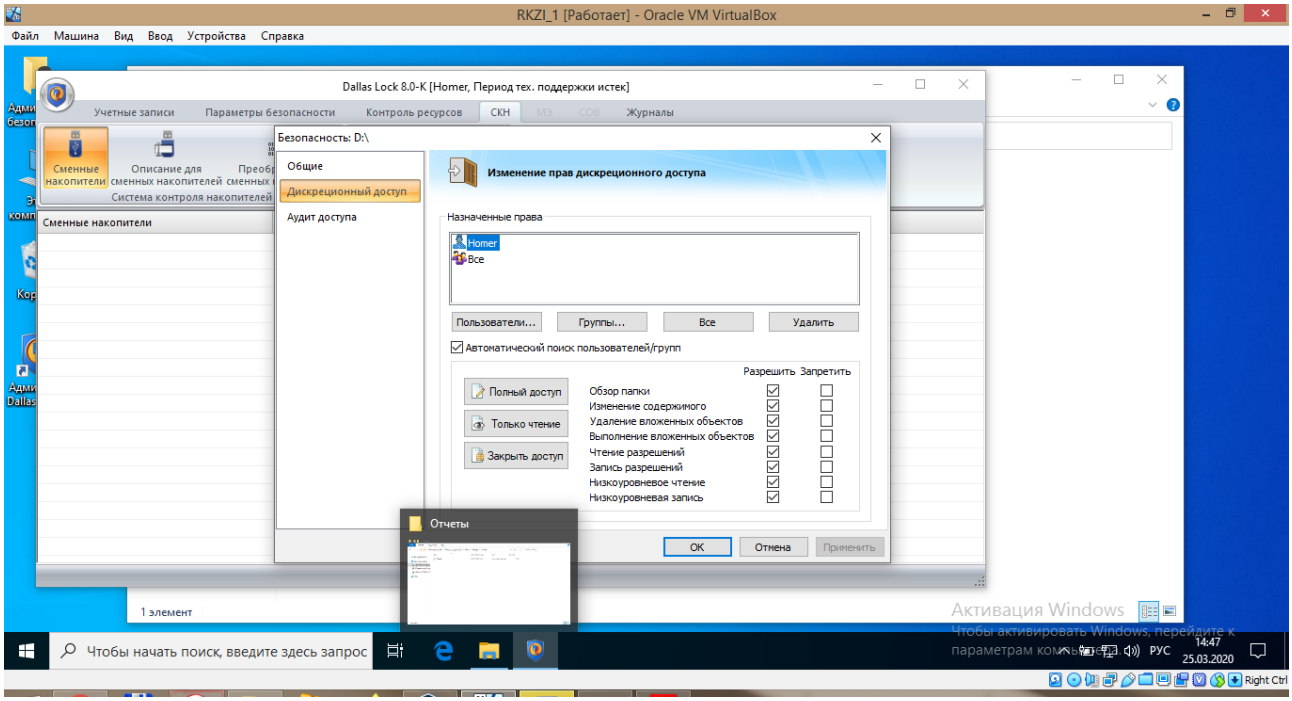

Рисунок 32

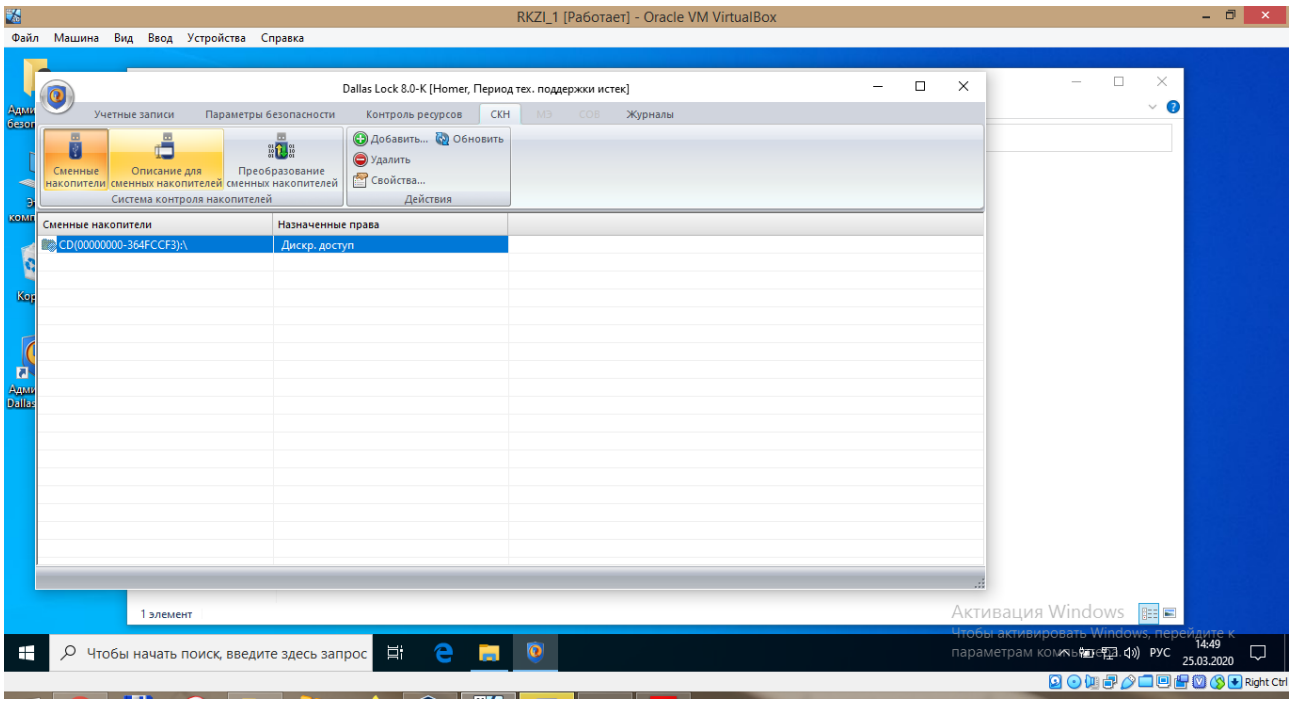

Рисунок 33

Выводы.

В ходе лабораторной работы были исследованы возможности СЗИ НСД «Dallas Lock» и получены практические навыки конфигурирования данного средства защиты путем выполнения настройки идентификации и аутентификации, очистки остаточной информации, регистрации событий для объектов доступа, контроля целостности файловой системы и программно-аппаратной среды, внешних носителей информации, а также установки правил разграничения доступа.